



TESIS PM-147501

**PERANCANGAN SISTEM MANAJEMEN KEAMANAN  
INFORMASI (SMKI) BERDASARKAN SNI ISO/IEC  
27001:2013 DAN SNI ISO/IEC 27005:2013 (STUDI KASUS  
DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN  
SISTEM INFORMASI - INSTITUT TEKNOLOGI  
SEPULUH NOPEMBER)**

Furqon Mauladani  
092114.5005.3024

DOSEN PEMBIMBING  
Daniel Oranova S, S.Kom., M.Sc., PD.Eng

DEPARTEMEN MANAJEMEN TEKNOLOGI  
BIDANG KEAHLIAN MANAJEMEN TEKNOLOGI INFORMASI  
FAKULTAS BISNIS DAN MANAJEMEN TEKNOLOGI  
INSTITUT TEKNOLOGI SEPULUH NOPEMBER  
SURABAYA  
2017



## LEMBAR PENGESAHAN

Tesis disusun untuk memenuhi salah satu syarat memperoleh gelar  
Magister Manajemen Teknologi (M.MT)  
di  
Institut Teknologi Sepuluh Nopember

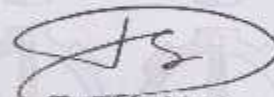
Oleh:

**FUROON MAULADANI**  
NRP. 092114.5005.3024

Tanggal Ujian : 20 Nopember 2017  
Periode Wisuda : September 2018

Disetujui oleh:

1. **Dr. Daniel Oranova Siahaan, S.Kom., M.Sc.,  
PDEng.**  
NIP. 197411232006041001

  
(Pembimbing)

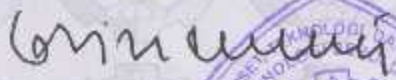
2. **Dr. Ir. Raden Venantius Hari Ginardi, M.Sc.**  
NIP. 196505181992031003

  
(Penguji)

3. **Prof. Dr. Drs. Mohammad Isa Irawan, M.T.**  
NIP. 196312251989031001

(Penguji)

Dekan Fakultas Bisnis dan Manajemen Teknologi,

  
**Prof. Dr. Ir. Udisubakti Ciptomulyono, M.Eng.Sc**  
NIP. 19590318 198701 1 001



*Halaman ini sengaja dikosongkan*



**PERANCANGAN SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI)  
BERDASARKAN SNI ISO/IEC 27001:2013 DAN SNI ISO/IEC 27005:2013  
(STUDI KASUS DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN  
SISTEM INFORMASI - INSTITUT TEKNOLOGI SEPULUH NOPEMBER)**

Oleh : Furqon Mauladani  
NRP : 092114.5005.3024  
Pembimbing : Daniel Oranova S, S.Kom., M.Sc., PD.Eng.

**ABSTRAK**

Semakin pesatnya penggunaan TIK membuat semakin tingginya ancaman terhadap aset informasi, seperti ancaman yang berasal dari luar (penyebaran *malware*, aktifitas *social engineering*), orang dalam (sengaja, tidak sengaja), kegagalan teknis (kesalahan penggunaan, kegagalan perangkat keras/lunak) ataupun bencana alam (kebakaran, gempa, banjir). Beberapa ancaman tersebut merupakan resiko yang berdampak merugikan bagi organisasi, seperti kerugian finansial, terganggunya proses bisnis, masalah peraturan/hukum, dan penurunan reputasi organisasi. Hal tersebut memiliki efek domino yang mengancam keberlangsungan aktifitas bisnis organisasi, tak terkecuali DPTSI-ITS. DPTSI-ITS merupakan badan yang bertugas mengelola teknologi dan sistem informasi terpadu di perguruan tinggi ITS.

Metode yang digunakan penelitian ini untuk penyelesaian masalah yang dibahas adalah melakukan manajemen resiko keamanan informasi berdasarkan SNI ISO/IEC 27005 dan perancangan dokumen SMKI berdasarkan SNI ISO/IEC 27001. Alasan penggunaan kedua standar tersebut karena pemerintah Indonesia melalui BSN telah menjadikan SNI ISO/IEC 27001 dan SNI ISO/IEC 27005 sebagai standar SNI dalam mengelola keamanan informasi untuk semua organisasi dengan tipe dan ukuran apapun. Manajemen resiko keamanan informasi digunakan untuk mengidentifikasi, menganalisa dan mengevaluasi resiko yang dihadapi oleh DPTSI-ITS. Setelah itu kita merencanakan penanganan resiko yang akan dilakukan, seperti *risk modification*, *risk avoidance*, *risk sharing*, atau *risk retention*.

Hasil penelitian ini adalah 60 resiko yang tidak diterima dari total 228 resiko yang telah teridentifikasi. Dari 60 resiko tersebut, terdapat 58 *risk modification*, 1 *risk avoidance*, dan 1 *risk sharing*. Tata kelola keamanan informasi yang dirancang berdasarkan SNI ISO/IEC 27001 adalah ruang lingkup SMKI, kebijakan SMKI, proses penilaian resiko, proses penanganan resiko, *statement of applicability*, dan sasaran keamanan informasi.

Kata kunci: SNI ISO/IEC 27001:2013, SNI ISO/IEC 27005:2013, Sistem Manajemen Keamanan Informasi (SMKI), Manajemen Resiko Keamanan Informasi, Tata Kelola.

*Halaman ini sengaja dikosongkan*

**DESIGNING INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)  
BASED ON SNI ISO/IEC 27001:2013 AND SNI ISO/IEC 27005:2013 (CASE  
STUDY DIRECTORATE OF TECHNOLOGY AND INFORMATION SYSTEM  
DEVELOPMENT - INSTITUT TEKNOLOGI SEPULUH NOPEMBER)**

Author : Furqon Mauladani  
NRP : 092114.5005.3024  
Supervisor : Daniel Oranova S, S.Kom., M.Sc., PD.Eng.

**ABSTRACT**

The rapid use of ICTs increased the threat on information assets. The threats include external threats (e.g. malware deployment, social engineering activities), insiders (i.e. intentionally and unintentionally), technical failure (e.g. misuse, hardware/software failure) or disaster nature (e.g. fire, earthquake, flood). Some threats introduce risks that adversely affect the organization, such as financial losses, business process disruption, regulatory/legal issues, and the deterioration of the organization's reputation. Risk have a domino effect which threatens the sustainability of business activities of the organization, not to mention DPTSI-ITS. DPTSI-ITS is the body which in charge of managing integrated ICT service in ITS.

The methods used for this research to solve mentioned problem is perform information security risk management based on SNI ISO/IEC 27005 and to design SMKI document based on SNI ISO/IEC 27001. The reason for the use of both standards is because the government of Indonesia through BSN has made SNI ISO/IEC 27001 and SNI ISO/IEC 27005 as SNI standard in managing information security for all organizations of any type and size. Information security risk management is used to identify, analyze and evaluate the risks faced by DPTSI-ITS. After that, we designed risk treatment plan. Risk treatment plan includes risk modification, risk avoidance, risk sharing or risk retention.

This research found 60 unacceptable risks from total of 228 risk after identified. Out of 66 risk, there are 58 risk modification, 1 risk avoidance, 1 risk sharing. Information security governance designed based on SNI ISO/IEC 27001 is ISMS scope, ISMS policy, risk assessment process, risk treatment process, statement of applicability, and information security objective.

**Keywords:** SNI ISO/IEC 27001:2013, SNI ISO/IEC 27005:2013, Information Security Management System (ISMS), Information Security Risk Management, Governance.

*Halaman ini sengaja dikosongkan*

## KATA PENGANTAR

Segala puji bagi Allah subhanahuwata'ala atas berbagai limpahan rahmat, hidayah, serta bimbingan-Nya. Serta tidak lupa shalawat dan salam semoga tercurah kepada bimbingan kita, nabi Muhammad shallallohu'alaihiwasallam. Akhirnya penulis dapat menyelesaikan tesis yang berjudul "Perancangan Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan SNI ISO/IEC 27001:2013 dan SNI ISO/IEC 27005:2013 (Studi Kasus DPTSI-ITS)". Selain itu penulis juga mengucapkan terimakasih kepada pihak yang secara langsung maupun tidak langsung membantu dalam penyusunan tesis ini:

1. Mama dan papa (almarhum) yang selalu membantu dari segi finansial, doa dan dukungannya untuk dapat kuliah S2 di MMT-ITS agar meraih gelar magister.
2. Bapak Dr. Ir. R.V. Hari Ginardi, M.Sc. selaku pemimpin program studi Magister Manajemen Teknologi di ITS.
3. Bapak Daniel Oranova S, S.Kom., M.Sc., PD.Eng. selaku pembimbing yang memberikan kritik dan saran selama penyusunan penelitian ini.
4. Bapak Dr.Eng. Febriliyan Samopa, S.Kom., M.Kom. selaku kepala DPTSI-ITS yang telah membantu dan memberikan izin penelitian ini.
5. Bapak Royyana, bapak Wicaksono, mas Jananta, bapak Jainul, ibu Widiyaningsih, ibu Hanim, ibu Anny dan karyawan lainnya di DPTSI-ITS yang membantu dalam wawancara dan peninjauan dokumen pada penelitian ini.
6. Bapak Abraham, mas Anto, mas Iqbal, mbak Sarah serta seluruh dosen dan teman-teman lainnya di MMT-ITS yang telah menemani selama proses perkuliahan.
7. Mas Eka yang telah membantu menjawab masalah yang dihadapi penulis dan memberikan masukan tentang SNI ISO/IEC 27001 dan SNI ISO/IEC 27005.

Setiap karya manusia pastinya memiliki beberapa kekurangan dan tidaklah sempurna seperti pada penelitian ini, maka dari itu penulis mengharapkan segala kritik dan saran yang membangun untuk pengembangan penelitian ini maupun untuk yang selanjutnya. Akhir kata, semoga penelitian ini dapat menjadi referensi dan mengembangkan ilmu pengetahuan di bidang keamanan informasi dan komputer.

Salam Hormat

Furqon Mauladani, S.Kom.

## DAFTAR ISI

|                                 |      |
|---------------------------------|------|
| LEMBAR PENGESAHAN.....          | i    |
| ABSTRAK.....                    | iii  |
| ABSTRACT.....                   | v    |
| KATA PENGANTAR.....             | vii  |
| DAFTAR ISI.....                 | ix   |
| DAFTAR GAMBAR.....              | xv   |
| DAFTAR TABEL.....               | xvii |
| DAFTAR LAMPIRAN.....            | xix  |
| BAB I PENDAHULUAN               |      |
| 1.1. Latar Belakang.....        | 1    |
| 1.2. Perumusan Masalah.....     | 7    |
| 1.3. Tujuan Penelitian.....     | 7    |
| 1.4. Manfaat Penelitian.....    | 7    |
| 1.5. Batasan Masalah.....       | 8    |
| BAB II KAJIAN PUSTAKA           |      |
| 2.1. DPTSI-ITS.....             | 9    |
| 2.1.1. Profil ITS.....          | 9    |
| 2.1.2. Profil DPTSI-ITS.....    | 10   |
| 2.1.3. Visi, Misi & Tujuan..... | 11   |
| 2.1.4. Struktur Organisasi..... | 12   |



|                                                                             |    |
|-----------------------------------------------------------------------------|----|
| 2.1.5. Proses Bisnis.....                                                   | 12 |
| 2.2. Keamanan Informasi dalam Organisasi.....                               | 14 |
| 2.2.1. Informasi.....                                                       | 14 |
| 2.2.2. Keamanan Informasi.....                                              | 15 |
| 2.2.3. Prinsip Keamanan Informasi.....                                      | 16 |
| 2.2.4. Standar untuk Tata Kelola Keamanan Informasi.....                    | 18 |
| 2.3. SNI ISO/IEC 27001 – Sistem Manajemen Keamanan Informasi (SMKI).....    | 20 |
| 2.3.1. SNI ISO/IEC 27001.....                                               | 20 |
| 2.3.2. Sistem Manajemen Keamanan Informasi (SMKI).....                      | 20 |
| 2.3.3. Struktur SNI ISO/IEC 27001.....                                      | 22 |
| 2.3.4. Keluarga SMKI.....                                                   | 28 |
| 2.3.5. Tahapan Perencanaan SMKI.....                                        | 30 |
| 2.3.5.1. Mendapatkan Persetujuan Pimpinan.....                              | 30 |
| 2.3.5.2. Mendefinisikan Ruang Lingkup dan Batasan.....                      | 31 |
| 2.3.5.3. Menetapkan Peran dan Tanggung Jawab.....                           | 31 |
| 2.3.5.4. Mendefinisikan Kebijakan SMKI.....                                 | 35 |
| 2.3.5.5. Melakukan Analisis Kesenjangan.....                                | 36 |
| 2.3.5.6. Melakukan Penilaian dan Perencanaan Penanganan<br>Resiko.....      | 37 |
| 2.3.5.7. Menetapkan Kontrol Keamanan dan Sasaran Keamanan<br>Informasi..... | 38 |
| 2.3.6. Dokumen SMKI.....                                                    | 39 |

|          |                                                              |    |
|----------|--------------------------------------------------------------|----|
| 2.3.6.1. | Struktur Dokumen SMKI.....                                   | 39 |
| 2.3.6.2. | Dokumen yang Dibutuhkan.....                                 | 40 |
| 2.3.7.   | Keuntungan Penerapan SNI ISO/IEC 27001.....                  | 43 |
| 2.3.8.   | Faktor Kesuksesan Penerapan SNI ISO/IEC 27001.....           | 44 |
| 2.4.     | SNI ISO/IEC 27002 – Kontrol Keamanan.....                    | 44 |
| 2.4.1.   | SNI ISO/IEC 27002.....                                       | 44 |
| 2.4.2.   | Kontrol Keamanan.....                                        | 45 |
| 2.5.     | SNI ISO/IEC 27005 – Manajemen Resiko Keamanan Informasi..... | 45 |
| 2.5.1.   | SNI ISO/IEC 27005.....                                       | 45 |
| 2.5.2.   | Resiko dalam Keamanan Informasi.....                         | 46 |
| 2.5.3.   | Manajemen Resiko Keamanan Informasi.....                     | 47 |
| 2.5.4.   | Penetapan Konteks ( <i>Context Establishment</i> ).....      | 49 |
| 2.5.4.1. | Pengaturan Kriteria Resiko.....                              | 49 |
| 2.5.4.2. | Pengaturan Kriteria Dampak dan Kemungkinan.....              | 50 |
| 2.5.4.3. | Mendefinisikan Ruang Lingkup dan Batasan.....                | 50 |
| 2.5.4.4. | Menetapkan Peran dan Tanggung Jawab.....                     | 51 |
| 2.5.5.   | Penilaian Resiko ( <i>Risk Assessment</i> ).....             | 51 |
| 2.5.5.1. | Identifikasi Resiko ( <i>Risk Identification</i> ).....      | 51 |
| 2.5.5.2. | Analisis Resiko ( <i>Risk Analysis</i> ).....                | 58 |
| 2.5.5.3. | Evaluasi Resiko ( <i>Risk Evaluation</i> ).....              | 63 |
| 2.5.6.   | Penanganan Resiko ( <i>Risk Treatment</i> ).....             | 63 |
| 2.5.6.1. | Modifikasi Resiko ( <i>Risk Modification</i> ).....          | 63 |

|                                                            |    |
|------------------------------------------------------------|----|
| 2.5.6.2. Menghindari Resiko ( <i>Risk Avoidance</i> )..... | 64 |
| 2.5.6.3. Membagi Resiko ( <i>Risk Sharing</i> ).....       | 64 |
| 2.5.6.4. Menyimpan Resiko ( <i>Risk Retention</i> ).....   | 65 |
| 2.5.7. Komunikasi dan Konsultasi.....                      | 65 |
| 2.5.8. Pengawasan dan Peninjauan.....                      | 66 |
| 2.5.9. Perbedaan Pemilik Resiko dan Pemilik Aset.....      | 66 |

### BAB III METODE PENELITIAN

|                                                        |    |
|--------------------------------------------------------|----|
| 3.1. Pendahuluan.....                                  | 70 |
| 3.1.1. Identifikasi Masalah.....                       | 70 |
| 3.1.2. Studi Literatur.....                            | 70 |
| 3.2. Pengumpulan Data.....                             | 70 |
| 3.2.1. Peninjauan Dokumen.....                         | 70 |
| 3.2.2. Wawancara.....                                  | 71 |
| 3.2.3. Observasi.....                                  | 71 |
| 3.3. Penetapan Konteks.....                            | 71 |
| 3.3.1. Pengaturan Kriteria Resiko.....                 | 71 |
| 3.3.2. Pengaturan Kriteria Dampak dan Kemungkinan..... | 71 |
| 3.3.3. Pendefinisian Ruang Lingkup dan Batasan.....    | 72 |
| 3.3.4. Penetapan Peran dan Tanggung Jawab.....         | 72 |
| 3.4. Pengusulan Kebijakan SMKI.....                    | 72 |
| 3.5. Pelaksanaan Analisis Kesenjangan.....             | 72 |
| 3.6. Penilaian Resiko.....                             | 74 |

|                                                        |     |
|--------------------------------------------------------|-----|
| 3.6.1. Identifikasi Resiko.....                        | 74  |
| 3.6.2. Analisis Resiko.....                            | 80  |
| 3.6.3. Evaluasi Resiko.....                            | 83  |
| 3.7. Perencanaan Penanganan Resiko.....                | 83  |
| 3.7.1. Pemilihan Penanganan Resiko.....                | 83  |
| 3.7.2. Penetapan Kontrol Keamanan dan Sasarannya.....  | 85  |
| 3.8. Perancangan Dokumen SMKI.....                     | 88  |
| 3.9. Pembuatan Kesimpulan dan Saran.....               | 88  |
| 3.10. Rencana dan Jadwal Kerja Penelitian.....         | 89  |
| <br>BAB IV HASIL PENELITIAN                            |     |
| 4.1. Pengumpulan Data.....                             | 91  |
| 4.1.1. Peninjauan Dokumen.....                         | 91  |
| 4.1.2. Wawancara.....                                  | 91  |
| 4.1.3. Observasi.....                                  | 92  |
| 4.2. Penetapan Konteks.....                            | 93  |
| 4.2.1. Pengaturan Kriteria Resiko.....                 | 93  |
| 4.2.2. Pengaturan Kriteria Dampak dan Kemungkinan..... | 94  |
| 4.2.3. Pendefinisian Ruang Lingkup dan Batasan.....    | 95  |
| 4.2.4. Penetapan Peran dan Tanggung Jawab.....         | 101 |
| 4.3. Pengusulan Kebijakan SMKI.....                    | 103 |
| 4.4. Pelaksanaan Analisis Kesenjangan (Sebelum).....   | 104 |
| 4.5. Penilaian Resiko.....                             | 106 |

|                                                       |     |
|-------------------------------------------------------|-----|
| 4.5.1. Identifikasi Resiko.....                       | 106 |
| 4.5.2. Analisis Resiko.....                           | 112 |
| 4.5.3. Evaluasi Resiko.....                           | 115 |
| 4.6. Perencanaan Penanganan Resiko.....               | 117 |
| 4.6.1. Pemilihan Penanganan Resiko.....               | 117 |
| 4.6.2. Penetapan Kontrol Keamanan dan Sasarannya..... | 118 |
| 4.7. Pelaksanaan Analisis Kesenjangan (Sesudah).....  | 124 |
| 4.8. Perancangan Dokumen SMKI.....                    | 127 |
| BAB V KESIMPULAN DAN SARAN                            |     |
| 5.1. Kesimpulan.....                                  | 129 |
| 5.2. Saran.....                                       | 131 |
| GLOSARIUM.....                                        | 133 |
| DAFTAR PUSTAKA.....                                   | 147 |
| LAMPIRAN-LAMPIRAN.....                                | 157 |

## DAFTAR GAMBAR

|             |                                                                                       |     |
|-------------|---------------------------------------------------------------------------------------|-----|
| Gambar 1.1  | Total Kerentanan dan Ancaman Tahunan.....                                             | 2   |
| Gambar 1.2  | Beberapa Ancaman yang Sering Terjadi di Organisasi.....                               | 3   |
| Gambar 1.3  | Alasan Mengapa Keamanan Informasi di Organisasi dapat Ditembus.....                   | 4   |
| Gambar 2.1  | Struktur Organisasi DPTSI-ITS.....                                                    | 12  |
| Gambar 2.2  | Aspek Keamanan Informasi.....                                                         | 15  |
| Gambar 2.3  | Perkembangan SNI ISO/IEC 27001.....                                                   | 20  |
| Gambar 2.4  | Model Proses <i>PDCA</i> dalam SMKI.....                                              | 21  |
| Gambar 2.5  | Hubungan Antar Standar Keluarga SMKI.....                                             | 28  |
| Gambar 2.6  | Struktur Tim Pengelola SMKI.....                                                      | 32  |
| Gambar 2.7  | Struktur Dokumen SMKI.....                                                            | 39  |
| Gambar 2.8  | Perkembangan SNI ISO/IEC 27005.....                                                   | 46  |
| Gambar 2.9  | Hubungan Resiko dengan Entitas Lainnya dalam Manajemen Resiko Keamanan Informasi..... | 47  |
| Gambar 2.10 | Proses Manajemen Resiko Keamanan Informasi Berdasarkan SNI ISO/IEC 27005:2013.....    | 48  |
| Gambar 3.1  | Alur Tahapan Penelitian.....                                                          | 69  |
| Gambar 4.1  | Halaman <i>Login</i> untuk Layanan <i>Email</i> Mandiri .....                         | 97  |
| Gambar 4.2  | Halaman Awal untuk Layanan <i>Email</i> Mandiri .....                                 | 98  |
| Gambar 4.3  | Halaman Buka <i>Email</i> untuk Layanan <i>Email</i> Mandiri .....                    | 98  |
| Gambar 4.4  | Topologi Jaringan ITS.....                                                            | 100 |
| Gambar 4.5  | Tim Pengelola SMKI .....                                                              | 102 |

|             |                                                                             |     |
|-------------|-----------------------------------------------------------------------------|-----|
| Gambar 4.6  | Persentasi Jumlah Tingkat Kesenjangan (Sebelum)...                          | 106 |
| Gambar 4.7  | Persentasi Jumlah Aset Berdasarkan Tipe Aset .....                          | 107 |
| Gambar 4.8  | Persentasi Jumlah Aset Berdasarkan Pemilik Resiko .....                     | 108 |
| Gambar 4.9  | Ancaman Terbanyak pada Aset .....                                           | 109 |
| Gambar 4.10 | Persentasi Jumlah Ancaman Berdasarkan Sumber Ancamannya ....                | 110 |
| Gambar 4.11 | Persentasi Jumlah Kelompok Kontrol Keamanan Berdasarkan Ketiga Area .....   | 111 |
| Gambar 4.12 | Persentasi Jumlah Resiko Berdasarkan Pemilik Resiko .....                   | 115 |
| Gambar 4.13 | Persentasi Jumlah Pengelompokkan Level Resiko .....                         | 116 |
| Gambar 4.14 | Persentasi Jumlah Pemilihan Penanganan Resiko .....                         | 118 |
| Gambar 4.15 | Persentasi Jumlah Tingkat Kesenjangan (Sesudah).....                        | 126 |
| Gambar 4.16 | Perbandingan Persentasi Jumlah Tingkat Kesenjangan Sebelum dan Sesudah..... | 127 |

## DAFTAR TABEL

|            |                                                                                    |    |
|------------|------------------------------------------------------------------------------------|----|
| Tabel 2.1  | Daftar Fakultas dan Departemen di ITS.....                                         | 9  |
| Tabel 2.2  | Kegiatan pada Proses <i>PDCA</i> .....                                             | 22 |
| Tabel 2.3  | Klausul pada SNI ISO/IEC 27001:2013 Berdasarkan Proses <i>PDCA</i>                 | 23 |
| Tabel 2.4  | Domain dan Sasaran Kontrol Keamanan pada <i>Annex A</i> .....                      | 24 |
| Tabel 2.5  | Contoh Sasaran Keamanan Informasi.....                                             | 38 |
| Tabel 2.6  | Daftar Dokumen <i>Mandatory</i> .....                                              | 41 |
| Tabel 2.7  | Pemetaan Proses <i>PDCA</i> dengan Proses Manajemen Resiko Keamanan Informasi..... | 49 |
| Tabel 2.8  | Contoh Kriteria Resiko.....                                                        | 49 |
| Tabel 2.9  | Peran dan Tanggung Jawab dalam Manajemen Resiko Keamanan Informasi.....            | 49 |
| Tabel 2.10 | Perbandingan Aset Informasi dengan Aset Nyata.....                                 | 52 |
| Tabel 2.11 | Katalog Aset.....                                                                  | 53 |
| Tabel 2.12 | Katalog Ancaman.....                                                               | 54 |
| Tabel 2.13 | Contoh Kontrol Keamanan pada Ketiga Area.....                                      | 55 |
| Tabel 2.14 | Contoh Skala Nilai Dampak.....                                                     | 59 |
| Tabel 2.15 | Contoh Skala Nilai Kemungkinan.....                                                | 60 |
| Tabel 2.16 | Lembar Kerja Penilaian Resiko.....                                                 | 61 |
| Tabel 3.1  | Contoh Topik Pertanyaan Analisa Kesenjangan dari <i>Annex A</i> .....              | 73 |
| Tabel 3.2  | Klasifikasi Tingkat Kepatuhan terhadap SNI ISO/IEC 27001.....                      | 74 |
| Tabel 3.3  | Contoh Daftar Inventaris Aset.....                                                 | 76 |



|            |                                                                                         |     |
|------------|-----------------------------------------------------------------------------------------|-----|
| Tabel 3.4  | Contoh Daftar Ancaman.....                                                              | 77  |
| Tabel 3.5  | Contoh Daftar Kelompok Kontrol Keamanan Saat Ini.....                                   | 78  |
| Tabel 3.6  | Contoh Daftar Kerentanan.....                                                           | 79  |
| Tabel 3.7  | Contoh Lembar Kerja Penilaian Resiko.....                                               | 82  |
| Tabel 3.8  | Contoh Evaluasi Resiko.....                                                             | 83  |
| Tabel 3.9  | Contoh Pemilihan Penanganan Resiko.....                                                 | 84  |
| Tabel 3.10 | Contoh Penetapan Kontrol Keamanan dan Sasaran Keamanan Informasi.....                   | 85  |
| Tabel 3.11 | Hubungan Kelompok Resiko dengan Domain Kontrol Keamanan SNI ISO/IEC 27001.....          | 88  |
| Tabel 3.12 | Rencana dan Jadwal Kerja Penelitian.....                                                | 89  |
| Tabel 4.1  | Kriteria Resiko .....                                                                   | 94  |
| Tabel 4.2  | Skala Nilai Dampak .....                                                                | 94  |
| Tabel 4.3  | Skala Nilai Kemungkinan .....                                                           | 95  |
| Tabel 4.4  | Spesifikasi dan Konfigurasi <i>Server</i> untuk Webmail ITS .....                       | 96  |
| Tabel 4.5  | Hasil Analisa Kesenjangan (Sebelum) .....                                               | 105 |
| Tabel 4.6  | Sebagian Kelompok Resiko yang Tidak Diterima .....                                      | 117 |
| Tabel 4.7  | Beberapa Hubungan Kelompok Resiko dengan Domain Kontrol Keamanan SNI ISO/IEC 27001..... | 119 |
| Tabel 4.8  | Penetapan Kontrol Keamanan dan Sasaran Keamanan Informasi ....                          | 120 |
| Tabel 4.9  | Hasil Analisa Kesenjangan (Sesudah).....                                                | 125 |

## DAFTAR LAMPIRAN

|            |                                                        |        |
|------------|--------------------------------------------------------|--------|
| Lampiran A | Daftar Wawancara.....                                  | L- 1   |
| Lampiran B | Contoh Kebijakan Keamanan TIK.....                     | L-3    |
| Lampiran C | Hasil Wawancara.....                                   | L-5    |
| Lampiran D | Analisis Kesenjangan (Sebelum).....                    | L- 77  |
| Lampiran E | Analisis Kesenjangan (Sesudah).....                    | L-177  |
| Lampiran F | Bukti Penunjang Analisis Kesenjangan.....              | L- 215 |
| Lampiran G | Ruang Lingkup Sistem Manajemen Keamanan Informasi..... | L- 285 |
| Lampiran H | Kebijakan Sistem Manajemen Keamanan Informasi.....     | L-289  |
| Lampiran I | Proses Penilaian Resiko.....                           | L- 291 |
| Lampiran J | Proses Penanganan Resiko.....                          | L-365  |
| Lampiran K | <i>Statement of Applicability</i> .....                | L- 401 |
| Lampiran L | Sasaran Keamanan Informasi.....                        | L-419  |

*Halaman ini sengaja dikosongkan*

# **BAB I**

## **PENDAHULUAN**

BAB ini membahas tentang latar belakang serta perumusan masalah yang diangkat untuk menggambarkan secara detail masalah yang hendak diteliti. Adapun tujuan yang akan dicapai serta manfaat yang akan dihasilkan pada penelitian ini akan dipaparkan setelahnya. Selain itu terdapat batasan permasalahan yang ada pada penelitian ini agar pembahasan tidak terlalu luas namun tetap berbobot.

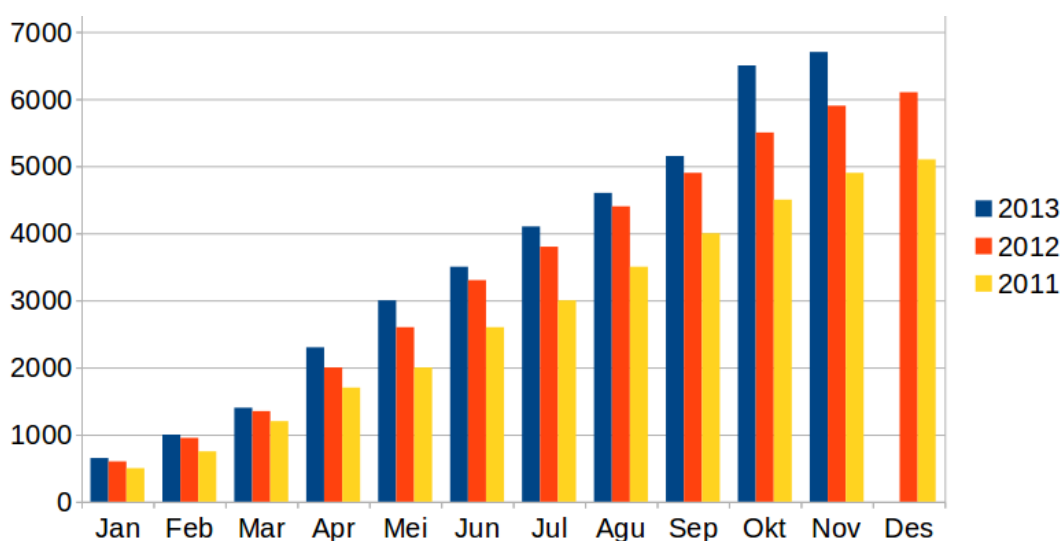
### **1.1. Latar Belakang**

Perkembangan Teknologi Informasi dan Komunikasi (TIK) yang semakin pesat yang salah satunya disebabkan karena banyaknya manfaat yang bisa didapat dalam penggunaannya. Masuknya penggunaan TIK mempengaruhi perkembangan suatu negara melalui pengembangan penyebaran pengetahuan (terutama dari negara maju ke negara berkembang) dan inovasi (Vu, 2011). Akibat manfaat tersebut serta dukungan pemerintah membuat penggunaan perangkat elektronik (komputer, laptop, *handphone*, *gadget*) serta jaringan (*internet*, *email*, media sosial) menjadi lumrah saat ini baik dilingkungan masyarakat maupun organisasi. Saat ini sudah banyak organisasi di Indonesia yang menggunakan TIK dalam menunjang aktifitas bisnisnya. Hal ini dibuktikan dalam *survey* dimana sekitar 92% organisasi menggunakan komputer dan sekitar 86% diantaranya menggunakan fasilitas *internet* (KEMENKOMINFO, 2011a). Penggunaan TIK tersebut dimanfaatkan oleh setiap organisasi untuk aktifitas pengolahan, penyimpanan maupun pertukaran informasi berharganya.

Namun pada penggunaan TIK, terdapat ancaman yang mengganggu keamanan informasi yang bersifat merusak dan merugikan selain manfaat yang didapat. Kerusakan yang terjadi tidak hanya merubah konfigurasi sistem komputer ataupun informasi yang disimpan seperti yang biasanya dialami saat terkena *virus*, akan tetapi lebih mengarah ke pelanggaran privasi dan pencurian informasi yang berorientasi profit. Berdasarkan laporan Symantec ditahun 2014, dilaporkan bahwa

terdapat 312 pelanggaran keamanan informasi yang mengakibatkan 348 juta informasi terbongkar, seperti kartu kredit, riwayat medis, data pribadi, ID *login*, dan lainnya (Symantec, 2015). Banyak metode yang dilakukan *hacker* dalam pencurian informasi, mulai dari penyebaran *malware* (*worm*, *virus*, *trojan horse* atau *spyware*), aktifitas *social engineering* (pengiriman *spam* atau pembuatan situs palsu) dan lainnya. Kebanyakan dari metode tersebut memanfaatkan media *internet* dan berbagi *file*. Di Indonesia sendiri, pernah dilaporkan bahwa Indonesia sempat menempati urutan pertama di dunia yang banyak terkena serangan *malware* selama periode 3 bulan dan urutan kesebelas penghasil *spam* (Sophos, 2013). Indonesia juga pernah mengalami kerugian akibat ancaman melalui *internet* dengan total kerugian yang bisa dihitung sekitar Rp.33,29 miliar (Tempo, 2015).

Yang patut diwaspadai dari itu semua adalah perkembangan jumlah ancaman maupun kerentanan yang terus meningkat setiap bulannya berdasarkan hasil analisa Cisco seperti yang ditampilkan pada Gambar 1.1.

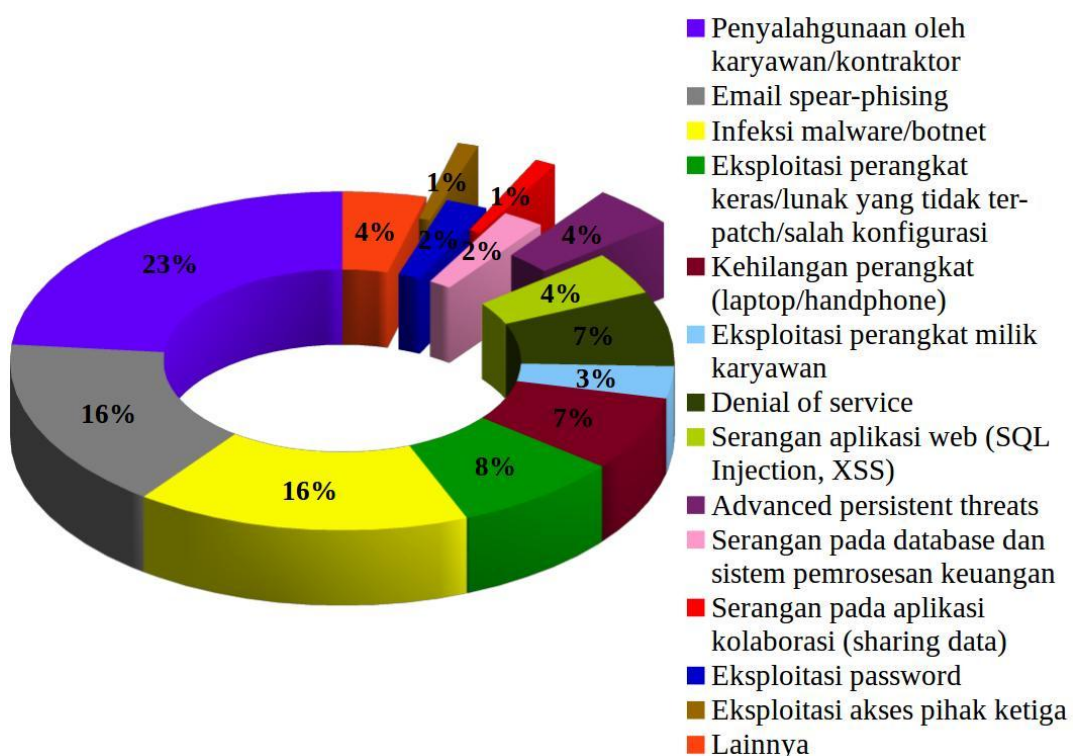


Gambar 1.1 Total Kerentanan dan Ancaman Tahunan (Cisco, 2014)

Selain dari ancaman dari luar yang pernah dialami 94% organisasi (Kaspersky, 2014), terdapat juga beberapa ancaman lain seperti ancaman dari dalam organisasi, kegagalan teknis dan bencana alam. Adapun untuk ancaman bencana alam (banjir, kebakaran, gempa bumi, gangguan hewan) maupun kegagalan teknis (kesalahan penggunaan ataupun kegagalan perangkat keras/lunak) dapat

menyebabkan hilangnya data, merusak perangkat TIK, menghambat layanan informasi ataupun mengganggu aktifitas bisnis organisasi. Hal tersebut dapat dikategorikan sebagai ancaman dalam keamanan informasi karena hilangnya aspek *availability*/ketersediaan.

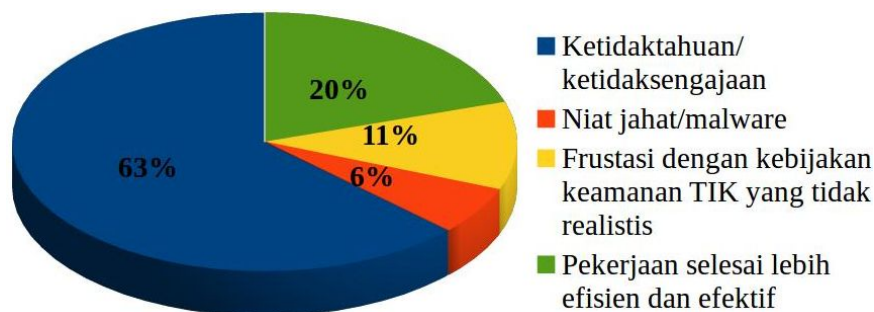
Sedangkan untuk ancaman dari dalam organisasi, biasanya dilakukan oleh orang dalam di organisasi (*insider*) baik disengaja ataupun tidak disengaja. Pengamanan dari orang dalam perlu dibangun karena mereka dapat mengakses beberapa sumber sensitif maupun bersentuhan langsung dengan perangkat TIK dan informasi tanpa bersusah payah mencari kerentanan untuk dieksploitasi seperti halnya ancaman dari luar. Ini dibuktikan dalam hasil *survey* pada Gambar 1.2 yang menyatakan beberapa ancaman yang sering terjadi di organisasi, dimana penyalahgunaan oleh karyawan atau kontraktor sangat banyak terjadi di organisasi.



Gambar 1.2 Beberapa Ancaman yang Sering Terjadi di Organisasi (Hardy, 2014)

Salah satu alasan terbesar mengapa keamanan informasi dapat ditembus berdasarkan *survey* yang ditunjukkan pada Gambar 1.3 adalah karena ketidaktahuan atau ketidaksengajaan orang dalam dengan persentase 63%, dimana hal ini dapat

membuka peluang terbukanya kerentanan tanpa disadari yang dapat dimanfaatkan oleh ancaman (bahkan 20% menyatakan sengaja dengan alasan pekerjaan malah menjadi lebih efisien dan efektif).



Gambar 1.3 Alasan Mengapa Keamanan Informasi di Organisasi dapat Ditembus (Turner, 2011)

Beberapa ancaman yang disebutkan sebelumnya merupakan resiko yang dapat mengakibatkan berbagai dampak yang merugikan bagi organisasi. Dampak yang bisa terjadi adalah kerugian finansial, terganggunya aktifitas bisnis, masalah hukum/peraturan dan penurunan reputasi organisasi (Hardy, 2014). Hal tersebut memiliki efek domino yang bisa mengancam keberlangsungan aktifitas bisnis organisasi, tak terkecuali Institut Teknologi Sepuluh Nopember (ITS). ITS merupakan perguruan tinggi negeri di Surabaya yang sudah berdiri sejak tahun 1957 dan merupakan salah satu perguruan tinggi terkemuka di Indonesia yang sudah terakreditasi A. Perguruan tinggi ini ditujukan untuk mendidik para lulusan yang unggul di bidang sains dan teknologi agar mengangkat Indonesia menjadi negara berperadaban maju dan tinggi. ITS memiliki visi yaitu menjadi perguruan tinggi dengan reputasi internasional dalam ilmu pengetahuan, teknologi, dan seni, terutama yang menunjang industri dan kelautan yang berwawasan lingkungan. Seperti halnya organisasi lainnya, ITS juga memanfaatkan berbagai fasilitas TIK dalam menjalankan aktifitas bisnisnya. Bahkan ITS memiliki perhatian lebih terhadap TIK dengan mencanangkan beberapa tujuan strategis berdasarkan laporan memorandum rektor ITS periode 2011 – 2015, seperti:

1. Setiap dosen dan karyawan memahami TIK.
2. Integrasi sistem informasi.

3. Proses administrasi *paperless*.
4. Pemanfaatan *e-learning* di seluruh jurusan.

Dalam menjalankan beberapa tujuan strategis tersebut, ITS menerapkan beragam fasilitas TIK disetiap instansi, baik berupa perangkat keras dan lunak (contohnya komputer, aplikasi perkantoran, perangkat *audio/video*, perangkat jaringan dan lainnya), maupun sistem informasi secara terpusat (contohnya SIM akademik, perpustakaan *digital*, sistem *sharing* materi akademik, SIM kepegawaian, SIM keuangan, SIM *payroll*, portal informasi dan lainnya). Sistem informasi terpusat tersebut ditujukan untuk pengintegrasian berbagai informasi yang ada kedalam satu sumber data terpadu dan mempercepat pertukaran informasi. Kesemua fasilitas TIK tersebut digunakan untuk menunjang kegiatan sehari-hari dosen, mahasiswa, karyawan dan pemangku kepentingan lainnya di ITS, seperti pengisian formulir rencana studi, penilaian mahasiswa, proses belajar-mengajar, proses administrasi, pengisian indeks kepuasan, penyebaran informasi, pembuatan laporan dan lainnya.

Dalam mengelola, mengordinasikan, mengendalikan, dan mengembangkan berbagai fasilitas TIK tersebut, terutama yang berhubungan dengan teknologi dan sistem informasi terpadu (*integrated ICT service*), ITS memiliki instansi khusus yaitu Direktorat Pengembangan Teknologi Sistem Informasi (DPTSI-ITS). Salah satu peran DPTSI-ITS juga memastikan bahwa setiap teknologi dan sistem informasi terpadu yang digunakan di lingkungan ITS beroperasi sebagaimana mestinya dan bebas dari setiap resiko. Karena apabila suatu insiden keamanan informasi terjadi, maka secara langsung ataupun tidak langsung dapat mengganggu aktifitas bisnis di ITS secara keseluruhan. Oleh karena itu kondisi yang stabil dan terjaganya aspek keamanan informasi seperti *confidentiality* (kerahasiaan), *integrity* (integritas) dan *availability* (ketersediaan) sudah menjadi harga mati bagi DPTSI-ITS demi memenuhi segala aktifitas bisnis yang ada di ITS. Apalagi sektor pendidikan/institusi menempati urutan ketiga dari sepuluh besar sektor yang mengalami insiden keamanan informasi terbanyak (Symantec, 2015).

Berdasarkan masalah keamanan informasi yang sudah dijelaskan, pihak DPTSI-ITS sudah seharusnya menggunakan standar SNI ISO/IEC 27001 sebagai acuan dalam merancang dokumen Sistem Manajemen Keamanan Informasi (SMKI).



SMKI merupakan bagian dari keseluruhan sistem manajemen organisasi untuk menetapkan, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan keamanan informasi yang dibangun dengan pendekatan resiko (KEMENKOMINFO, 2011b). Karena SMKI memerlukan pendekatan resiko, maka standar SNI ISO/IEC 27005 diperlukan sebagai acuan untuk manajemen resiko keamanan informasi. Alasan penggunaan SNI ISO/IEC 27001 dan SNI ISO/IEC 27005 karena pemerintah Indonesia melalui BSN telah menjadikan kedua standar tersebut sebagai standar SNI dalam mengelola keamanan informasi untuk semua organisasi di Indonesia. Standar SNI ISO/IEC 27001 melingkupi seluruh tipe organisasi (seperti perusahaan komersil, pemerintahan dan organisasi non-profit) dan semua ukuran dari bisnis mikro sampai multi-nasional (Itradat, 2014). Sudah banyak yang menggunakan SNI ISO/IEC 27001 diseluruh dunia dengan jumlah 23.972 organisasi, dimana sekitar 64 organisasi berasal dari Indonesia (ISO, 2014). Bahkan DPTSI juga berencana menggunakan SNI ISO/IEC 27001 dan melakukan sertifikasi oleh badan sertifikasi di tahun 2017 berdasarkan Tahapan Implementasi *Masterplan* 2013-2017.

Pemanfaatan standar SNI ISO/IEC 27001 untuk penelitian ilmiah yang bertema perancangan SMKI sudah pernah dilakukan di ITS, seperti penelitian di Biro Administrasi & Akademik Kemahasiswaan (BAAK-ITS) dengan ruang lingkup SIM Akademik (Sari, 2009). Sedangkan untuk penelitian perancangan SMKI diluar ITS pernah dilakukan di Departemen Luar Negeri RI dengan ruang lingkup infrastruktur jaringan (Ariefianto, 2006), Information Communication and E-learning Center (ICET) di Hashemite University dengan ruang lingkup Hashemite University Information System (Itradat, 2014), dan PT. Sentra Vidya Utama (Purnomo, 2016). Selain itu penelitian yang menggunakan SNI ISO/IEC 27005 untuk manajemen resiko keamanan informasi pernah dilakukan di Badan Pengkajian dan Penerapan Teknologi dengan ruang lingkup infrastruktur jaringan (Salim, 2012).

Hasil dari penelitian ini adalah rancangan tata kelola keamanan informasi berupa SMKI berdasarkan SNI ISO/IEC 27001:2013. Isi dari rancangan tata kelola keamanan informasi adalah ruang lingkup SMKI yang dapat dilihat pada Lampiran G, kebijakan SMKI yang dapat dilihat pada Lampiran H, proses penilaian resiko

yang dapat dilihat pada Lampiran I, proses penanganan resiko yang dapat dilihat pada Lampiran J, *statement of applicability* yang dapat dilihat pada Lampiran K, dan sasaran keamanan informasi yang dapat dilihat pada Lampiran L.

## **1.2. Perumusan Masalah**

Berdasarkan penjelasan singkat pada latar belakang, maka permasalahan yang akan dibahas pada penelitian ini adalah sebagai berikut:

1. Bagaimana mengidentifikasi, menganalisis dan mengevaluasi resiko yang dihadapi oleh DPTSI-ITS melalui manajemen resiko keamanan informasi berdasarkan SNI ISO/IEC 27005:2013?
2. Bagaimana rancangan tata kelola keamanan informasi di DPTSI-ITS berdasarkan SNI ISO/IEC 27001:2013?

## **1.3. Tujuan Penelitian**

Berikut ini adalah beberapa tujuan diadakannya penelitian ini berdasarkan perumusan masalah yang ada:

1. Mengidentifikasi, menganalisis dan mengevaluasi resiko yang dihadapi oleh DPTSI-ITS melalui manajemen resiko keamanan informasi berdasarkan SNI ISO/IEC 27005:2013.
2. Merancang tata kelola keamanan informasi yang berupa SMKI berdasarkan SNI ISO/IEC 27001:2013 yang dibutuhkan oleh DPTSI-ITS.

## **1.4. Manfaat Penelitian**

Manfaat yang akan didapatkan jika tujuan dari penelitian ini tercapai adalah sebagai berikut:

1. Membantu pihak DPTSI-ITS dalam mengidentifikasi, menganalisis dan mengevaluasi resiko keamanan informasi yang dihadapi.

2. Mendapat pedoman jelas dan terstruktur yang memudahkan bagi pihak DPTSI-ITS dalam mengelola keamanan informasi untuk melindungi aset berharganya.
3. Memudahkan pengambilan keputusan maupun proses pengembangan bagi pihak DPTSI-ITS yang berkaitan dengan keamanan informasi.
4. Memperbanyak referensi ilmu dibidang keamanan informasi dan keamanan TIK terutama dalam pemanfaatan SNI ISO/IEC 27001:2013 dan SNI ISO/IEC 27005:2013 bagi kalangan akademik maupun praktisi.

### **1.5. Batasan Masalah**

Beberapa batasan masalah yang akan ditetapkan pada penelitian ini adalah sebagai berikut:

1. Batasan ruang lingkup penelitian ini adalah layanan *email* (Webmail ITS) yang dikelola oleh DPTSI-ITS. Pembatasan ini dilakukan karena resiko yang harus diidentifikasi, dianalisa dan ditangani akan lebih banyak sesuai dengan banyaknya setiap aset yang dimiliki organisasi jika tidak adanya pembatasan ruang lingkup. Selain itu aktifitas pelaksanaan analisis kesenjangan dengan SNI ISO/IEC 27001:2013 akan semakin kompleks. Contohnya terdapat kontrol keamanan A.9.4.2. Prosedur *login* yang aman yang menjabarkan beberapa poin keamanan informasi dalam proses *login* yang harus ada pada setiap sistem dan aplikasi. Jika pembatasan tidak dilakukan, maka semua sistem dan aplikasi yang dikelola oleh DPTSI-ITS harus dianalisis kesenjangannya.
2. Dokumen SMKI yang dirancang hanya berada dicakupan proses *plan* dalam proses *Plan-Do-Check-Act* (PDCA).
3. Tidak merancang dokumen bukti kemampuan/kompetensi karena isinya menyangkut informasi yang bersifat rahasia seperti CV karyawan (riwayat pendidikan, pelatihan dan pengalaman).

## **BAB II**

### **KAJIAN PUSTAKA**

BAB ini membahas beberapa kajian yang mendasari penulisan penelitian ini, seperti DPTSI-ITS, keamanan informasi dalam organisasi, SNI ISO/IEC 27001 – sistem manajemen keamanan informasi (SMKI), SNI ISO/IEC 27002 – kontrol keamanan, dan SNI ISO/IEC 27005 – manajemen resiko keamanan informasi.

#### **2.1. DPTSI-ITS**

##### **2.1.1. Profil ITS**

Institut Teknologi Sepuluh Nopember (ITS) merupakan perguruan tinggi di Surabaya yang berdiri tanggal 10 November 1957 oleh Yayasan Perguruan Tinggi Teknik (YPTT) yang diketuai Dr. Angka Nitisastro. Saat itu ITS hanya memiliki 2 jurusan, yaitu Teknik Sipil dan Teknik Mesin. Pendirian ITS dipelopori oleh para pejuang kemerdekaan sejak tahun 1957, seperti Dr. Angka Nitisastro, Soedjasmono, K.H. Yahya Hasyim, dan Roeslan Abdulgani. Untuk mempertahankan sejarah pemberian nama awal, kata "Nopember" tidak diubah menjadi "November" sebagaimana dalam Kamus Besar Bahasa Indonesia. Visi awal ITS adalah mengangkat Republik Indonesia menjadi negara berperadaban maju dan tinggi melalui aktifitas mendidik para pemimpin yang unggul di bidang sains dan teknologi. ITS menempati 3 area untuk lokasi kampus, seperti Sukolilo, Manyar dan Cokroaminoto. Tabel 2.1 merupakan daftar fakultas dan jurusan yang ada di ITS.

Tabel 2.1 Daftar Fakultas dan Departemen di ITS

| <b>Fakultas</b>                   | <b>Departemen</b>                                                                         |
|-----------------------------------|-------------------------------------------------------------------------------------------|
| Fakultas Teknologi Industri (FTI) | Teknik Mesin, Teknik Fisika, Teknik Industri, Teknik Material dan Metalurgi, Teknik Kimia |
| Fakultas Teknologi Elektro (FTE)  | Teknik Elektro, Teknik Biomedik, Teknik Komputer                                          |

|                                                          |                                                                                                                                           |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Fakultas Teknologi Informasi Dan Komunikasi (FTIK)       | Informatika, Sistem Informasi, Teknologi Informasi                                                                                        |
| Fakultas Sains                                           | Fisika, Kimia, Biologi                                                                                                                    |
| Fakultas Vokasi                                          | Teknik Infrastruktur Sipil, Teknik Mesin Industri, Teknik Elektro Otomasi, Teknik Kimia Industri, Teknik Instrumentasi, Statistika Bisnis |
| Fakultas Teknologi Kelautan (FTK)                        | Teknik Perkapalan, Teknik Sistem Perkapalan, Teknik Kelautan, Transportasi Laut                                                           |
| Fakultas Teknik Sipil, Lingkungan, Dan Kebumihan (FTSLK) | Teknik Sipil, Teknik Lingkungan, Teknik Geomatika, Teknik Geofisika                                                                       |
| Fakultas Arsitektur, Desain, Dan Perencanaan (FADP)      | Arsitektur, Perencanaan Wilayah dan Kota, Desain Produk Industri, Desain Interior                                                         |
| Fakultas Matematika, Komputasi, Dan Sains Data (FMKS)    | Matematika, Statistika, Aktuaria                                                                                                          |
| Fakultas Bisnis Dan Manajemen Teknologi (FBMT)           | Manajemen Bisnis, Manajemen Teknologi, Studi Pembangunan                                                                                  |

Sumber: Penelitian

### 2.1.2. Profil DPTSI-ITS

Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) bertugas untuk menyediakan dan mengelola layanan Teknologi Informasi disekitar lingkungan ITS. DPTSI-ITS berperan dalam mendukung aktifitas akademik, penelitian dan pengabdian masyarakat, serta manajerial di lingkungan ITS dalam rangka membantu ITS mencapai visi misinya. Pada awal didirikannya DPTSI-ITS ditahun 1982, DPTSI-ITS dinamakan UPT Pusat Komputer (Puskom) yang dilengkapi sistem *Honeywell Bull Mini 6* yang mendukung pemrosesan data maupun menyelesaikan persamaan matematik bagi para staf peneliti ITS untuk penelitian. Sekitar tahun 1988, Puskom mentransformasi teknologi mini komputer ke teknologi yang sedang berkembang yaitu PC. Mulai tahun 1992, Puskom dipercaya dan diberi tanggung jawab dalam memroses pengetesan data untuk mahasiswa baru pada

perguruan tinggi negeri di wilayah Indonesia Timur, dan untuk calon pegawai negeri melalui kerjasama dengan Pemkot/Pemkab di Jawa Timur.

Sejak tahun 1999, Puskom dimandatkan untuk mengelola ITS-net, yaitu jaringan untuk ITS secara keseluruhan baik *intranet* maupun *internet*. Semua data dan informasi di lingkungan ITS dapat dihubungkan secara menyeluruh dengan adanya tugas tersebut. Ditahun 2003 berdasarkan statuta saat itu, Puskom berada dibawah dan bertanggung jawab langsung kepada rektor dan dibina sehari-hari oleh Pembantu Rektor I. Puskom saat itu bertugas untuk mengumpulkan, menyimpan, memroses, dan menyajikan informasi serta memberikan layanan untuk program-program pendidikan, penelitian, dan pengabdian kepada masyarakat.

### **2.1.3. Visi, Misi & Tujuan**

Visi yang dicanangkan DPTSI-ITS yang menggambarkan tujuan kedepan instansi adalah sebagai berikut:

- “Mewujudkan ITS *Smart Campus*, ITS in one hand”.

Misi yang dilakukan DPTSI-ITS untuk mencapai gambaran kedepan/visi yang dimiliki instansi adalah sebagai berikut:

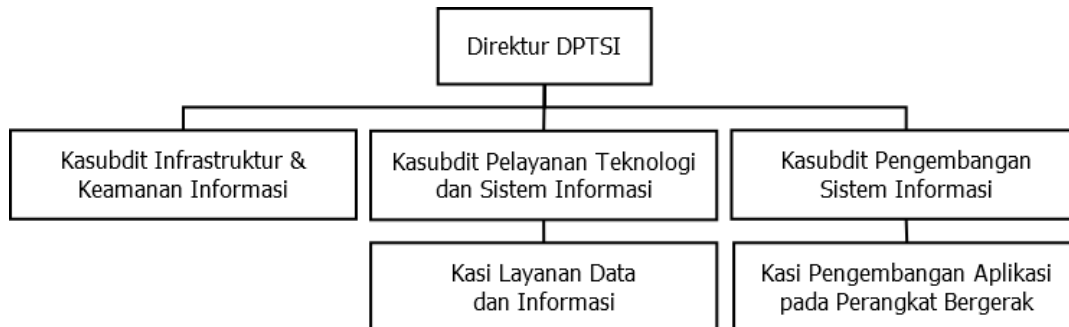
1. Menyediakan TIK beserta pendukungnya.
2. Mengembangkan infrastruktur informasi kampus.
3. Menjalinkan kerjasama dan kemitraan baik didalam maupun diluar kampus.

Tujuan yang dicanangkan DPTSI-ITS agar mencapai berbagai misi yang dimiliki instansi adalah sebagai berikut:

1. Meningkatkan sumber daya manusia yang profesional.
2. Meningkatkan aksesibilitas informasi.
3. Meningkatkan proses efisiensi.
4. Menyediakan pelayanan dan dukungan.
5. Mengikuti dan mengembangkan teknologi informasi.

#### 2.1.4. Struktur Organisasi

Struktur organisasi yang menggambarkan beberapa peran yang ada di DPTSI-ITS dapat dilihat pada Gambar 2.1.



Gambar 2.1 Struktur Organisasi DPTSI-ITS (Penelitian)

#### 2.1.5. Proses Bisnis

DPTSI-ITS bertugas melaksanakan, mengkoordinasi, memonitor dan mengevaluasi kegiatan penelitian dan pengembangan teknologi dan sistem informasi. Dalam melaksanakan tugasnya, DPTSI-ITS menyelenggarakan fungsi sebagai berikut:

1. Penyusunan rencana, program dan anggaran, serta pelaksanaan urusan administrasi instansi.
2. Pelaksanaan penelitian dan pengembangan teknologi dan sistem informasi.
3. Pelaksanaan penjamin keamanan sistem informasi.
4. Pelaksanaan peningkatan kemampuan dan kompetensi tenaga kependidikan di bidang teknologi dan sistem informasi.
5. Pengelolaan sistem informasi berbasis *web*.
6. Penyediaan layanan jasa dibidang teknologi dan sistem informasi.
7. Pelaksanaan koordinasi dan kerjasama antar institusi berbasis teknologi dan sistem informasi.
8. Pengawasan dan evaluasi pengembangan teknologi dan sistem informasi.

DPTSI-ITS terdiri atas 3 bagian, yaitu Subdirektorat Infrastruktur dan Keamanan Teknologi Informasi (Subdit Infrastruktur), Subdirektorat Pengembangan Sistem Informasi (Subdit Pengembangan) yang dibantu Seksi Pengembangan Aplikasi pada Perangkat Bergerak, dan Subdirektorat Layanan Teknologi dan Sistem Informasi (Subdit Layanan) yang dibantu Seksi Layanan Data dan Informasi. Berdasarkan Peraturan Rektor nomor 10 tahun 2016 tentang Institut Teknologi Sepuluh Nopember, berikut ini merupakan beberapa fungsi yang ada pada setiap subdirektorat dan seksi:

**A. Subdirektorat Infrastruktur & Keamanan Informasi**

1. Penyiapan bahan perumusan kebijakan dan standar mutu pengembangan infrastruktur dan keamanan TIK.
2. Pelaksanaan pengembangan infrastruktur dan keamanan TIK.
3. Pelaksanaan pengawasan dan pemantauan pengembangan infrastruktur dan keamanan TIK.
4. Pelaksanaan pemeliharaan infrastruktur dan keamanan TIK.
5. Pelaksanaan evaluasi dan pelaporan infrastruktur dan keamanan TIK.

**B. Subdirektorat Pelayanan Teknologi dan Sistem Informasi**

1. Penyiapan bahan perumusan kebijakan dan standar mutu layanan TIK.
2. Pelaksanaan operasional layanan TIK.
3. Pelaksanaan pengawasan dan pemantauan layanan TIK.
4. Pelaksanaan evaluasi dan pelaporan layanan TIK.

**C. Seksi Layanan Data dan Informasi**

1. Penyusunan bahan perumusan kebijakan untuk layanan data dan informasi.
2. Penyiapan dan pengorganisasian data untuk layanan data dan informasi.
3. Pengawasan dan pengendalian untuk layanan data dan informasi.



4. Evaluasi dan pelaporan untuk layanan data dan informasi.

#### **D. Subdirektorat Pengembangan Sistem Informasi**

1. Penyiapan bahan perumusan kebijakan dan standar mutu pengembangan sistem informasi.
2. Pelaksanaan pengembangan sistem informasi.
3. Pelaksanaan pengawasan dan pemantauan pengembangan sistem informasi.
4. Pelaksanaan pemeliharaan data dan sistem informasi.
5. Pelaksanaan evaluasi dan pelaporan pengembangan sistem informasi.

#### **E. Seksi Pengembangan Aplikasi pada Perangkat Bergerak**

1. Penyusunan bahan perumusan kebijakan untuk pengembangan aplikasi pada perangkat *mobile*.
2. Pelaksanaan pengembangan aplikasi pada perangkat *mobile*.
3. Pengawasan dan pengendalian untuk pengembangan aplikasi pada perangkat *mobile*.
4. Evaluasi dan pelaporan untuk pengembangan aplikasi pada perangkat *mobile*.

## **2.2. Keamanan Informasi dalam Organisasi**

### **2.2.1. Informasi**

Informasi adalah sekumpulan fakta dari hasil pemrosesan, manipulasi dan pengaturan data (UN-APCICT, 2009). Informasi hadir dalam berbagai macam bentuk, seperti (Kamat, 2012):

1. Dicitak atau tertulis pada kertas.
2. Disimpan secara elektronik.
3. Disebar melalui metode *post* maupun cara elektronik lainnya.
4. *Visual*, seperti video atau sketsa.

5. *Verbal*, seperti percakapan atau panggilan telepon.
6. *Intangible*/tak terlihat, seperti pengetahuan, pengalaman, keahlian atau ide.

Informasi itu sendiri diartikan sebagai sebuah aset yang memiliki nilai dan karenanya harus dilindungi (UN-APCICT, 2009). Sangat pentingnya nilai sebuah informasi menyebabkan seringkali hanya orang-orang tertentu saja yang dapat mengakses informasi, karena jika informasi tersebut jatuh ke tangan yang tidak seharusnya mendapatkan informasi tersebut (misalnya pihak pesaing bisnis yang mendapatkan informasi pengembangan produk) maka dapat menimbulkan kerugian bagi pemilik informasi (Sarno, 2009).

### 2.2.2. Keamanan Informasi

Keamanan informasi adalah menjaga informasi dari seluruh ancaman yang mungkin terjadi dalam upaya menjamin/memastikan keberlangsungan bisnis, meminimasi resiko bisnis, dan mempercepat/memaksimalkan pengembalian investasi dan peluang bisnis (Sarno, 2009). Keamanan informasi memiliki tiga aspek utama seperti yang digambarkan pada Gambar 2.2.



Gambar 2.2 Aspek Keamanan Informasi (Sarno, 2009)

Berikut ini adalah beberapa pengertian dari ketiga aspek keamanan informasi berdasarkan Gambar 2.1 (BSN, 2014a):

1. *Confidentiality* (kerahasiaan) yaitu bersifat tidak dibuat tersedia atau tertutup kepada pihak, entitas, atau proses yang tidak berwenang.
2. *Integrity* (integritas) yaitu bersifat tidak dapat dimodifikasi atau dihapus tanpa izin dan tanpa diketahui.

3. *Availability* (ketersediaan) yaitu bersifat dapat diperoleh/diterima dan dapat dipakai saat dibutuhkan oleh yang berwenang.

Selain ketiga aspek keamanan informasi utama, terdapat aspek lain yang berhubungan dengan keamanan informasi, yaitu:

1. *Authenticity* (keaslian) yaitu sifat untuk menjadi asli serta menjadi dapat dibuktikan/verifikasi dan dipercaya (Kissel, 2013).
2. *Accountability* (dapat dipertanggung jawabkan) yaitu tujuan keamanan yang menghasilkan kebutuhan bagi tindakan dari entitas agar dapat dilacak secara unik (Kissel, 2013).
3. *Non-repudiation* (tak dapat disangkal) yaitu pengamanan terhadap penolakan palsu oleh individu yang melakukan tindakan tertentu (Kissel, 2013).
4. *Reliability* (dapat dipercaya) yaitu bersifat konsisten pada perilaku dan hasilnya (BSN, 2014a).

Keamanan informasi bisa didapat melalui penerapan kumpulan kontrol keamanan yang tepat, termasuk kebijakan, proses, prosedur, struktur organisasi, serta fungsi perangkat lunak dan perangkat keras (BSN, 2014b).

### **2.2.3. Prinsip Keamanan Informasi**

Keamanan informasi memiliki beberapa prinsip yang berasal dari berbagai sudut pandang. Berikut ini adalah beberapa prinsip keamanan informasi tersebut (GHKSAR, 2012a):

1. Sasaran keamanan informasi

Sasaran/tujuan keamanan informasi dideskripsikan kedalam tiga aspek seperti *confidentiality*, *integrity* dan *availability*. Kebijakan dan kontrol keamanan dibangun dan diterapkan berdasarkan sasaran tersebut. Contohnya hanya pengguna yang diizinkan saja pada sistem informasi yang dibolehkan mengetahui, mengakses, merubah atau menghapus informasi yang disimpan atau diproses oleh sistem informasi.

2. *Preventive, detective, response dan recovery*

Keamanan informasi merupakan kombinasi dari kontrol keamanan *preventive, detective, response* dan *recovery*. *Preventive* untuk mencegah atau menghalangi terjadinya kejadian yang tidak diharapkan. *Detective* untuk mengidentifikasi terjadinya kejadian yang tidak diharapkan. *Response* untuk mengkoordinasikan balasan untuk sesuatu yang mengandung kerusakan ketika kejadian yang tidak diinginkan terjadi. *Recovery* untuk memperbaiki *confidentiality, integrity* dan *availability* dari sistem informasi menuju keadaan yang diharapkan.

3. Perlindungan dari informasi ketika sedang diproses, dikirim dan disimpan

Kontrol keamanan harus dipertimbangkan dan diterapkan secara tepat untuk memelihara *confidentiality, integrity* dan *availability* dari informasi ketika sedang diproses, dikirim dan disimpan. Contohnya jaringan *wireless* tanpa perlindungan memiliki kerentanan untuk diserang, dimana kontrol keamanan harus diadopsi ketika mengirim informasi rahasia.

4. Sistem eksternal diasumsikan tidaklah aman

Umumnya sistem eksternal atau sesuatu hal yang tidak dibawah kontrol harus dipertimbangkan tidaklah aman. Tambahan kontrol keamanan dibutuhkan ketika aset informasi atau sistem informasi berada dilokasi atau berhubungan dengan sistem eksternal. Infrastruktur sistem informasi dapat dipisah secara fisik atau logis untuk memisahkan lingkungan dengan level resiko yang berbeda.

5. Keuletan dari sistem informasi kritis

Setiap sistem informasi kritis harus ulet untuk menghadapi gangguan besar dengan kontrol keamanan yang ada. Keuletan merujuk kepada kemampuan sistem informasi untuk beroperasi dibawah kondisi merugikan atau tertekan, bahkan jika dalam kondisi melemah dan menurun ketika dipelihara/*maintenance*.

#### 6. *Auditability* dan *accountability*

*Auditability* merujuk kepada kemampuan untuk memeriksa aktifitas dalam sistem informasi, dimana bukti yang digunakan untuk verifikasi didapat dari audit *trail*, *log*/catatan sistem, *alarm* atau notifikasi lainnya. Fungsinya adalah membantu merekonstruksi sejarah kejadian sehari-hari secara lengkap dari sistem, karena itulah *auditability* berguna untuk menemukan dan menginvestigasi suatu sistem pada waktu insiden keamanan informasi.

*Accountability* merujuk kepada kemampuan untuk mengaudit tindakan dari semua pemangku kepentingan dan proses yang berinteraksi dengan sistem informasi. Peran dan tanggung jawab harus didefinisikan, diidentifikasi dan diberi kuasa pada tingkatan yang sepadan dengan kesensitifan dari informasi.

#### 2.2.4. Standar untuk Tata Kelola Keamanan Informasi

Untuk menjaga aspek keamanan informasi, terdapat beberapa standar yang dapat digunakan oleh organisasi. Standar untuk tata kelola keamanan informasi menentukan parameter untuk kebijakan dan memastikan bahwa kebijakan tersebut mempertimbangkan sumber daya TIK (orang, dokumen informasi, perangkat keras, perangkat lunak, layanan), mencerminkan hukum dan peraturan internasional, dan memenuhi prinsip *confidentiality*, *integrity*, *availability*, *accountability* dan jaminan dari informasi (UN-APCICT, 2009). Tata kelola keamanan informasi memiliki beberapa prinsip, seperti menyusun kebijakan organisasi untuk keamanan informasi, mengadopsi pendekatan berbasis resiko, menyusun arah untuk investasi, memastikan kesesuaian dengan persyaratan/kebutuhan, mengembangkan lingkungan keamanan yang positif dan meninjau performa yang terkait dengan hasil dari aktifitas bisnis (UCISA, 2015).

Strategi memilih standar untuk mengontrol keamanan informasi sebagai rujukan untuk memulai, menerapkan, mengukur, dan mengevaluasi rupa serta mengelola resiko keamanannya telah dilakukan beberapa organisasi untuk menghadapi tantangan dan ancaman yang meningkat pada keamanan TIK-nya

(Symantec, 2015). Berikut ini adalah beberapa standar yang dapat digunakan untuk tata kelola keamanan informasi (Komalasari, 2014):

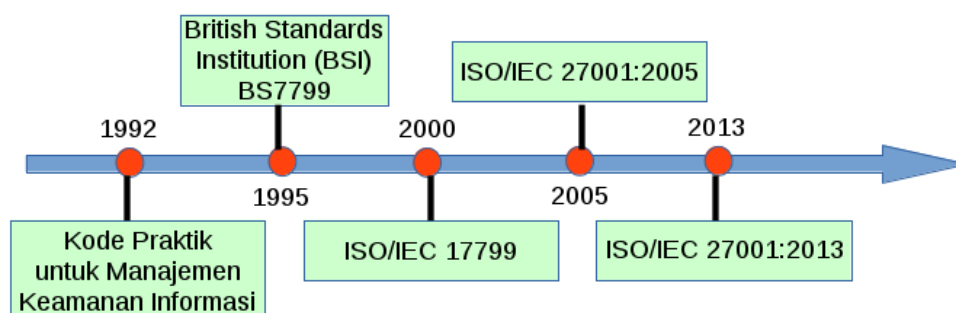
1. SNI ISO/IEC 27001 adalah standar keamanan informasi yang diterbitkan oleh ISO (*International Organization for Standardization*) dan IEC (*International Electrotechnical Commission*) yang menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa, dan memelihara serta mendokumentasikan SMKI. Versi terbaru yang dipublikasikan dari standar ini adalah SNI ISO/IEC 27001:2013.
2. PCI DSS (*The Payment Card Industry Data Security Standard*) adalah standar keamanan informasi diseluruh dunia yang ditetapkan oleh *Payment Card Industry Security Council*. PCI DSS diciptakan untuk membantu proses organisasi industri dalam pembayaran dan pencegahan penipuan kartu kredit melalui peningkatan kontrol data. Versi terbaru yang dipublikasikan dari standar ini adalah PCI DSS versi 3.0.
3. COBIT (*Control Objectives for Information and related Technology*) adalah sertifikasi yang dibuat ISACA dan IT Governance Institute. COBIT merupakan standar tata kelola TIK dan seperangkat alat yang mendukung manajer dalam menjembatani kesenjangan antara persyaratan kontrol, masalah teknis, resiko bisnis, dan masalah keamanan. Versi terbaru yang dipublikasikan dari standar ini adalah COBIT 5.
4. ITIL (*The Information Technology Infrastructure Library*) adalah seperangkat konsep dan praktek manajemen layanan TIK, pengembangan TIK dan operasi TIK yang memiliki bagian yang berfokus pada keamanan seperti *Service Support*, *Service Delivery*, *ICT Infrastructure Management*, *Security Management*, *Application Management*, *Software Aset Management*, *Plan to Implement Service Management* dan *Small-Scale Implementation*. Versi terbaru yang dipublikasikan dari standar ini adalah ITIL v3.

## 2.3. SNI ISO/IEC 27001 – Sistem Manajemen Keamanan Informasi (SMKI)

### 2.3.1. SNI ISO/IEC 27001

SNI ISO/IEC 27001 adalah standar yang digunakan untuk menspesifikasikan kebutuhan untuk membangun, menerapkan, mengawasi dan meningkatkan secara berkala pada manajemen orang, proses dan TIK disebuah organisasi baik berskala kecil, sedang maupun besar (GHKSAR, 2015). Standar ini bersifat independen terhadap produk TIK (tidak bergantung pada produk tertentu), mensyaratkan penggunaan pendekatan manajemen berbasis resiko, serta dirancang agar menjamin beberapa kontrol keamanan yang digunakan mampu melindungi aset informasi dari berbagai resiko dan memberi keyakinan keamanan bagi para pemangku kepentingan (KEMENPORA, 2012).

Kekuatan dari standar ini adalah kemampuannya untuk dapat disesuaikan keberbagai macam kebutuhan dari organisasi (Shuff, 2015). Selain itu pemenuhan persyaratan dalam SNI ISO/IEC 27001 dapat dinilai dan disertifikasi secara formal, dimana SMKI yang tersertifikasi membangun kepercayaan dalam pendekatan organisasi dalam manajemen keamanan informasi diantara para pemangku kepentingan (Carter, 2012). Perkembangan versi SNI ISO/IEC 27001 dari awal sampai yang terbaru dapat dilihat pada Gambar 2.3.



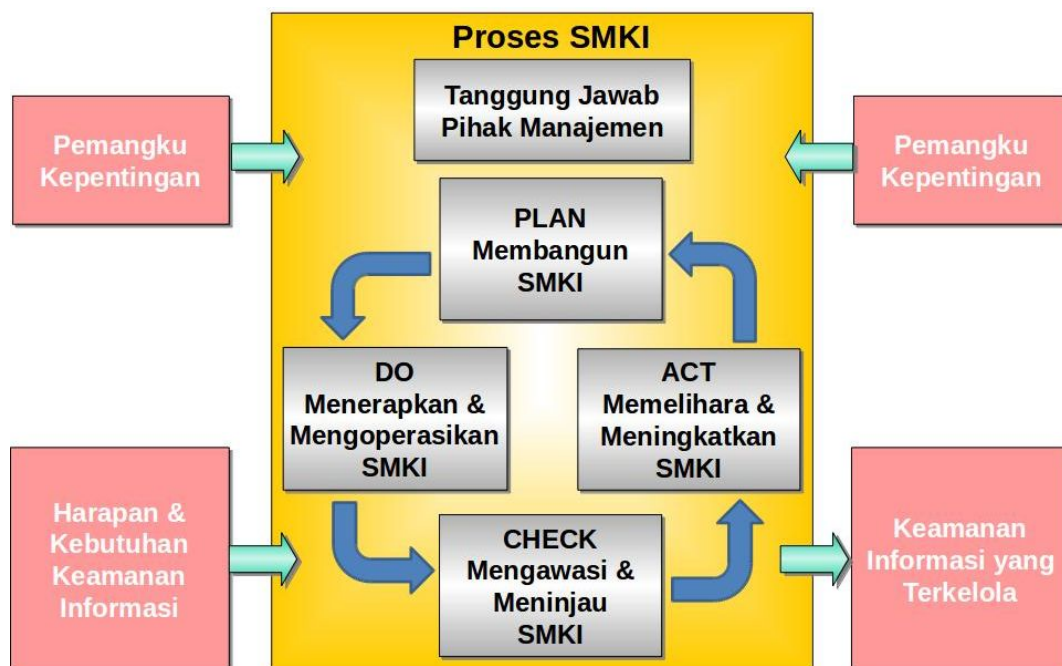
Gambar 2.3 Perkembangan SNI ISO/IEC 27001 (GHKSAR, 2015)

### 2.3.2. Sistem Manajemen Keamanan Informasi (SMKI)

SNI ISO/IEC 27001 merupakan standar internasional yang menggambarkan pembuatan dan pemeliharaan Sistem Manajemen Keamanan Informasi (SMKI)

(UCISA, 2015). SMKI itu sendiri terdiri dari tata cara, petunjuk, dan peraturan yang menghubungkan aktifitas dan sumber daya untuk diatur bersamaan oleh organisasi dalam pemenuhan pengamanan aset informasinya (BSN, 2014a). SMKI didesain untuk melindungi aset informasi dari setiap pelanggaran keamanan informasi (Itradat, 2014). Pembentukan dan penerapan SMKI organisasi dipengaruhi oleh kebutuhan dan tujuan organisasi, persyaratan keamanan, proses yang digunakan organisasi serta ukuran dan struktur dari organisasi (BSN, 2013a).

Struktur seluruh proses SMKI diatur dengan penggunaan model proses *Plan-Do-Check-Act* (PDCA) yang diadopsi oleh SNI ISO/IEC 27001:2009 (UN-APCICT, 2009). Namun pada SNI ISO/IEC 27001:2013, proses PDCA tidak ditampilkan secara jelas dalam pengenalan standar yang menyebabkan banyak yang mengira telah dihilangkan (Shuff, 2015). Proses PDCA dalam SMKI yang bisa digunakan pada SNI ISO/IEC 27001:2013 dapat dilihat pada Gambar 2.4.



Gambar 2.4 Model Proses PDCA dalam SMKI (Kamat, 2012)

Proses PDCA dilakukan secara berkelanjutan atau tidak berhenti pada suatu proses. Siklus proses PDCA yang berkelanjutan adalah salah satu kunci yang disediakan SNI ISO/IEC 27001 untuk membantu organisasi dalam memastikan



adanya adaptasi ke perubahan baru secara konstan terhadap lingkup ancaman (Honan, 2010). Rincian kegiatan yang ada didalam proses *PDCA* dapat dilihat pada Tabel 2.2.

Tabel 2.2 Kegiatan pada Proses *PDCA*

| <b><i>PDCA</i></b> | <b>Kegiatan</b>                                                                                                                                                                                                                                 |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Plan</i>        | Menetapkan kebijakan, prosedur, sasaran keamanan informasi, dan proses SMKTI yang bersangkutan untuk mengelola resiko dan meningkatkan keamanan informasi agar memberikan hasil yang sesuai dengan keseluruhan kebijakan dari sasaran tersebut. |
| <i>Do</i>          | Menerapkan dan mengoperasikan kebijakan, prosedur, kontrol keamanan, dan proses SMKTI.                                                                                                                                                          |
| <i>Check</i>       | Menilai dan mengukur kinerja proses terhadap kebijakan, sasaran keamanan informasi, praktek SMKTI dan melaporkannya ke pihak manajemen untuk ditinjau.                                                                                          |
| <i>Act</i>         | Melakukan tindakan perbaikan berdasarkan hasil audit dan tinjauan pihak manajemen atau informasi terkait lainnya agar mencapai peningkatan yang berkelanjutan.                                                                                  |

Sumber: Carter, 2012

### 2.3.3. Struktur SNI ISO/IEC 27001

Struktur standar SNI ISO/IEC 27001 terdiri dari dua bagian, yaitu klausul dan *Annex A*. Berikut ini adalah pengertian dari klausul dan *Annex A* tersebut (Sarno, 2009):

1. Klausul (*mandatory process*) merupakan persyaratan yang harus dipenuhi jika organisasi menerapkan SMKTI menggunakan standar SNI ISO/IEC 27001. Tabel 2.3 berisikan semua klausul pada SNI ISO/IEC 27001:2013 yang dikelompokkan berdasarkan proses *PDCA*.

Tabel 2.3 Klausul pada SNI ISO/IEC 27001:2013 Berdasarkan Proses *PDCA*

| <i>PDCA</i>  | Klausul                  | Sub-Klausul                                                   |
|--------------|--------------------------|---------------------------------------------------------------|
| <i>Plan</i>  | 4.<br>Konteks organisasi | 4.1.Mengerti organisasi dan konteksnya.                       |
|              |                          | 4.2.Memahami kebutuhan dan ekspektasi pemangku kepentingan.   |
|              |                          | 4.3. Menentukan ruang lingkup SMKI.                           |
|              |                          | 4.4. SMKI.                                                    |
|              | 5.<br>Kepemimpinan       | 5.1. Kepemimpinan dan komitmen.                               |
|              |                          | 5.2. Kebijakan.                                               |
|              |                          | 5.3. Tanggung jawab dan kewenangan.                           |
|              | 6.<br>Perencanaan        | 6.1.Tindakan untuk mengalamatkan resiko dan keuntungan.       |
|              |                          | 6.2.Sasaran dan rencana keamanan informasi untuk mencapainya. |
|              | 7.<br>Dukungan           | 7.1. Sumber daya.                                             |
|              |                          | 7.2. Kompetensi.                                              |
|              |                          | 7.3. Kesadaran.                                               |
|              |                          | 7.4. Komunikasi.                                              |
|              |                          | 7.5. Dokumentasi informasi.                                   |
| <i>Do</i>    | 8.<br>Operasi            | 8.1. Perencanaan dan kontrol operasional.                     |
|              |                          | 8.2. Penilaian resiko keamanan informasi.                     |
|              |                          | 8.3. Penanganan keamanan informasi.                           |
| <i>Check</i> | 9.<br>Evaluasi performa  | 9.1.Pengawasan, pengukuran, penganalisaan dan pengevaluasian. |
|              |                          | 9.2. Audit internal.                                          |
|              |                          | 9.3. Tinjauan pihak manajemen.                                |

|            |                    |                                               |
|------------|--------------------|-----------------------------------------------|
| <i>Act</i> | 10.<br>Peningkatan | 10.1. Ketidaksesuaian dan tindakan perbaikan. |
|            |                    | 10.2. Peningkatan berkelanjutan.              |

Sumber: Shuff, 2015; BSN, 2013a

2. *Annex A (security control)* merupakan dokumen referensi yang disediakan dan dapat dijadikan rujukan untuk menentukan kontrol keamanan apa yang perlu diterapkan dalam SMKI. Tabel 2.4 berisikan domain kontrol keamanan berikut sasaran kontrol keamanannya pada *Annex A* didalam SNI ISO/IEC 27001:2013.

Tabel 2.4 Domain dan Sasaran Kontrol Keamanan pada *Annex A*

| No<br><i>Annex</i> | Domain & Sasaran Kontrol Keamanan                  | Penjelasan Sasaran Kontrol Keamanan                                                                                                                    |
|--------------------|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.5                | Kebijakan keamanan informasi                       |                                                                                                                                                        |
| A.5.1              | Arahan pihak manajemen terhadap keamanan informasi | Menyediakan arahan dan dukungan manajemen terhadap keamanan informasi yang sesuai dengan kebutuhan bisnis serta hukum dan peraturan yang bersangkutan. |
| A.6                | Organisasi untuk keamanan informasi                |                                                                                                                                                        |
| A.6.1              | Organisasi internal                                | Membangun kerangka kerja manajemen untuk memulai dan mengontrol penerapan dan pengoperasian dari keamanan informasi dalam organisasi.                  |
| A.6.2              | Perangkat <i>mobile</i> dan <i>teleworking</i>     | Memastikan keamanan <i>teleworking</i> dan penggunaan perangkat <i>mobile</i> .                                                                        |
| A.7                | Keamanan sumber daya manusia                       |                                                                                                                                                        |
| A.7.1              | Sebelum perekrutan karyawan                        | Memastikan karyawan dan kontraktor mengerti tanggung jawab mereka dan sesuai atas peran yang telah mereka pertimbangkan.                               |

|        |                                           |                                                                                                                                                                  |
|--------|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.7.2  | Selama karyawan bekerja                   | Memastikan karyawan dan kontraktor sadar dan memenuhi tanggung jawab keamanan informasi mereka.                                                                  |
| A.7.3  | Pemberhentian dan penggantian karyawan    | Melindungi kepentingan organisasi sebagai bagian dari proses pergantian dan pemberhentian karyawan.                                                              |
| A.8    | Manajemen aset                            |                                                                                                                                                                  |
| A.8.1  | Tanggung jawab terhadap aset              | Mengidentifikasi aset organisasi dan mendefinisikan tanggung jawab pengamanan yang tepat.                                                                        |
| A.8.2  | Klasifikasi informasi                     | Memastikan informasi mendapatkan tingkat pengamanan yang tepat sesuai dengan kepentingannya pada organisasi.                                                     |
| A.8.3  | Penanganan media                          | Mencegah penyingkapan/penyebaran, modifikasi, pembuangan atau penghancuran informasi yang disimpan padamedia tanpa izin.                                         |
| A.9    | Kontrol akses                             |                                                                                                                                                                  |
| A.9.1  | Persyaratan bisnis terhadap kontrol akses | Membatasi akses untuk informasi dan fasilitas pemrosesan informasi.                                                                                              |
| A.9.2  | Manajemen akses pengguna                  | Memastikan keabsahan akses pengguna dan untuk mencegah akses tanpa izin ke sistem dan layanan.                                                                   |
| A.9.3  | Tanggung jawab pengguna                   | Memastikan pengguna bertanggung jawab untuk mengamankan informasi autentikasi mereka.                                                                            |
| A.9.4  | Kontrol akses sistem dan perangkat lunak  | Mencegah akses tanpa izin ke sistem dan perangkat lunak.                                                                                                         |
| A.10   | Kriptografi                               |                                                                                                                                                                  |
| A.10.1 | Kontrol kriptografi                       | Memastikan penggunaan kriptografi yang tepat dan efektif untuk melindungi <i>confidentiality</i> , <i>authenticity</i> dan/atau <i>integrity</i> dari informasi. |

|        |                                               |                                                                                                                         |
|--------|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| A.11   | Keamanan fisik dan lingkungan                 |                                                                                                                         |
| A.11.1 | Area yang aman                                | Mencegah akses, kerusakan dan gangguan fisik tanpa izin kepada informasi dan fasilitas pemrosesan informasi organisasi. |
| A.11.2 | Peralatan                                     | Mencegah kerugian, kerusakan, pencurian atau pelanggaran atas aset dan gangguan pada aktifitas organisasi.              |
| A.12   | Keamanan operasional                          |                                                                                                                         |
| A.12.1 | Tanggung jawab dan prosedur operasional       | Memastikan aktifitas pada fasilitas pemrosesan informasi benar dan aman.                                                |
| A.12.2 | Perlindungan dari <i>malware</i>              | Memastikan bahwa informasi dan fasilitas pemrosesan informasi terlindungi dari <i>malware</i> .                         |
| A.12.3 | <i>Backup</i>                                 | Melindungi dari kehilangan data.                                                                                        |
| A.12.4 | Perekaman dan pengawasan                      | Merekam kejadian dan menghasilkan bukti.                                                                                |
| A.12.5 | Kontrol perangkat lunak operasional           | Memastikan <i>integrity</i> dari sistem operasional.                                                                    |
| A.12.6 | Manajemen kerentanan teknis                   | Mencegah eksploitasi kerentanan yang bersifat teknis.                                                                   |
| A.12.7 | Pertimbangan/perhatian audit sistem informasi | Meminimalkan dampak dari aktifitas audit pada sistem operasional.                                                       |
| A.13   | Keamanan komunikasi                           |                                                                                                                         |
| A.13.1 | Manajemen keamanan jaringan                   | Memastikan perlindungan informasi pada jaringan dan fasilitas pemrosesan informasi pendukungnya.                        |
| A.13.2 | Pertukaran informasi                          | Memelihara keamanan dari informasi yang dikirim didalam organisasi dan dengan setiap entitas eksternal lainnya.         |
| A.14   | Akusisi, pengembangan dan pemeliharaan sistem |                                                                                                                         |

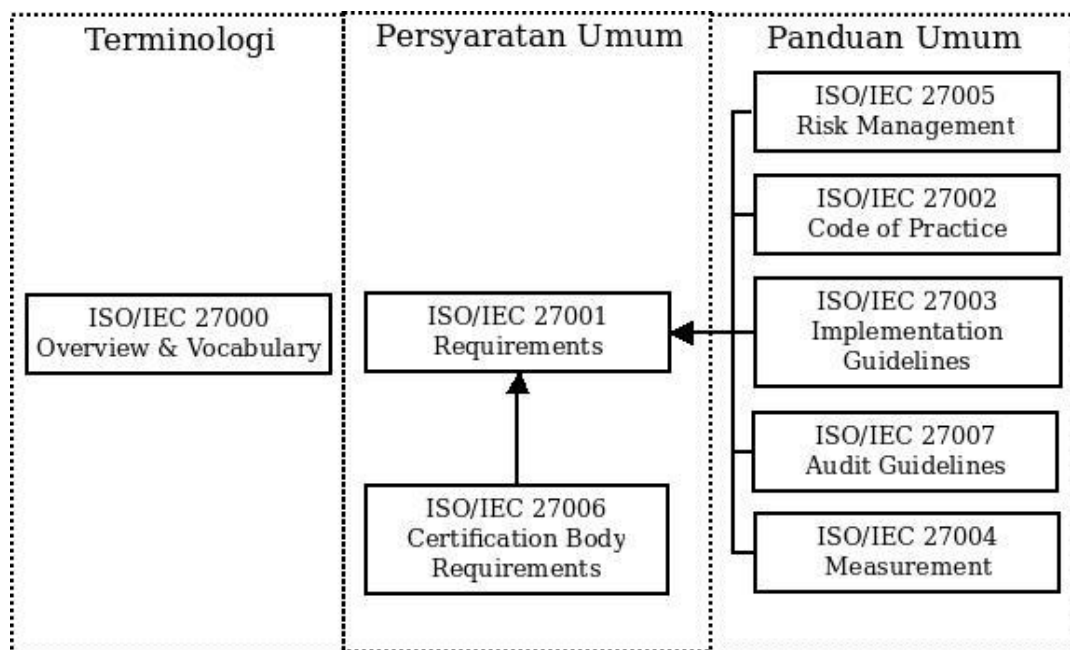
|        |                                                                 |                                                                                                                                                                                                                            |
|--------|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.14.1 | Persyaratan keamanan untuk sistem informasi                     | Memastikan bahwa keamanan informasi merupakan bagian pelengkap dari sistem informasi disemua daur hidupnya. Hal ini termasuk persyaratan untuk sistem informasi yang menyediakan beberapa layanan melalui jaringan publik. |
| A.14.2 | Keamanan dalam proses pengembangan dan <i>support</i> /dukungan | Memastikan keamanan informasi didesain dan diterapkan dalam daur hidup pengembangan sistem informasi.                                                                                                                      |
| A.14.3 | Pengujian data                                                  | Memastikan perlindungan data yang digunakan untuk pengujian.                                                                                                                                                               |
| A.15   | Relasi dengan vendor                                            |                                                                                                                                                                                                                            |
| A.15.1 | Keamanan informasi dalam hubungan dengan vendor                 | Memastikan perlindungan pada aset organisasi yang dapat diakses oleh vendor.                                                                                                                                               |
| A.15.2 | Manajemen kualitas layanan vendor                               | Memelihara tingkat keamanan informasi dan kualitas layanan yang disetujui dalam perjanjian dengan vendor.                                                                                                                  |
| A.16   | Manajemen insiden keamanan informasi                            |                                                                                                                                                                                                                            |
| A.16.1 | Manajemen dan perbaikan insiden keamanan informasi              | Memastikan pendekatan yang konsisten dan efektif untuk manajemen insiden keamanan informasi, termasuk komunikasi pada kejadian dan kelemahan keamanan.                                                                     |
| A.17   | Aspek keamanan informasi akan manajemen keberlangsungan bisnis  |                                                                                                                                                                                                                            |
| A.17.1 | Keberlangsungan keamanan informasi                              | Keberlangsungan keamanan informasi harus dimasukkan kedalam sistem manajemen keberlangsungan bisnis organisasi.                                                                                                            |
| A.17.2 | Redundansi                                                      | Memastikan <i>availability</i> dari fasilitas pemrosesan informasi.                                                                                                                                                        |
| A.18   | Kepatuhan                                                       |                                                                                                                                                                                                                            |

|        |                                              |                                                                                                                                                   |
|--------|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| A.18.1 | Kepatuhan akan persyaratan hukum dan kontrak | Mencegah pelanggaran hukum/ peraturan atau perjanjian kontrak yang berhubungan dengan keamanan informasi dan setiap persyaratan keamanan lainnya. |
| A.18.2 | Peninjauan keamanan informasi                | Memastikan keamanan informasi diterapkan dan dioperasikan sesuai dengan prosedur dan kebijakan organisasi.                                        |

Sumber: BSN, 2013a

#### 2.3.4. Keluarga SMKI

Sudah lama ISO dan IEC mengembangkan sejumlah standar tentang SMKI baik dalam bentuk persyaratan maupun panduan. Standar SMKI tersebut dikelompokkan sebagai standar keluarga SMKI atau seri SNI ISO/IEC 27000 yang dapat dilihat pada Gambar 2.5.



Gambar 2.5 Hubungan Antar Standar Keluarga SMKI (KEMENKOMINFO, 2011b)

Berikut ini adalah penjelasan dari beberapa standar keluarga SMKI berdasarkan Gambar 2.5 (BSN, 2014a):

1. SNI ISO/IEC 27000 – *Information technology – Security techniques – Information security management systems – Overview and vocabulary* adalah dokumen yang berisi tentang peninjauan standar keluarga SMKI, pengenalan SMKI, dan semua istilah serta definisi yang digunakan diseluruh standar keluarga SMKI.
2. SNI ISO/IEC 27001 – *Information technology – Security techniques – Information security management systems – Requirements* adalah dokumen yang berisi tentang spesifikasi persyaratan untuk membangun, menerapkan, mengoperasikan, mengawasi, meninjau, memelihara dan meningkatkan SMKI dalam konteks resiko bisnis keseluruhan organisasi. Tujuan SNI ISO/IEC 27001 adalah menyediakan persyaratan untuk mengembangkan dan mengoperasikan SMKI, termasuk kumpulan kontrol keamanan untuk mengontrol dan memitigasi resiko yang ada pada aset informasi yang dicoba oleh organisasi untuk diamankan melalui pengoperasian SMKI.
3. SNI ISO/IEC 27002 – *Information technology – Security techniques – Code of practice for information security controls* adalah dokumen yang berisi daftar sasaran kontrol keamanan dan praktik kontrol keamanan terbaik yang diterima secara umum, yang digunakan sebagai panduan penerapan ketika memilih dan menerapkan kontrol keamanan untuk mendapatkan keamanan informasi.
4. SNI ISO/IEC 27003 – *Information technology – Security techniques – Information security management system implementation guidance* adalah dokumen yang berisi panduan praktek penerapan dan menyediakan informasi lebih lanjut untuk membangun, menerapkan, mengoperasikan, mengawasi, meninjau, memelihara dan meningkatkan SMKI berdasarkan SNI ISO/IEC 27001. Tujuan utama dari SNI ISO/IEC 27003 adalah menyediakan pendekatan berbasis proses untuk mensukseskan penerapan SMKI berdasarkan SNI ISO/IEC 27001.



5. SNI ISO/IEC 27004 – *Information technology – Security techniques – Information security management – Measurement* adalah dokumen yang berisi petunjuk serta saran dalam pengembangan dan penggunaan suatu pengukuran/metrik saat menilai keefektifan SMKI, sasaran keamanan informasi dan kontrol keamanan yang digunakan untuk menerapkan dan mengatur keamanan informasi seperti yang dispesifikasikan dalam SNI ISO/IEC 27001.
6. SNI ISO/IEC 27005 – *Information technology – Security techniques – Information security risk management* adalah dokumen yang berisi panduan dalam penerapan proses yang berorientasikan pendekatan manajemen resiko untuk mendapatkan kepuasan dalam penerapan dan pemenuhan persyaratan manajemen resiko keamanan informasi pada SNI ISO/IEC 27001.
7. SNI ISO/IEC 27006 – *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems* adalah dokumen yang berisi spesifikasi persyaratan dan menyediakan panduan bagi badan yang menyediakan audit dan sertifikasi SMKI yang sesuai dengan SNI ISO/IEC 27001, sebagai tambahan untuk persyaratan yang tertera dalam SNI ISO/IEC 17021.
8. SNI ISO/IEC 27007 – *Information technology – Security techniques – Guidelines for information security management systems auditing* adalah dokumen yang berisi panduan untuk kebutuhan organisasi dalam mengadakan audit SMKI baik secara internal maupun eksternal atau untuk mengatur program audit SMKI terhadap beberapa persyaratan yang dispesifikasikan dalam SNI ISO/IEC 27001.

### **2.3.5. Tahapan Perancangan SMKI**

#### **2.3.5.1. Mendapatkan Persetujuan Pimpinan**

Hal pertama yang dilakukan adalah mendapatkan persetujuan dari pimpinan dalam organisasi. Pimpinan harus mendapatkan penjelasan yang memadai sebelum memulai proyek SMKI tentang seluk beluk, nilai penting dan untung rugi menerapkan SMKI serta konsekuensi ataupun komitmen yang dibutuhkan dari

pimpinan sebagai tindak lanjut persetujuan terhadap proyek SMKI (KEMENKOMINFO, 2011b). Persetujuan pimpinan penting sekali untuk memastikan komitmen berkelanjutan kearah penerapan SMKI (CSM, 2013). Persetujuan ini harus diikuti dengan arahan dan dukungan selama berlangsungnya proyek tersebut agar setiap masalah yang memerlukan pengambilan keputusan pimpinan dapat diselesaikan secara cepat dan tepat (KEMENKOMINFO, 2011b).

#### **2.3.5.2. Mendefinisikan Ruang Lingkup dan Batasan**

Setelah mendapat persetujuan dari pimpinan, selanjutnya adalah mendefinisikan ruang lingkup SMKI. Ruang lingkup dapat didefinisikan menurut istilah dari karakteristik bisnis, organisasi, lokasinya, aset informasinya dan teknologinya (Carter, 2012). Ruang lingkup dapat melingkupi sebagian atau keseluruhan organisasi (Humphreys, 2007). Berikut ini adalah contoh dari ruang lingkup SMKI (KEMENKOMINFO, 2011b):

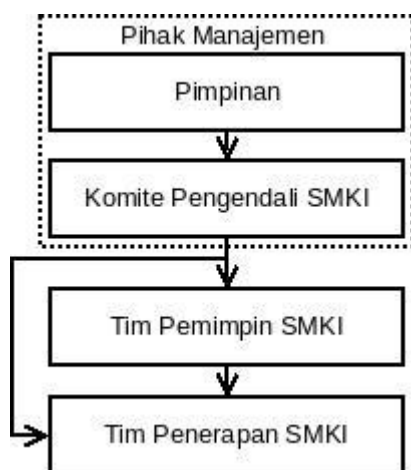
1. Kegiatan dan/atau proses, misalnya pengamanan pusat data, penyediaan layanan publik, pengembangan perangkat lunak, penggunaan jaringan dan fasilitas *email*, dan lainnya.
2. Satuan kerja, misalnya direktorat, departemen atau bidang.
3. Lokasi kerja, misalnya pusat, daerah atau kedua-duanya.

Ruang lingkup SMKI bisa didapat dari resiko yang diketahui di organisasi, contohnya resiko akses tanpa izin pada transaksi *online* di institusi keuangan yang berdampak kritis pada operasional bisnis, maka ruang lingkup organisasi tersebut dapat didefinisikan tentang layanan transaksi *online* (CSM, 2013).

#### **2.3.5.3. Menetapkan Peran dan Tanggung Jawab**

Setelah ruang lingkup SMKI sudah didefinisikan, selanjutnya adalah menetapkan tim pengelola SMKI. Hal ini dikarenakan SNI ISO/IEC 27001 membutuhkan penetapan peran dan tanggung jawab untuk membangun, menerapkan, mengoperasikan, mengawasi, meninjau, memelihara dan meningkatkan SMKI (BSN, 2013c). Maka dari itu diperlukan penetapan tim

pengelola SMKI, dimana tugas utamanya adalah menyiapkan, menjamin dan/atau melakukan seluruh kegiatan dalam tahapan penerapan SMKI agar dapat terlaksana dengan baik sesuai rencana (KEMENKOMINFO, 2011b). Struktur dari tim pengelola SMKI dapat dilihat pada Gambar 2.6.



Gambar 2.6 Struktur Tim Pengelola SMKI (CSM, 2013)

Yang perlu diperhatikan adalah struktur, sumber daya dan peran untuk keamanan informasi bisa berbeda disetiap organisasi karena ukuran, tipe dan struktur organisasi, contohnya beberapa peran di organisasi kecil dibawa oleh orang yang sama (BSN, 2013b). Berikut ini adalah perincian peran dari Gambar 2.6:

#### A. Pimpinan (*top management*)

Pimpinan adalah orang atau kelompok orang yang memimpin dan mengontrol organisasi ditingkat tertinggi organisasi (BSN, 2014a). Pimpinan bertanggung jawab terhadap visi, keputusan strategis dan mengkoordinasikan aktifitas untuk memimpin dan mengontrol organisasi (BSN, 2013b). Pimpinan dapat termasuk *Chief Executive Officer (CEO)*, *Chief Operating Officer (COO)*, *president* (ketua/direktur/rektor) atau yang serupa. Berikut ini adalah peran dan tanggung jawab pimpinan terhadap SMKI (BSN, 2013a):

1. Memastikan kebijakan dan sasaran keamanan informasi telah ditetapkan dan sesuai dengan arah strategis organisasi.

2. Memastikan integrasi persyaratan SMKI kedalam proses organisasi.
3. Memastikan tersedianya sumber daya yang dibutuhkan untuk SMKI.
4. Mengkomunikasikan pentingnya patuh terhadap persyaratan SMKI dan manajemen keamanan informasi yang efektif.
5. Mengarahkan dan mendukung pemangku kepentingan untuk berkontribusi dalam keefektifan SMKI.
6. Memastikan SMKI mencapai hasil yang diharapkan dan memajukan peningkatan berkelanjutan.
7. Mendukung peran pihak manajemen terkait lainnya untuk menunjukkan kepemimpinannya yang termasuk area tanggung jawab mereka.

#### **B. Komite pengendali SMKI (*ISMS steering committee*)**

Komite pengendali SMKI berperan memimpin SMKI dan menangani aset informasi di organisasi (BSN, 2013b). Komite ini merupakan landasan untuk mendiskusikan persoalan apapun yang berhubungan dengan SMKI dan keamanan informasi secara umum (CSM, 2013). Komite pengendali SMKI idealnya dapat terdiri dari (CSM, 2013):

- *Chairman*/ketua: bertanggung jawab untuk memastikan sasaran SMKI sejalan dengan sasaran strategis organisasi. Ketua sebaiknya ditetapkan dari jajaran manajemen atas. Contohnya jika *Chief Information Security Officer (CISO)* ditetapkan sebagai ketua, idealnya *CISO* sebaiknya berada di manajemen atas dan melaporkan secara langsung kepada *CEO* organisasi.
- *Line manager* (contohnya kepala unit organisasi): bertanggung jawab terhadap setiap unit dan operasional bisnis, serta memastikan hasil dari aktifitas penilaian resiko menyatu dalam setiap aktifitas operasional.
- Pemilik aset dan/atau proses: bertanggung jawab untuk memastikan kontrol yang tepat diterapkan dan setiap aset terlindungi.

Berikut ini contoh peran dan tanggung jawab komite pengendali SMKI terhadap SMKI (CSM, 2013):

1. Memastikan kesesuaian penerapan kebijakan dan sasaran keamanan informasi.
2. Melaksanakan tinjauan manajemen.
3. Memastikan peningkatan berkelanjutan dilakukan dengan segera tanpa penundaan.
4. Memastikan kecukupan langkah yang diambil secara teratur untuk meningkatkan keamanan informasi pada organisasi.
5. Menyediakan arahan yang jelas pada strategi SMKI organisasi dalam mengelola keamanan informasi.
6. Memperlihatkan komitmen dalam mendukung pimpinan untuk mencapai sasaran strategis organisasi.

#### **C. Tim pemimpin SMKI (*ISMS lead team*)**

Tim pemimpin SMKI sebaiknya yang memiliki pengetahuan yang dalam dan/atau berpengalaman dalam keamanan informasi, memahami SMKI secara luas baik penerapan SMKI dan pengelolaan resiko keamanan informasi (CSM, 2013). Berikut ini adalah peran dan tanggung jawab tim pemimpin SMKI (CSM, 2013):

1. Merencanakan, mengerakkan, dan mengatur aktifitas yang berhubungan dengan SMKI.
2. Mengelola resiko keamanan informasi secara berkala.
3. Mengkoordinasi aktifitas secara umum yang berhubungan dengan SMKI, komite pengendali SMKI dan program keamanan informasi lainnya dalam organisasi.

#### **D. Tim penerapan SMKI (*ISMS implementation team*)**

Tim penerapan SMKI adalah yang bertanggung jawab untuk melakukan aktifitas SMKI yang direncanakan oleh tim pemimpin SMKI (CSM, 2013). Bergantung dari ruang lingkup SMKI dan struktur organisasi, tim penerapan SMKI dapat terdiri dari karyawan dari departemen seperti (CSM, 2013):

- Pihak manajemen resiko: bertanggung jawab terhadap standar atau kerangka kerja manajemen resiko organisasi.
- Bagian *human resource*: bertanggung jawab secara keseluruhan terhadap karyawan di organisasi, termasuk persyaratan perekrutan, pemberhentian, dan pelatihan bagi karyawan.
- Bagian TIK: bertanggung jawab terhadap keamanan sistem TIK organisasi dan seluruh sumber daya TIK yang dibutuhkan untuk penerapan SMKI.
- Bagian keuangan dan akuntansi: bertanggung jawab terhadap manajemen anggaran belanja secara keseluruhan dalam penerapan SMKI.
- Bagian administrasi bangunan dan fasilitas: bertanggung jawab terhadap keamanan fisik dan administrasi umum tempat fisik organisasi.
- Auditor: bertanggung jawab dalam pelaksanaan audit SMKI. Pemimpin tim auditor yang bertanggung jawab dalam perencanaan program audit SMKI.

Tim penerapan SMKI bertanggung jawab dalam menerapkan kebijakan dan prosedur (termasuk kontrol keamanan) secara sesuai, serta melaporkan dan mengatasi setiap insiden keamanan informasi dengan segera (CSM, 2013).

#### **2.3.5.4. Mendefinisikan Kebijakan SMKI**

Setelah menetapkan tim pengelola SMKI, selanjutnya adalah mendefinisikan kebijakan SMKI. SNI ISO/IEC 27001 mengharuskan organisasi untuk memiliki kebijakan SMKI selain kebijakan tentang keamanan informasi (BSN, 2013b). Berdasarkan standar SNI ISO/IEC 27003, kebijakan SMKI maupun kebijakan dapat memiliki struktur/*template* sebagai berikut (BSN, 2013b):

- Pendahuluan: berisi penjelasan singkat terkait topik dari kebijakan yang dibuat.
- Ruang lingkup: mendeskripsikan bagian atau aktivitas dari organisasi yang dipengaruhi oleh kebijakan yang dibuat.
- Sasaran: mendeskripsikan maksud dari kebijakan yang dibuat.

- Hasil yang diharapkan: mendeskripsikan hasil yang akan diperoleh organisasi ketika sasaran kebijakan tercapai.
- Prinsip keamanan informasi: mendeskripsikan beberapa peraturan mengenai tindakan dan keputusan untuk mencapai sasaran.
- Tanggung jawab: mendeskripsikan siapa saja yang bertanggung jawab terhadap tindakan untuk memenuhi persyaratan kebijakan yang dibuat.
- Kebijakan terkait: mendeskripsikan kebijakan lainnya yang terkait untuk mencapai sasaran dari kebijakan yang dibuat.

#### **2.3.5.5. Melakukan Analisis Kesenjangan**

Setelah mendefinisikan kebijakan SMKI, selanjutnya adalah melakukan analisis kesenjangan. Analisis kesenjangan merupakan perangkat atau teknik yang memungkinkan organisasi membandingkan hasil sebenarnya dengan standar (Candiwan, 2014). Dengan analisis kesenjangan, pihak manajemen dapat mengidentifikasi kondisi organisasi saat ini, kondisi organisasi lain saat ini untuk perbandingan, kondisi yang diinginkan organisasi, dan pertumbuhan yang diinginkan antara *as-is* dan *to-be* (Komalasari, 2014). Berikut ini adalah tujuan dari analisis kesenjangan (CSM, 2013):

1. Menilai tingkat kesiapan untuk menerapkan SMKI.
2. Mengurangi kemiripan dan/atau konflik setiap tugas.
3. Memperkirakan waktu dan sumberdaya yang diperlukan untuk penerapan SMKI.

Dalam analisis kesenjangan, perlunya pengidentifikasian apakah kebijakan dan prosedur sebagaimana dicantumkan telah terpenuhi untuk menilai pada aspek kerangka kerja, selain itu perlunya pemeriksaan ketersediaan rekaman sebagai bukti-bukti penerapan untuk menilai pada aspek penerapan (KEMENPORA, 2012).

#### 2.3.5.6. Melakukan Penilaian dan Perencanaan Penanganan Resiko

Setelah kebijakan SMKI sudah didefinisikan, selanjutnya adalah melakukan penilaian resiko dan perencanaan penanganan resiko. Hal pertama yang dilakukan adalah memeriksa apakah organisasi telah memiliki atau menetapkan kebijakan/metodologi penilaian resiko, jika belum maka penyusunan metodologinya dilakukan dengan merujuk pada standar yang ada, misalnya AS/NZS 4360, SNI ISO/IEC 27005, NIST SP800-30 (KEMENKOMINFO, 2011b). Penilaian resiko merupakan aktifitas untuk mengidentifikasi tingkatan keamanan informasi saat ini, contohnya prosedur saat ini untuk menangani perlindungan informasi (BSN, 2013b). Aktifitas ini juga dilakukan untuk menyediakan evaluasi ancaman dimasa depan dan meredakan resiko ke level yang dapat diterima oleh organisasi (Gordas, 2014). Bergantung dari tujuan dan ruang lingkup, penilaian resiko dapat dikategorikan menjadi tiga tipe, seperti (GHKSAR, 2012b):

1. *High-level assessment* (penilaian tingkat tinggi) yang menekankan pada analisa rupa keamanan organisasi, seperti keseluruhan infrastruktur atau desain dari sistem.
2. *Comprehensive assessment* (penilaian secara luas) yang dilakukan secara berkala untuk menjamin keamanan seluruh sistem informasi atau sistem informasi yang dipilih pada organisasi.
3. *Pre-production assessment* (penilaian sebelum produksi) yang dilakukan pada sistem informasi baru sebelum dijalankan atau setelah adanya perubahan fungsional besar-besaran.

Sedangkan pengertian penanganan resiko adalah proses untuk memilih dan menerapkan tindakan untuk mengurangi resiko (CSM, 2013). Penanganan resiko dapat melibatkan aktifitas seperti menghindari resiko melalui tidak memulai atau melanjutkan aktifitas yang meningkatkan resiko, memindahkan sumber resiko, mengubah dampaknya, mengubah kemungkinannya, membagi resiko ke pihak lain dan menahan resiko lalu menginformasikannya (BSN, 2014a).



### 2.3.5.7. Menetapkan Kontrol Keamanan dan Sasaran Keamanan Informasi

Setelah penilaian dan perencanaan penanganan resiko, selanjutnya adalah menetapkan kontrol keamanan. Beberapa kontrol keamanan dapat dipilih dari SNI ISO/IEC 27002 atau diluar daftar kontrol keamanan, atau kontrol keamanan baru dapat dibuat untuk memenuhi kebutuhan spesifik selama kontrol keamanan tersebut cocok (BSN, 2014b). Kontrol keamanan yang dipilih sebaiknya yang memiliki kemampuan untuk (CSM, 2013):

1. Mengurangi resiko ke level yang dapat diterima.
2. Mengurangi kemungkinan ancaman atau kerentanan penyebab resiko.
3. Mengurangi dampak yang mungkin ada jika resiko terjadi.
4. Memastikan pemenuhan kebutuhan bisnis dan hukum/peraturan.
5. Mendeteksi aktifitas atau insiden keamanan informasi yang tidak diinginkan, serta tindakan untuk memperbaiki dan memulihkannya.

Setelah menentukan kontrol keamanan, lalu menetapkan sasaran keamanan informasinya. Sasaran kontrol keamanan dapat ditetapkan sebagai sasaran keamanan informasi tahunan yang digunakan sebagai patokan untuk mengukur efektivitas penerapan SMKI pada periode yang ditetapkan (KEMENKOMINFO, 2011b). Tabel 2.5 berisikan contoh sasaran keamanan informasi.

Tabel 2.5 Contoh Sasaran Keamanan Informasi

| No<br><i>Annex</i> | Kontrol SNI ISO/IEC 27001                               | Sasaran Keamanan Informasi                                                                                                |
|--------------------|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| A.6.1.2            | Pemisahan tugas                                         | Setiap pemasangan perangkat lunak harus dilakukan oleh penanggung jawab operasional TIK, bukan oleh <i>programmer</i> .   |
| A.7.2.2            | Kepedulian, pendidikan dan pelatihan keamanan informasi | Seluruh karyawan dalam satuan kerja yang dimasukkan dalam ruang lingkup harus telah mengikuti program kesadaran keamanan. |

|          |                                                       |                                                                                                                                    |
|----------|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| A.9.2.4  | Manajemen informasi autentikasi rahasia dari pengguna | 80% perangkat komputer yang sensitif sudah menerapkan <i>password</i> yang kuat.                                                   |
| A.9.2.6  | Penghapusan atau penyesuaian hak akses                | Hak akses pengguna yang menjalani mutasi/berhenti bekerja harus ditutup maksimum 2 hari setelah statusnya dilaporkan secara resmi. |
| A.11.1.2 | Akses pusat data (ruangan <i>server</i> )             | Seluruh pihak ketiga (vendor, konsultan) yang memasuki pusat data harus didampingi karyawan.                                       |
| A.12.1.2 | Manajemen perubahan                                   | Versi perangkat lunak yang operasional harus sama dengan versi <i>source code</i> terakhir.                                        |

Sumber: KEMENKOMINFO, 2011b (dengan penyesuaian nomor *Annex* dari versi SNI ISO/IEC 27001:2009 ke versi SNI ISO/IEC 27001:2013 berdasarkan BSI, 2013)

## 2.3.6. Dokumen SMKI

### 2.3.6.1. Struktur Dokumen SMKI

Berdasarkan standar SNI ISO/IEC 27001, setiap dokumen baik kebijakan, prosedur dan lainnya diharuskan tersedia dalam informasi yang terdokumentasi, dikomunikasikan dalam organisasi dan tersedia untuk pemangku kepentingan yang tepat (BSN, 2013a). Dalam urusan dokumentasi, secara umum SMKI memiliki struktur dokumen berupa hirarki yang terdiri dari tiga tingkatan seperti yang terlihat pada Gambar 2.7.



Gambar 2.7 Struktur Dokumen SMKI (KEMENKOMINFO, 2011b)

Berikut ini adalah penjelasan ketiga tingkatan dari struktur dokumen SMKI berdasarkan Gambar 2.7:

1. Dokumen tingkat 1 (bersifat strategis)

Dokumen ini memuat komitmen yang dituangkan dalam bentuk kebijakan, standar, sasaran dan rencana terkait pengembangan, penerapan dan peningkatan SMKI (KEMENKOMINFO, 2011b). Dokumen ini mencakup semua hal yang terkait pada klausul-klausul di SNI ISO/IEC 27001.

2. Dokumen tingkat 2 (bersifat operasional)

Dokumen ini memuat prosedur dan panduan yang dikembangkan oleh organisasi secara internal dan memuat cara penerapan kebijakan yang telah ditetapkan serta menjelaskan penanggung jawab kegiatan (KEMENKOMINFO, 2011b). Prosedur menetapkan "siapa melakukan apa", "dimana", dan "bilamana", dan bisa juga "bagaimana" (Djarmiko, 2015).

3. Dokumen tingkat 3 (bersifat opsional)

Dokumen ini memuat instruksi kerja, petunjuk teknis dan formulir untuk mendukung pelaksanaan prosedur tertentu sampai ketinggian teknis (KEMENKOMINFO, 2011b). Instruksi kerja mencakup salah satu kegiatan dari suatu prosedur, dimana instruksi kerja menetapkan lebih spesifik dan detail mengenai "bagaimana" dan "dengan apa" (Djarmiko, 2015). Jika prosedur sudah menguraikan langkah aktivitas yang jelas dan mudah dipahami penanggung jawab kegiatan maka instruksi kerja tidak diperlukan lagi (KEMENKOMINFO, 2011b).

#### **2.3.6.2. Dokumen yang Dibutuhkan**

Dalam SNI ISO/IEC 27001 terdapat istilah dokumen *mandatory*. Dokumen *mandatory* adalah dokumentasi informasi yang harus diproduksi, didokumentasi dan dirawat sebagai pembuktian bahwa organisasi telah menerapkan SMKI (CSM, 2013). Tabel 2.6 berisikan daftar dokumen *mandatory* yang dinyatakan pada beberapa klausul dalam SNI ISO/IEC 27001:2013.

Tabel 2.6 Daftar Dokumen *Mandatory*

| <b>Dokumen</b>                          | <b>Deskripsi</b>                                                                                                                                                                                                                                                                                                                                                  | <b>Referensi Klausul</b> |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| Ruang lingkup SMKI                      | Dokumen ini berisikan ruang lingkup dan batasan pada SMKI. Setiap perubahan terhadap dokumen ini dapat mencerminkan perubahan terhadap dokumentasi informasi lainnya.                                                                                                                                                                                             | 4.3                      |
| Kebijakan SMKI                          | Dokumen ini berisikan kebijakan level tinggi yang melingkupi kebijakan pendukung lainnya dalam penerapan SMKI. Kebijakan harus dibuat tersedia kepada masing-masing orang didalam organisasi, termasuk pemangku kepentingan lainnya.                                                                                                                              | 5.2                      |
| Proses penilaian resiko                 | Dokumen ini berisikan tahap demi tahap proses penilaian resiko.                                                                                                                                                                                                                                                                                                   | 6.1.1                    |
| Proses penanganan resiko                | Dokumen ini berisikan pemilihan penanganan resiko yang tepat yang mengacu terhadap hasil penilaian resiko.                                                                                                                                                                                                                                                        | 6.1.2                    |
| <i>Statement of Applicability</i> (SoA) | Dokumen ini berisikan kontrol keamanan yang diperlukan dan pembenaran/alasan untuk memilih atau tidak memilih, serta apakah kontrol keamanan tersebut sudah diterapkan atau tidak.                                                                                                                                                                                | 6.1.2                    |
| Sasaran keamanan informasi              | Dokumen ini berisikan sasaran keamanan informasi yang dapat diukur, dikomunikasikan dan diperbaharui ketika dibutuhkan.                                                                                                                                                                                                                                           | 6.2                      |
| Bukti kemampuan/kompetensi              | Organisasi sebaiknya menentukan kompetensi yang dibutuhkan bagi penanggung jawab yang melakukan aktifitas terkait SMKI dan kontrol keamanan yang dapat mempengaruhi SMKI. Dokumen ini berisikan pelatihan sebelumnya, serta jika memungkinkan tindakan yang dilakukan untuk memperoleh kompetensi yang diperlukan dan evaluasi keefektifan tindakan yang diambil. | 7.2                      |

|                                                                                  |                                                                                                                                                                                                                                                                                                                                                                     |     |
|----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Dokumen untuk memenuhi kepercayaan agar proses yang dilakukan sesuai perencanaan | Organisasi sebaiknya merencanakan dan menerapkan proses dan aktifitas operasional untuk memenuhi kebutuhan keamanan serta mengacu resiko dan peluang (menerapkan perencanaan untuk mencapai sasaran keamanan informasi). Dokumen ini juga berisikan setiap perubahan proses dan aktifitas operasional sebagai bukti bahwa aktifitas telah dilakukan sesuai rencana. | 8.1 |
| Hasil penilaian resiko                                                           | Penilaian resiko harus dilakukan sesuai periode yang direncanakan atau ketika terdapat perubahan yang dapat memperkenalkan ancaman baru dalam organisasi. Dokumen ini berisikan hasil dari aktifitas penilaian resiko tersebut.                                                                                                                                     | 8.2 |
| Hasil penanganan resiko                                                          | Dokumen ini berisikan hasil dari aktifitas penanganan resiko yang menjelaskan keadaan dari penanganan resiko, serta harus diserahkan ke pihak manajemen untuk disetujui.                                                                                                                                                                                            | 8.3 |
| Bukti dari hasil pengawasan dan pengukuran                                       | Dokumen ini berisikan setiap bukti yang ada sebagai hasil dari pengukuran dan pengawasan, seperti apa yang diawasi & diukur, mekanisme untuk melakukannya dan juga karyawan yang bertanggung jawab untuk mengawasi, mengukur, menganalisa dan mengevaluasi hasil dari pengawasan dan pengukuran SMKI.                                                               | 9.1 |
| Bukti dari program audit dan hasilnya                                            | Dokumen ini berisikan bukti yang ada sebagai hasil dari audit internal, seperti (tapi tidak terbatas pada) program audit, kebijakan dan prosedur yang berhubungan dengan audit internal SMKI, laporan audit dan catatan audit.                                                                                                                                      | 9.2 |
| Bukti dari hasil tinjauan pihak manajemen                                        | Dokumen ini berisikan setiap bukti yang ada sebagai hasil dari peninjauan pihak manajemen, seperti (tapi tidak terbatas pada) laporan rapat, <i>memo</i> , lembar persetujuan dan <i>email</i> yang berhubungan dengan SMKI.                                                                                                                                        | 9.3 |

|                                            |                                                                                                                                                                                                                                                                                |      |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| Bukti dari sifat ketidak-sesuaian          | Dokumen ini berisikan tindakan yang dilakukan untuk mencatat ketidak-sesuaian, seperti (tapi tidak terbatas pada) kebijakan, prosedur, dan laporan yang tidak sesuai.                                                                                                          | 10.1 |
| Bukti dari hasil setiap tindakan perbaikan | Dokumen ini berisikan tindakan yang dilakukan untuk memperbaiki ketidak-sesuaian, seperti (tapi tidak terbatas pada) rincian dari tindakan perbaikan yang dilakukan untuk merubah ketidak-sesuaian, keadaan dari tindakan perbaikan dan durasi untuk merubah ketidak-sesuaian. | 10.1 |

Sumber: CSM, 2013

### 2.3.7. Keuntungan Penerapan SNI ISO/IEC 27001

Berikut ini adalah beberapa keuntungan yang bisa didapat organisasi jika menerapkan SMKI (BSN, 2014a):

1. Menurunkan resiko keamanan informasi (mengurangi kemungkinan dan/atau dampaknya akibat insiden keamanan informasi).
2. Standar terstruktur yang mendukung proses penentuan, penerapan, pengoperasian dan pemeliharaan SMKI yang memenuhi kebutuhan organisasi.
3. Membantu pihak manajemen untuk mengelola dan mengoperasikan pendekatan mereka menuju manajemen keamanan informasi dalam konteks pengelolaan dan tata kelola resiko organisasi.
4. Kepercayaan para pemangku kepentingan di organisasi dapat bertambah.
5. Penetapan konsep standar dan bahasa umum untuk keamanan informasi akan mempermudah menaruh kepercayaan pada rekan bisnis dengan SMKI, terutama jika mereka mensyaratkan mau berekan dengan yang tersertifikasi SNI ISO/IEC 27001 oleh badan sertifikasi yang terakreditasi.
6. Peningkatan dalam tata cara keamanan informasi yang baik dan diterima secara global dibanding dengan cara yang tidak berpetunjuk.

7. Memberi organisasi kebebasan mengadopsi dan meningkatkan kontrol keamanan yang cocok dengan keadaan khusus organisasi, serta untuk memelihara organisasi untuk menghadapi perubahan internal dan eksternal.

### **2.3.8. Faktor Kesuksesan Penerapan SNI ISO/IEC 27001**

Berikut ini adalah beberapa faktor kesuksesan yang penting dalam penerapan SMKI yang harus dipertimbangkan organisasi (CSM, 2013):

1. Komitmen dan dukungan dari semua pihak manajemen harus diperoleh terlebih dahulu dalam penerapan dan pemeliharaannya.
2. Penerapan SMKI harus sejalan dengan strategi dan bisnis organisasi.
3. Peraturan dan prosedur dari keamanan informasi dikomunikasikan secepatnya ke semua level karyawan, dari manajemen sampai *front desk* untuk memastikan tidak ada kesalahpahaman dan kekurangan informasi diantara karyawan.
4. Aktifitas mendesain SMKI didukung dengan beberapa metode dan pendekatan kreatif sehingga "keinginan untuk berubah" dapat terlihat dan diterima oleh semua level karyawan.
5. Karyawan yang terlibat pada penerapan SMKI harus dibekali dengan kemampuan dan kompetensi yang relevan.
6. Program kesadaran keamanan seluruh karyawan yang relevan dilakukan secara konsisten dan berkala untuk membuat budaya keamanan sehingga seluruh karyawan tersebut sangat mengerti aturan dan tanggung jawabnya.
7. Pengawasan aktif dan peningkatan berkala sangat penting untuk memastikan resiko dan/atau insiden keamanan informasi cepat ditangani.

## **2.4. SNI ISO/IEC 27002 – Kontrol Keamanan**

### **2.4.1. SNI ISO/IEC 27002**

SNI ISO/IEC 27002 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol keamanan tertentu

agar mencapai sasaran kontrol keamanan yang ditetapkan (KEMENPORA, 2012). SNI ISO/IEC 27002 menyerahkan kepada organisasi untuk memilih dan menerapkan kontrol keamanan yang tepat sesuai kebutuhannya, dengan mempertimbangkan hasil penilaian resiko yang telah dilakukan organisasi (KEMENKOMINFO, 2011b). Daftar kontrol keamanan yang disediakan standar ini tidaklah lengkap, dimana organisasi bebas untuk menambah kontrol keamanan baru yang diperlukan atau mengidentifikasi kontrol keamanan tambahan dari sumber manapun yang dianggap penting (CSM, 2013).

#### **2.4.2. Kontrol Keamanan**

Kontrol keamanan adalah alat untuk mencegah terjadinya resiko, meliputi kebijakan, prosedur, panduan, tindakan atau struktur organisasi yang dapat bersifat administratif, teknis, manajemen atau peraturan (KEMENKOMINFO, 2011b). SNI ISO/IEC 27002 merinci 114 kontrol keamanan yang diorganisir kedalam 14 domain dan 35 sasaran kontrol keamanan (GHKSAR, 2015). Kontrol keamanan yang dispesifikasikan dalam SNI ISO/IEC 27002 diakui sebagai praktik terbaik pada sebagian besar organisasi dan siap disesuaikan untuk mengakomodasi berbagai ukuran dan kekompleksitasan organisasi (BSN, 2014a). Sasaran kontrol keamanan dan kontrol keamanan yang terdaftar pada *Annex A* didalam SNI ISO/IEC 27001 secara langsung didapat dari dan disesuaikan dengan yang terdaftar di SNI ISO/IEC 27002 (BSN, 2014a).

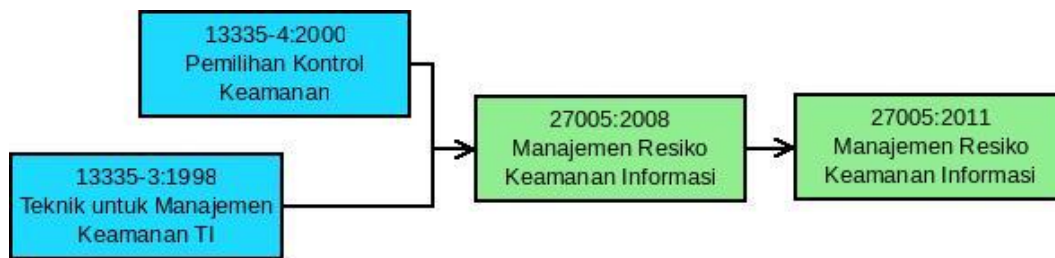
### **2.5. SNI ISO/IEC 27005 – Manajemen Resiko Keamanan Informasi**

#### **2.5.1. SNI ISO/IEC 27005**

SNI ISO/IEC 27005 merupakan standar yang menyediakan pedoman manajemen resiko keamanan informasi, termasuk saran penilaian resiko, penanganan resiko, penerimaan resiko, pengkomunikasian resiko, pengawasan dan peninjauan resiko (BSN, 2014a). Standar ini dapat diterapkan untuk semua tipe organisasi (contohnya perusahaan komersial, pemerintahan, organisasi non-profit) yang berniat untuk mengelola resiko yang dapat mengganggu keamanan informasi di organisasinya (BSN, 2013c). Hubungan antara standar SNI ISO/IEC 27005



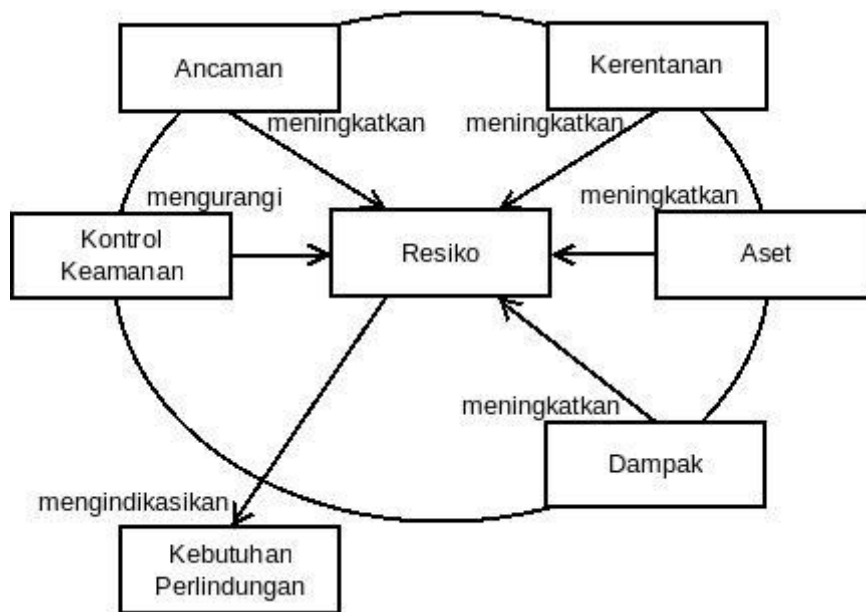
dengan SNI ISO/IEC 27001 adalah menyediakan pendekatan yang konsisten pada manajemen resiko keamanan informasi untuk proses *PDCA* yang ada didalam SNI ISO/IEC 27001 (Humphreys, 2007). Perkembangan versi SNI ISO/IEC 27005 dari awal sampai yang terbaru dapat dilihat pada Gambar 2.8.



Gambar 2.8 Perkembangan SNI ISO/IEC 27005 (Ionita, 2013)

### 2.5.2. Resiko dalam Keamanan Informasi

Resiko dalam keamanan informasi adalah potensi bahwa suatu ancaman akan mengeksploitasi kerentanan dari satu atau sekelompok aset dan karenanya membahayakan organisasi (KEMENKOMINFO, 2011b). Resiko dapat digolongkan dengan kombinasi dua faktor, yaitu kemungkinan dari terjadinya kejadian yang tidak diinginkan dan dampaknya (Ionita, 2013). Dalam hubungannya dengan SMKI, resiko adalah dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam keamanan informasi di organisasi, dalam hal ini ancaman terhadap aspek keamanan informasi yaitu CIA (*confidentiality*, *integrity* dan *availability*) (Sarno, 2009). Hubungan resiko dalam manajemen resiko keamanan informasi dapat dilihat pada Gambar 2.9.



Gambar 2.9 Hubungan Resiko dengan Entitas Lainnya dalam Manajemen Resiko Keamanan Informasi (Ionita, 2013)

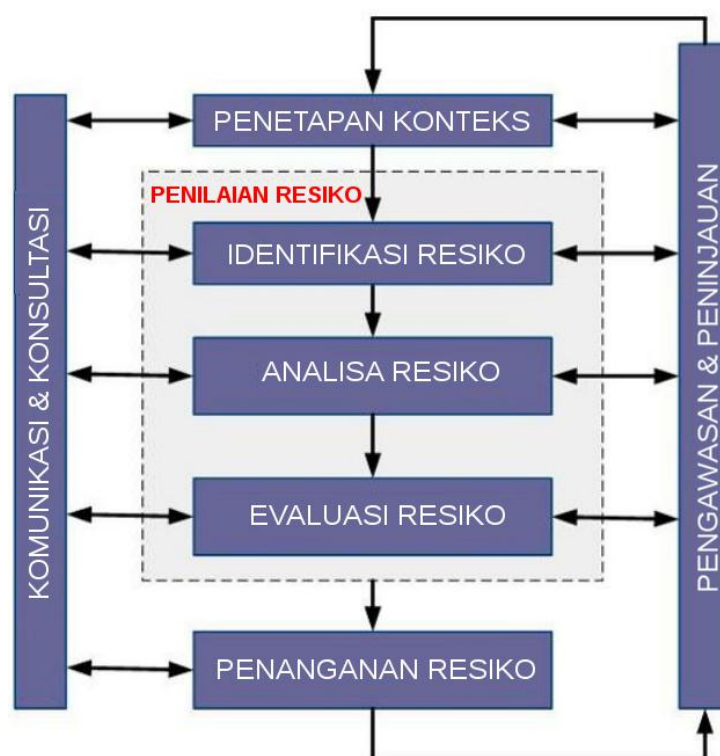
### 2.5.3. Manajemen Resiko Keamanan Informasi

Manajemen resiko keamanan informasi adalah proses untuk menganalisa apa yang terjadi dan dampak yang ada sebelum memutuskan apa yang seharusnya diselesaikan dan kapan untuk mengurangi resiko ke level yang diterima (CSM, 2013). Aktivitas manajemen resiko keamanan informasi pada umumnya mencakup penerapan kebijakan yang tepat dan kontrol keamanan yang berhubungan, meningkatkan kesadaran, dan mengevaluasi kebijakan dan keefektifan kontrol keamanan (Ionita, 2013). Manajemen resiko keamanan informasi bertujuan menjelaskan pada organisasi tentang (Sarno, 2009):

1. Menentukan seberapa besar resiko atau dampak jika terjadi kegagalan keamanan informasi didalam organisasi.
2. Apa saja ancaman terhadap informasi dan juga kerentanan yang dimiliki oleh informasi pada organisasi yang dapat menyebabkan kegagalan keamanan informasi.
3. Bagaimana menangani resiko pada kegagalan keamanan informasi yang terjadi.

4. Menentukan kontrol keamanan yang dibutuhkan untuk memenuhi kriteria manajemen resiko keamanan informasi yang telah dilakukan.

Selain itu organisasi tidak dapat menentukan kontrol keamanan yang dibutuhkan saat menerapkan SMKI tanpa keberadaan manajemen resiko keamanan informasi, sedangkan kontrol keamanan sendiri merupakan hal terpenting dalam merencanakan SMKI (Sarno, 2009). Proses manajemen resiko keamanan informasi berdasarkan standar SNI ISO/IEC 27005:2013 dapat dilihat pada Gambar 2.10.



Gambar 2.10 Proses Manajemen Resiko Keamanan Informasi Berdasarkan SNI ISO/IEC 27005:2013 (BSN, 2013c)

Proses manajemen resiko keamanan informasi terjadi berulang dan sebaiknya dilakukan lagi setidaknya diakhir tahun, dimana tim penilai di organisasi sebaiknya mempertimbangkan evaluasi ulang ketika perubahan pada sistem informasi besar-besaran maupun perubahan pada proses bisnis terjadi (Gordas, 2014). Tabel 2.7 berisikan proses *PDCA* berdasarkan SNI ISO/IEC 27001 yang dipetakan dengan proses manajemen resiko berdasarkan SNI ISO/IEC 27005.

Tabel 2.7 Pemetaan Proses PDCA dengan Proses Manajemen Resiko Keamanan Informasi

| <b>PDCA</b>  | <b>Kegiatan</b>                                                                            |
|--------------|--------------------------------------------------------------------------------------------|
| <i>Plan</i>  | Penetapan konteks, penilaian resiko, merencanakan penanganan resiko, dan penerimaan resiko |
| <i>Do</i>    | Penerapan rencana penanganan resiko                                                        |
| <i>Check</i> | Mengawasi dan meninjau resiko berkelanjutan                                                |
| <i>Act</i>   | Memelihara dan meningkatkan proses manajemen resiko                                        |

Sumber: BSN, 2013c

#### 2.5.4. Penetapan Konteks (*Context Establishment*)

##### 2.5.4.1. Pengaturan Kriteria Resiko

Aktifitas ini dilakukan untuk menetapkan kriteria resiko yang terdiri dari kriteria penerimaan resiko dan kriteria untuk melakukan penilaian resiko keamanan informasi (kriteria evaluasi resiko) (BSN, 2013a). Kriteria evaluasi resiko harus dibangun untuk mengevaluasi resiko pada organisasi karena dapat digunakan untuk menspesifikasikan prioritas untuk penanganan resiko (BSN, 2013c). Sedangkan kriteria penerimaan resiko dibangun untuk mengindikasikan sampai level resiko mana pihak manajemen rela untuk menerima resiko (Siram, 2012). Kriteria resiko dapat mencakup beberapa batasan dengan sasaran level resiko yang diinginkan, namun ketentuan bagi pihak manajemen untuk dapat menerima resiko diluar batas level dalam situasi yang telah dispesifikasikan (BSN, 2013c). Contoh kriteria resiko berdasarkan level resiko dapat dilihat pada Tabel 2.8.

Tabel 2.8 Contoh Kriteria Resiko

| <b>Level Resiko</b> |               | <b>Kegiatan</b>                                                         |
|---------------------|---------------|-------------------------------------------------------------------------|
| 1 – 5               | <i>Low</i>    | Menerima resiko atau rencana tindakan perbaikan bisa dilakukan          |
| 6 – 11              | <i>Medium</i> | Rencana tindakan perbaikan dapat dilakukan pada waktu yang memungkinkan |

|         |                |                                                   |
|---------|----------------|---------------------------------------------------|
| 12 – 19 | <i>High</i>    | Rencana tindakan perbaikan harus segera dilakukan |
| 20 - 25 | <i>Extreme</i> | Resiko level tertinggi                            |

Sumber: Albone, 2009

#### 2.5.4.2. Pengaturan Kriteria Dampak dan Kemungkinan

Aktifitas ini dilakukan untuk menetapkan beberapa kriteria dari dampak dan kemungkinan untuk memudahkan dalam proses penilaian resiko nantinya. Kriteria yang ditetapkan tadi akan dijadikan skala nilai dari kecil ke besar dengan jumlah yang sama. Artinya jika skala nilai dampak berjumlah 5 maka skala nilai kemungkinan juga berjumlah 5. Setiap skala nilai dapat berbentuk satuan kerugian uang atau kemungkinan terjadi setiap tahun agar persepsi dampak bisnis atau kemungkinan yang terjadi mendekati sama untuk setiap persepsi masing-masing pemberi nilai (Purnomo, 2016). Untuk skala nilai dampak juga dapat berupa hilangnya aspek keamanan informasi, gangguan operasional, kerusakan reputasi, atau pelanggaran hukum/kontrak (BSN, 2013c). Contoh dari skala nilai berdasarkan kriteria dampak dan kemungkinan dapat dilihat pada Tabel 2.14 dan Tabel 2.15.

#### 2.5.4.3. Mendefinisikan Ruang Lingkup dan Batasan

Aktifitas ini merupakan proses untuk menentukan parameter global untuk melaksanakan manajemen resiko dalam organisasi (ENISA, 2006). Ruang lingkup dari proses manajemen risiko keamanan informasi perlu ditetapkan untuk memastikan bahwa semua aset yang relevan diperhitungkan dalam penilaian resiko (BSN, 2013c). Apabila ruang lingkup tidak didefinisikan secara baik, maka akan menghasilkan pembuangan sumber daya yang tidak perlu (waktu, biaya dan usaha). Hal ini dikarenakan ketika penilaian resiko dilakukan diruang lingkup berbeda, maka akan menghasilkan identifikasi resiko yang tidak akurat (CSM, 2013).

Jika ruang lingkup dan batasan pada SMKI sudah ditetapkan, maka tidak perlu lagi menentukan ruang lingkup dan batasan pada manajemen resiko keamanan informasi. Hal ini dikarenakan ruang lingkup dan batasan pada SMKI yang diperlukan dalam ISO/IEC 27001 berkaitan dengan ruang lingkup dan batasan pada manajemen resiko keamanan informasi (BSN, 2013c).

#### **2.5.4.4. Menetapkan Peran dan Tanggung Jawab**

Aktifitas ini dilakukan untuk menetapkan siapa yang melakukan proses manajemen resiko keamanan informasi. Berdasarkan SNI ISO/IEC 27005, yang berperan dalam operasional manajemen resiko keamanan informasi dapat dianggap sebagai salah satu sumber daya yang dibutuhkan oleh SNI ISO/IEC 27001 dalam proses SMKI (BSN, 2013c). Jika tim pengelola SMKI sudah ditetapkan, maka tidak perlu lagi menetapkan siapa yang berperan dan bertanggung jawab dalam proses manajemen resiko keamanan informasi. Hal ini dikarenakan tim pengelola SMKI terdiri dari tim pemimpin SMKI dan/atau pihak manajemen resiko yang tugasnya melakukan proses manajemen resiko keamanan informasi.

#### **2.5.5. Penilaian Resiko (*Risk Assessment*)**

##### **2.5.5.1. Identifikasi Resiko (*Risk Identification*)**

Identifikasi resiko adalah proses menemukan, mengenali dan mendeskripsikan resiko (BSN, 2013c). Proses ini dapat melibatkan data historis, opini/pemberitahuan dari para ahli, analisa teoritis, atau kebutuhan pemangku kepentingan (BSN, 2014a). Selama tahapan ini, penting untuk mengidentifikasi dan mencatat semua resiko tanpa menghiraukan fakta bahwa beberapa mungkin sudah dikenali dan dikontrol oleh organisasi (ENISA, 2006). Tujuan identifikasi resiko adalah menentukan faktor potensial apa yang menyebabkan kerugian serta dimana dan kapan itu akan terjadi (BSN, 2013c). Berikut ini adalah beberapa hal yang dilakukan saat identifikasi resiko:

##### **1. Identifikasi aset**

Ditahapan ini akan dilakukan pengidentifikasian aset apa saja yang ada didalam ruang lingkup dan batasan yang telah ditetapkan. Aset adalah segala sesuatu yang memiliki nilai untuk organisasi dan karenanya membutuhkan suatu perlindungan (BSN, 2013c). Namun yang perlu dipahami adalah aset yang dibahas bukanlah yang tidak berkaitan dengan informasi atau bisa disebut aset nyata. Perbandingan dari aset informasi dengan aset nyata dapat dilihat pada Tabel 2.10.

Tabel 2.10 Perbandingan Aset Informasi dengan Aset Nyata

| Karakteristik        | Aset Informasi                                                   | Aset Nyata                                                                           |
|----------------------|------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| Bentuk pemeliharaan  | Tidak memiliki bentuk fisik dan bersifat fleksibel.              | Memiliki bentuk fisik.                                                               |
| Variabel nilai       | Bernilai lebih tinggi ketika digabung dan diproses.              | Total nilai adalah jumlah dari tiap nilai.                                           |
| Berbagi              | Reproduksi tak terbatas dan setiap orang dapat berbagi nilainya. | Reproduksi tidak mungkin, dimana nilai aset akan berkurang jika terdapat reproduksi. |
| Ketergantungan media | Perlu disampaikan melalui media.                                 | Dapat disampaikan secara independen (karena bentuk fisiknya).                        |

Sumber: UN-APCICT, 2009

Aktifitas identifikasi aset mencakup semua aset yang berhubungan dengan informasi, baik yang berfungsi sebagai pengolah, pengirim, media/penyimpanan maupun pendukung. Yang perlu diperhatikan adalah setiap organisasi dapat memiliki ribuan bahkan jutaan aset yang tidak mungkin diharapkan untuk diidentifikasi semua secara individu, namun beberapa aset yang cukup serupa dapat diacu secara kumpulan jika unik dan cukup bernilai/kritis untuk diperhatikan secara individu (UCISA, 2015). Contoh beberapa aset yang dapat diidentifikasi dapat dilihat pada Tabel 2.11.

Tabel 2.11 Katalog Aset

| Tipe            | Aset                                                                 |
|-----------------|----------------------------------------------------------------------|
| Informasi       | Data dan informasi yang diatur oleh sistem manajemen <i>database</i> |
|                 | Data dan informasi yang berbentuk <i>file</i> dan di- <i>share</i>   |
|                 | Data/informasi yang disimpan dimedia (kertas ataupun <i>file</i> )   |
| Perangkat keras | <i>Server</i> (termasuk sistem operasinya)                           |
|                 | Penyimpanan (termasuk sistem operasinya)                             |
|                 | <i>Workstation</i> /komputer (termasuk sistem operasinya)            |
|                 | Perangkat jaringan (termasuk sistem operasinya)                      |

|                     |                                                                                                                        |
|---------------------|------------------------------------------------------------------------------------------------------------------------|
| Perangkat lunak     | Perangkat lunak bisnis (paket standar yang spesifik bagi organisasi/industri tertentu)                                 |
|                     | Sistem manajemen <i>database</i>                                                                                       |
|                     | Perangkat penengah yang memfasilitasi <i>integrity</i> diantara perangkat lunak bisnis                                 |
| Jaringan Komunikasi | <i>Local Area Network (LAN)</i>                                                                                        |
|                     | Jaringan tambahan yang menghubungkan <i>LAN</i> ke jaringan yang lebih luas ( <i>WAN, MAN, internet</i> , dan lainnya) |
| Fasilitas fisik     | Pusat data atau <i>disaster recovery center</i> /pusat pemulihan bencana                                               |
|                     | Ruang kerja                                                                                                            |
| Perangkat Pelengkap | Sistem <i>HVAC (Heating, Ventilating, Air Conditioning)</i>                                                            |
|                     | Sumber tenaga listrik                                                                                                  |
|                     | Kabel telekomunikasi dan listrik                                                                                       |
| Karyawan            | Karyawan pengguna yang menjalankan sistem informasi                                                                    |
|                     | Karyawan TIK yang berperan sebagai pemelihara sistem informasi atau pendukung teknis                                   |

Sumber: Rahmad at al., 2010

Setelah identifikasi aset, pemilik aset sebaiknya juga diidentifikasi terhadap setiap aset (CSM, 2013). Pemilik aset adalah individu atau entitas yang disetujui oleh pihak manajemen untuk bertanggung jawab terhadap daur hidup aset (BSN, 2014b). Tanggung jawab yang dimiliki oleh pemilik aset dapat berupa pembuatan, pengembangan, pemeliharaan, penggunaan dan/atau pelaksanaan pengamanan yang sesuai pada aset.

## 2. Identifikasi ancaman

Ditahapan ini akan dilakukan pengidentifikasian beberapa ancaman pada aset yang telah teridentifikasi sebelumnya. Ancaman merupakan setiap kejadian atau tindakan yang berpotensi merusak/mengganggu/merugikan sistem atau aset yang mempengaruhi penggunaan dan operasional normal, dalam istilah *confidentiality*, *integrity* dan *availability* (GHKSAR, 2012b). Beberapa ancaman mungkin saja



mempengaruhi lebih dari satu aset serta dapat menyebabkan dampak yang berbeda tergantung aset mana yang dipengaruhi (BSN, 2013c). Identifikasi ancaman dapat dibuat berdasarkan riwayat insiden keamanan informasi sebelumnya (jika itu terjadi), keterangan pemilik/pengguna aset dan katalog ancaman eksternal (Gordas, 2014). Contoh beberapa ancaman berikut sumber ancamannya dapat dilihat pada Tabel 2.12.

Tabel 2.12 Katalog Ancaman

| Sumber Ancaman                  | Ancaman                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bencana Alam                    | Kebakaran, banjir, petir, badai/angin topan, gempa bumi, letusan gunung berapi.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Lingkungan/<br>kegagalan teknis | Kerusakan akibat air, gangguan elektromagnetik dari perangkat, hubungan arus pendek, kegagalan daya listrik, polusi/debu/korosi, kegagalan perangkat keras, kegagalan perangkat jaringan, kegagalan perangkat lunak, tidak sesuai kondisi temperatur atau/dan kelembaban, penurunan kondisi media penyimpanan, kegagalan <i>HVAC</i> .                                                                                                                                                                                        |
| Ketidaksengajaan manusia        | Kesalahan pengguna, kesalahan administrator, kesalahan konfigurasi, penyebaran <i>malware</i> , bocornya informasi, perubahan informasi tanpa sengaja, kesalahan pembuatan data, penurunan kualitas media informasi, kerusakan informasi, penyingkapan/penyebaran informasi, kesalahan/ <i>bug</i> pada perangkat lunak, kurangnya pemeliharaan/pembaharuan perangkat lunak, kurangnya pemeliharaan perangkat keras, kurangnya pemeliharaan jaringan, kegagalan akibat penggunaan melebihi batas kapasitas, absensi karyawan. |
| Kesengajaan manusia             | Diintai oleh orang asing, perusakan dari luar (peluru/barang yang dilepas dari luar), perusakan dari dalam (karyawan, kontraktor), teroris (sabotase, bom), pencurian perangkat keras, pencurian perangkat jaringan, pencurian dokumen/media penyimpanan, perubahan tanpa izin konfigurasi jaringan, perubahan tanpa izin konfigurasi perangkat keras, perubahan tanpa izin konfigurasi perangkat lunak, penghapusan/penambahan tanpa izin perangkat lunak, penghapusan tanpa                                                 |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kesengajaan manusia<br>(lanj.) | izin data, lambatnya jaringan karena <i>worm</i> , pengaksesan dan penyebaran tanpa izin data, penyimpanan data yang dimasukkan, penghapusan perangkat lunak oleh <i>malware</i> , perubahan fungsi/operasi perangkat lunak oleh <i>malware</i> , penggunaan perangkat lunak ilegal, gangguan ke sistem oleh pihak ketiga yang kontrak dengan organisasi, karyawan operasional absen, <i>masquerading</i> identitas pengguna, <i>sniffing</i> , penyalahgunaan hak akses, penyalahgunaan perangkat lunak, penyalahgunaan perangkat keras, penyalahgunaan jaringan, penyalahgunaan dokumen, penyebaran <i>malware</i> , akses tanpa izin, <i>eavesdropping</i> , manipulasi perangkat lunak, <i>denial of service</i> , pemerasan, <i>social engineering</i> . |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Sumber: Rahmad, 2010

### 3. Identifikasi kontrol keamanan yang ada

Ditahapan ini akan dilakukan pengidentifikasian kontrol keamanan yang ada di organisasi. Hal ini dilakukan untuk mengukur resiko yang ada sebenarnya pada aset dan untuk mencegah identifikasi kontrol keamanan yang serupa (CSM, 2013). Pengertian dari kontrol keamanan adalah teknik, aktifitas atau teknologi yang digunakan untuk mengurangi resiko pada suatu aset informasi di organisasi (Landoll, 2011). Contoh kontrol keamanan pada ketiga area dapat dilihat pada Tabel 2.13.

Tabel 2.13 Contoh Kontrol Keamanan pada Ketiga Area

| Area           | Contoh                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Administrative | <b>Definisi:</b> kebijakan, prosedur atau aktifitas yang melindungi aset informasi organisasi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|                | <i>Background check</i> , program kesadaran keamanan, pelatihan kerja, kebijakan penggunaan peralatan, kebijakan yang berisi sangsi, prosedur pemberhentian, prosedur pemeliharaan, prosedur pengawasan, pelabelan informasi, prosedur penghancuran media, prosedur pembuatan akun pengguna, peninjauan hak akses, prosedur penghapusan akun pengguna, pemisahan tugas pada aktifitas kritis, <i>disaster recovery plan</i> , <i>business continuity plan</i> , <i>hardening</i> untuk <i>server</i> , perjanjian kontrak, persyaratan keamanan minimum, pengujian keamanan pada <i>server</i> , prosedur |

|                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Administrative</i><br>(lanj.) | penanganan insiden keamanan informasi, pelatihan penanganan insiden keamanan informasi, audit secara internal, tinjauan dari pihak ketiga, penilaian resiko/manajemen resiko, perjanjian menjaga kerahasiaan, inventarisasi aset, prosedur pelacakan aset, standar dalam pembuatan perangkat lunak, peninjauan <i>source code</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <i>Physical</i>                  | <p><b>Definisi:</b> perlindungan fisik pada karyawan dan fasilitas organisasi.</p> <p>Pengatur tegangan, pembangkit tenaga listrik, sistem <i>HVAC</i>, pendeteksi/pencatat temperatur, pengatur kelembaban, pendeteksi/pencatat kelembaban, konstruksi material bangunan yang aman, jalur evakuasi, pendeteksi asap, perangkat <i>alarm</i> setempat/kota, pemadam api, perlindungan dari kerusakan air, penangkal petir, tempat perlindungan angin topan, karung pasir, tanda pengenal, pagar, kunci, pintu, kontrol akses fisik, pencahayaan darurat, <i>CCTV</i>, sensor pendeteksi gangguan, pembaca kartu masuk, akses <i>biometrics</i>, inspeksi barang.</p>                                                                                                                                                                                                                                                           |
| <i>Technical</i>                 | <p><b>Definisi:</b> perlindungan logis pada aset informasi organisasi.</p> <p>Teknologi <i>monitoring</i> (kebiasaan, riwayat <i>URL</i>, dan lainnya), audit <i>trail</i>, kontrol akses logis, <i>checksum</i>, <i>anti-virus</i>, <i>anti-spam</i>, perangkat pembersih <i>spyware</i>, autentikasi dua faktor, perangkat peretas <i>password</i>, teknologi <i>backup</i> data, perangkat analisa forensik, perangkat pemindaian kerentanan, perangkat tes penetrasi, sistem manajemen <i>patch</i>, sistem manajemen konfigurasi, sistem manajemen identitas, perangkat pembuat <i>password</i> yang aman, <i>firewall</i>, <i>intrusion detection system</i> jaringan/host, <i>digital signatures</i>, segmentasi jaringan, <i>demilitarized zone (DMZ)</i>, <i>secure socket layer (SSL)</i> atau <i>transport layer security (TLS)</i>, <i>virtual private network (VPN)</i>, enkripsi <i>file/email/jaringan</i>.</p> |

Sumber: Landoll, 2011

Ketika mengidentifikasi kontrol keamanan yang ada, pengecekan sebaiknya dilakukan untuk memastikan bahwa kontrol keamanan berkerja secara benar, karena dapat menyebabkan kerentanan jika kontrol tidak berkerja seperti yang diharapkan (BSN, 2013c). Berikut ini adalah beberapa aktifitas yang membantu dalam identifikasi kontrol keamanan yang ada maupun yang akan direncanakan (BSN, 2013c):

1. Meninjau dokumen yang berisi informasi kontrol keamanan (contohnya rencana penanganan resiko).
2. Meninjau hasil audit tentang keamanan informasi yang telah dilakukan.
3. Memeriksa orang yang bertanggung jawab terhadap keamanan informasi (misalnya karyawan sistem keamanan informasi, manajer bangunan atau manajer operasional) dan pengguna untuk memastikan kontrol keamanan mana yang benar-benar diterapkan.
4. Meninjau langsung dilapangan, membandingkan kontrol keamanan yang telah diterapkan dengan daftar kontrol keamanan apa yang seharusnya ada disana.

#### **4. Identifikasi kerentanan**

Ditahapan ini akan dilakukan pengidentifikasian kerentanan yang ada di organisasi. Kerentanan bisa diartikan kelemahan dari kontrol keamanan atau tidak adanya kontrol keamanan (Landoll, 2011). Kehadiran kerentanan apapun tidak akan merusak sampai dimanfaatkan oleh ancaman (CSM, 2013). Berikut ini beberapa contoh kerentanan (Humphreys, 2007):

1. Kurangnya prosedur yang efektif, tidak tepatnya prosedur, susah nya penggunaan prosedur, prosedur yang tidak terbaru/*update*.
2. Pelatihan terhadap karyawan yang tidak tepat atau cukup.
3. Kurangnya kontrol keamanan yang memadai untuk menangani media komputer atau akun pengguna.
4. Kesalahan/*error* pada peralatan.
5. *Bug* dan cacat pada perangkat lunak, kesalahan *source code* dan lainnya.

Yang perlu diperhatikan adalah kontrol keamanan yang tidak benar atau digunakan secara tidak benar dapat menyebabkan kerentanan, misalnya mengharuskan *password* yang kompleks tanpa pelatihan yang tepat sehingga membuat pengguna menuliskan *password* (BSN, 2013c). Selain itu suatu ancaman bisa memiliki beberapa kemungkinan dalam mengeksploitasi satu atau lebih

kerentanan yang ada di organisasi. Contohnya ancaman akses tanpa izin akan menjadi insiden keamanan informasi jika (Humphreys, 2007):

- Akses ke sistem komputer melalui lemahnya *password*/tidak cukupnya manajemen pengguna akan *password*, akun masih terbuka saat karyawan pergi, kurangnya kontrol terhadap penipuan/*scam*, buruknya konfigurasi *server/firewall*/komponen jaringan lainnya, atau kurangnya program kesadaran keamanan.
- Akses fisik ke gedung, kantor atau ruang komputer lemah seperti kunci berkualitas rendah, kontrol *password* pintu mudah ditebak, kekuatan pintu tidak cukup menahan *brute force*, atau jendela dibiarkan terbuka.

Metode yang digunakan untuk menentukan kerentanan dapat berupa pencarian sumber-sumber kerentanan (data teknik sistem TIK, data kelemahan sistem perangkat lunak, dokumentasi analisis resiko), pengujian sistem keamanan (sistem keamanan diuji secara langsung dengan metode tes penetrasi ataupun pemindaian kerentanan) maupun membuat daftar kebutuhan keamanan (membuat daftar kebutuhan keamanan lalu dibandingkan dengan keamanan yang ada) (Sarno, 2009). Metode pencarian kerentanan juga dapat mencakup kegiatan seperti peninjauan *source code*, wawancara/kuisioner dengan pemangku kepentingan, pemeriksaan fisik dan analisis dokumen (BSN, 2013c).

#### **2.5.5.2. Analisis Resiko (*Risk Analysis*)**

Analisis resiko adalah proses memahami sifat dasar dari resiko dan menentukan level resiko yang besarnya dinyatakan dengan kombinasi dari dampak dan kemungkinan (BSN, 2014a). Berikut ini adalah beberapa hal yang dilakukan saat analisis resiko:

##### **1. Penilaian dampak**

Ditahapan ini akan dilakukan penilaian dampak yang akan diterima organisasi jika ancaman terjadi. Dampak adalah hasil dari kejadian yang mempengaruhi tujuan, dan biasanya negatif dalam konteks keamanan informasi (BSN, 2014a). Penilaian dampak bisa diartikan memperkirakan tingkat kerugian atau

kerusakan yang akan terjadi (GHKSAR, 2012b). Dalam penilaian dampak secara kualitatif, nilai yang diberikan harus sesuai dengan besarnya dampak berdasarkan skala nilai dampak. Contoh dari skala nilai dampak dapat dilihat pada Tabel 2.14.

Tabel 2.14 Contoh Skala Nilai Dampak

| Nilai                  | Kriteria Dampak                                                                                                                                                                                                                                                                                                                                       |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Very Low</i><br>(1) | <ul style="list-style-type: none"> <li>• Gangguan layanan kecil/tidak ada.</li> <li>• Kerugian finansial dapat diabaikan.</li> <li>• Dampak reputasi kecil.</li> <li>• Masalah hukum tidak ada.</li> <li>• Kesehatan &amp; keselamatan tidak ada/kecil.</li> </ul>                                                                                    |
| <i>Low</i><br>(2)      | <ul style="list-style-type: none"> <li>• Gangguan layanan &lt; 1 hari.</li> <li>• Kerugian finansial &lt; 5% dari pendapatan sebelum pajak.</li> <li>• Dampak reputasi berupa keluhan.</li> <li>• Masalah hukum berupa tindakan hukum.</li> <li>• Kesehatan &amp; keselamatan seperti luka atau memar.</li> </ul>                                     |
| <i>Medium</i><br>(3)   | <ul style="list-style-type: none"> <li>• Gangguan layanan 1 hari.</li> <li>• Kerugian finansial 5-15% dari pendapatan sebelum pajak.</li> <li>• Dampak reputasi berupa perhatian media lokal atau pemerintah.</li> <li>• Masalah hukum berupa tindakan hukum.</li> <li>• Kesehatan &amp; keselamatan seperti patah tulang atau izin sakit.</li> </ul> |
| <i>High</i><br>(4)     | <ul style="list-style-type: none"> <li>• Gangguan layanan 1-5 hari.</li> <li>• Kerugian finansial 15-50% dari pendapatan sebelum pajak.</li> <li>• Dampak reputasi berupa perhatian media nasional atau pemerintah.</li> <li>• Masalah hukum berupa tindakan hukum.</li> <li>• Kesehatan &amp; keselamatan seperti kematian atau cacat.</li> </ul>    |

|                                 |                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><i>Very High</i><br/>(5)</p> | <ul style="list-style-type: none"> <li>• Gangguan layanan &gt; 1 minggu atau gagal mencapai satu atau lebih sasaran organisasi.</li> <li>• Kerugian finansial &gt; 50% dari pendapatan sebelum pajak.</li> <li>• Dampak reputasi berupa perhatian media luar.</li> <li>• Masalah hukum berupa tindakan hukum (termasuk hukuman tahanan). .</li> </ul> |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Sumber: CSRM, 2012

## 2. Penilaian kemungkinan

Ditahapan ini akan dilakukan penilaian kemungkinan atau *likelihood* terjadinya ancaman yang dihadapi organisasi. Kemungkinan merupakan kesempatan terjadinya sesuatu (BSN, 2014a). Penilaian kemungkinan bisa diartikan memperkirakan frekwensi dari ancaman yang terjadi (GHKSAR, 2012b). Saat menilai, organisasi mungkin perlu untuk merujuk ke data historis, laporan sebelumnya dan/atau wawancara dengan pemilik aset, begitu juga statistik insiden keamanan informasi (jika ada) (CSM, 2013). Dalam penilaian kemungkinan secara kualitatif, nilai yang diberikan harus sesuai dengan frekuensi kejadian berdasarkan skala nilai kemungkinan. Contoh dari skala nilai kemungkinan dapat dilihat pada Tabel 2.15.

Tabel 2.15 Contoh Skala Nilai Kemungkinan

| Nilai                  | Kriteria Kemungkinan                                                                                                                                    |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Rare</i><br>(1)     | <ul style="list-style-type: none"> <li>• Tidak ada sejarah kejadian.</li> <li>• Kejadian hanya mungkin terjadi pada keadaan yang luar biasa.</li> </ul> |
| <i>Unlikely</i><br>(2) | Kejadian bisa terjadi (berulang) pada suatu waktu.                                                                                                      |
| <i>Possible</i><br>(3) | <ul style="list-style-type: none"> <li>• Telah terjadi di masa lalu.</li> <li>• Kejadian mungkin kerap terjadi (berulang) pada suatu waktu.</li> </ul>  |
| <i>Likely</i><br>(4)   | Kejadian akan terjadi (berulang) pada sebagian besar keadaan.                                                                                           |

|                       |                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <i>Certain</i><br>(5) | <ul style="list-style-type: none"> <li>• Sejarah terjadinya berulang.</li> <li>• Kejadian akan terjadi (berulang).</li> </ul> |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------|

Sumber: CSRM, 2012

### 3. Menentukan level resiko

Ditahapan ini akan dilakukan penentuan level resiko dari suatu ancaman. Level resiko adalah besarnya resiko yang dinyatakan dalam istilah kombinasi dampak dan kemungkinan (BSN, 2014a). Penentuan level resiko dapat dihitung dengan rumus sebagai berikut (Itradat, 2014):

$$Resiko = Kemungkinan \times Dampak \quad (2.1)$$

dimana:

*Resiko* = Nilai level resiko yang dicari

*Kemungkinan* = Nilai kemungkinan dari resiko

*Dampak* = Nilai dampak dari resiko

Setelah level resiko sudah ditentukan, selanjutnya adalah memetakan semua yang saling berhubungan dari hasil identifikasi dan analisis resiko kedalam lembar kerja penilaian resiko. Lembar kerja penilaian resiko dapat dilihat pada Tabel 2.16.



Tabel 2.16 Lembar Kerja Penilaian Resiko

| Aset       | Ancaman                   | Kontrol Keamanan                                                                                                                 | Kerentanan                                                                                 | Aspek CIA | Probabilitas | Dampak | Level Resiko |
|------------|---------------------------|----------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-----------|--------------|--------|--------------|
| Database X | Aktifitas <i>hack</i>     | Kebijakan dan prosedur perlindungan data, kontrol keamanan jaringan, kontrol keamanan sistem                                     | Koneksi <i>internet</i> , kurang memadainya perlindungan <i>firewall</i>                   | C + I     | 1            | 4      | 4            |
|            | Buruknya kualitas data    | Pengecekan <i>integrity</i> yang tersedia, prosedur rutin untuk memeriksa dan memperbaiki data, pengecekan ulang secara terpisah | Kurangnya kualitas informasi yang disediakan, tidak lengkapnya pemeriksaan dan pembaharuan | I + A     | 3            | 2      | 6            |
|            | <i>Social engineering</i> | Kebijakan dan prosedur perlindungan data, program kesadaran keamanan                                                             | Kurang patuhnya terhadap prosedur, kurangnya kesadaran terhadap ancaman                    | C         | 1            | 3      | 3            |

Sumber: Ralph, 2010

#### **2.5.5.3. Evaluasi Resiko (*Risk Evaluation*)**

Tujuan aktifitas ini adalah untuk membantu dalam pembuatan keputusan (resiko mana yang perlu ditangani dan mana yang tidak) dan prioritas untuk penerapan penanganan resiko berdasarkan hasil analisis resiko (Itradat, 2014). Untuk itulah perlu dilakukan perbandingan nilai level resiko yang ditentukan selama analisis resiko dengan kriteria resiko yang didapat saat penetapan konteks (BSN, 2013c). Normalnya semakin tinggi level resiko maka prioritas yang tinggi harus diberikan, dengan kata lain resiko dengan prioritas tinggi biasanya tidak diterima dan membutuhkan perhatian lebih dari pihak manajemen (GHKSAR, 2012b).

#### **2.5.6. Penanganan Resiko (*Risk Treatment*)**

##### **2.5.6.1. Modifikasi Resiko (*Risk Modification*)**

Pilihan ini digunakan untuk mengurangi resiko pada organisasi ke level yang dapat diterima melalui adopsi tambahan kontrol keamanan atau meningkatkan kontrol keamanan yang ada (Landoll, 2011). Secara umum kontrol keamanan bisa menyediakan satu atau lebih tipe pengamanan, seperti mengoreksi, mengeliminasi, mencegah, mengurangi dampak, menolak, mendeteksi, memperbaiki, mengawasi dan menyadarkan (BSN, 2013c). Berikut ini adalah contoh kontrol keamanan untuk memodifikasi resiko (GHKSAR, 2012b):

1. Membangun/meningkatkan kebijakan, prosedur, instruksi kerja keamanan informasi untuk memastikan perlindungan yang efektif.
2. Mengkonfigurasi ulang sistem operasi, komponen jaringan dan perangkat untuk menangani kerentanan yang diidentifikasi selama penilaian resiko.
3. Menerapkan prosedur kontrol *password* atau mekanisme autentikasi untuk memastikan kekuatan *password*.
4. Menerapkan enkripsi atau teknologi autentikasi untuk mengamankan transmisi data.
5. Meningkatkan perlindungan keamanan fisik.
6. Membangun penanganan insiden keamanan informasi dan prosedur pelaporan.

7. Membangun program kesadaran keamanan kepada karyawan untuk memastikan kepatuhan terhadap kebutuhan keamanan.

Yang harus diperhatikan saat pemilihan kontrol keamanan adalah harus memenuhi kebutuhan dan sesuai dengan organisasi, serta merupakan hasil dari penilaian resiko yang dilakukan organisasi terhadap aset yang dimiliki (Sarno, 2009).

#### **2.5.6.2. Menghindari Resiko (*Risk Avoidance*)**

Cara menghindari resiko adalah dengan tidak membiarkan tindakan yang menyebabkan resiko muncul (BSN, 2014a). Hal ini bisa dilakukan dengan membatalkan suatu kegiatan yang direncanakan/ada atau mengubah kondisi dimana kegiatan tersebut dijalankan (BSN, 2013c). Menghindari resiko bisa dicapai melalui (Siram, 2012):

- Tidak melakukan aktifitas tugas tertentu (contohnya tidak memproses informasi melalui infrastruktur bersama/*shared*).
- Memindahkan aset jauh dari lokasi resiko (contohnya memindahkan manajemen layanan tertentu ke pengelola layanan yang berbeda).
- Memutuskan untuk tidak memproses informasi sensitif tertentu (contohnya dengan pihak ketiga jika kecukupan perlindungan tidak bisa dijamin).

#### **2.5.6.3. Membagi Resiko (*Risk Sharing*)**

Membagi resiko melibatkan keputusan untuk membagikan resiko tertentu dengan pihak eksternal (CSM, 2013). Membagi resiko dapat diselesaikan dengan asuransi yang mendukung dampak (dari resiko yang dimaksud) atau dengan mengontrak pihak yang berperan mengawasi sistem informasi dan mengambil tindakan langsung untuk menghentikan serangan sebelum mencapai level kerusakan yang telah didefinisikan (BSN, 2013c). Aktifitas ini bisa juga dikarenakan pihak lain mampu untuk menerima resiko dan memiliki kontrol keamanan yang lebih bagus atas resiko (GHKSAR, 2012b).

Yang harus diperhatikan pada beberapa kasus adalah tanggung jawab tertinggi untuk keamanan pada informasi dan fasilitas pemrosesan informasi yang dibagi risikonya tetap ada pada organisasi (Siram, 2012). Jadi meskipun dimungkinkan untuk mengalihkan tanggung jawab mengelola resiko ke pihak lain, namun tidak mungkin untuk membagi tanggung jawab terhadap dampak, karena biasanya pelanggan akan menghubungkan dampak buruk sebagai kesalahan dari organisasi (BSN, 2013c). Selain itu, membagi resiko dapat membuat resiko baru atau memodifikasi resiko saat ini yang teridentifikasi, dimana penanganan resiko tambahan mungkin saja diperlukan (CSM, 2013).

#### **2.5.6.4. Menyimpan Resiko (*Risk Retention*)**

Keputusan ini dipilih oleh organisasi ketika keputusan telah dibuat untuk menerima resiko dan memikul dampaknya ketika resiko terjadi (CSM, 2013). Ini terjadi jika level resiko mencukupi kriteria penerimaan resiko, yang mana tidak diperlukan lagi penerapan kontrol keamanan tambahan (BSN, 2013c). Keputusan untuk menyimpan resiko diberitahukan (kepada pemangku kepentingan yang terlibat) untuk menerima resiko tertentu (BSN, 2014a).

#### **2.5.7. Komunikasi dan Konsultasi**

Aktifitas ini merupakan proses yang dilakukan secara berkelanjutan dan berulang untuk menyediakan, membagi atau memperoleh informasi, serta mengikut sertakan para pemangku kepentingan dalam diskusi mengenai manajemen resiko (BSN, 2013c). Informasi dapat berhubungan dengan kehadiran, sifat, bentuk, kemungkinan, signifikansi, evaluasi, penerimaan dan penanganan resiko (BSN, 2014a). Komunikasi tentang resiko ini sebaiknya dilakukan untuk (BSN, 2013c):

1. Menyediakan jaminan dari hasil manajemen resiko keamanan informasi di organisasi.
2. Mengumpulkan informasi resiko.
3. Menyebarkan hasil dari penilaian dan rencana penanganan resiko.

4. Untuk mendukung pembuat keputusan.
5. Untuk memperoleh ilmu keamanan informasi baru.
6. Untuk mengkoordinasikan dengan pihak lain dan merencanakan balasan untuk mengurangi dampak dari setiap insiden keamanan informasi.
7. Untuk meningkatkan kesadaran.

#### **2.5.8. Pengawasan dan Peninjauan**

Setiap organisasi secara terus menerus menghadapi sejumlah ancaman dan kerentanan baru atau berubah yang tidak ada habisnya, yang mana bisa mempengaruhi aktifitas operasional atau pemenuhan sasaran dari organisasi (ENISA, 2006). Untuk itu diperlukan pengawasan dan peninjauan berkelanjutan terhadap perubahan resiko yang dihadapi organisasi. Selain itu kontrol keamanan diharuskan dievaluasi keefektifannya, karena bisa saja kontrol keamanan yang ada bisa menjadi tidak efektif, tidak cukup ataupun tidak selaras, dimana kontrol keamanan baru harus dipertimbangkan (Gordas, 2014). Organisasi sebaiknya memastikan pengawasan secara berkala pada poin-poin dibawah (BSN, 2013c):

1. Aset baru yang telah dimasukkan kedalam ruang lingkup manajemen resiko keamanan informasi.
2. Modifikasi yang diperlukan pada nilai aset, contohnya perubahan kebutuhan bisnis.
3. Ancaman baru yang dapat aktif diluar/didalam organisasi yang belum dinilai.
4. Kemungkinan kerentanan yang baru atau bertambah yang membuat ancaman bisa memanfaatkan kerentanan tersebut.
5. Insiden keamanan informasi.

#### **2.5.9. Perbedaan Pemilik Resiko dan Pemilik Aset**

SNI ISO/IEC 27001:2013 mensyaratkan untuk mengidentifikasi pemilik resiko yang nantinya akan memberikan nilai pada resiko, dimana pemilik resiko merupakan istilah baru pada SNI ISO/IEC 27005:2013 dan SNI ISO/IEC 27001:2009.

Pemilik aset adalah orang yang bertanggung jawab terhadap setiap aset didalam organisasi (Kosutic, 2013). Tanggung jawab yang dimiliki pemilik aset bisa berupa pembuatan, pengembangan, pemeliharaan, penggunaan dan/atau pelaksanaan pengamanan yang sesuai pada aset. Sering kali pemilik aset tidak memiliki wewenang untuk memecahkan masalah resiko keamanan informasi yang berpotensi (Shuff, 2015). Sedangkan pemilik resiko adalah orang yang memiliki akuntabilitas dan wewenang/kuasa untuk mengelola resiko (BSN, 2014a). Pemilik resiko umumnya diharuskan (Shah, 2015):

1. Memiliki kemampuan untuk memerintahkan sumber daya yang dibutuhkan di organisasi untuk mengurangi atau mengatasi sepenuhnya resiko yang potensial.
2. Memiliki keterlibatan sangat tinggi atau setidaknya memiliki pemahaman yang kuat terhadap area bisnis dimana resiko diidentifikasi.

Kesimpulan dari beberapa hal diatas adalah pemilik aset merupakan orang yang bertanggung jawab terhadap aset (contohnya *administrator*, *programmer*, staf TIK, operator, dan lainnya), sedangkan pemilik resiko merupakan orang yang berwenang/memiliki akuntabilitas untuk mengelola resiko yang ada dari aset tersebut (contoh ketua/kepala departemen, pimpinan organisasi, dan lainnya). Contoh perbedaannya adalah kepala departemen TIK berwenang dalam penerapan kontrol keamanan seperti pelatihan keamanan informasi terhadap *administrator*, namun *administrator* tidak berwenang untuk mengajukan kontrol keamanan tersebut (Purnomo, 2016).

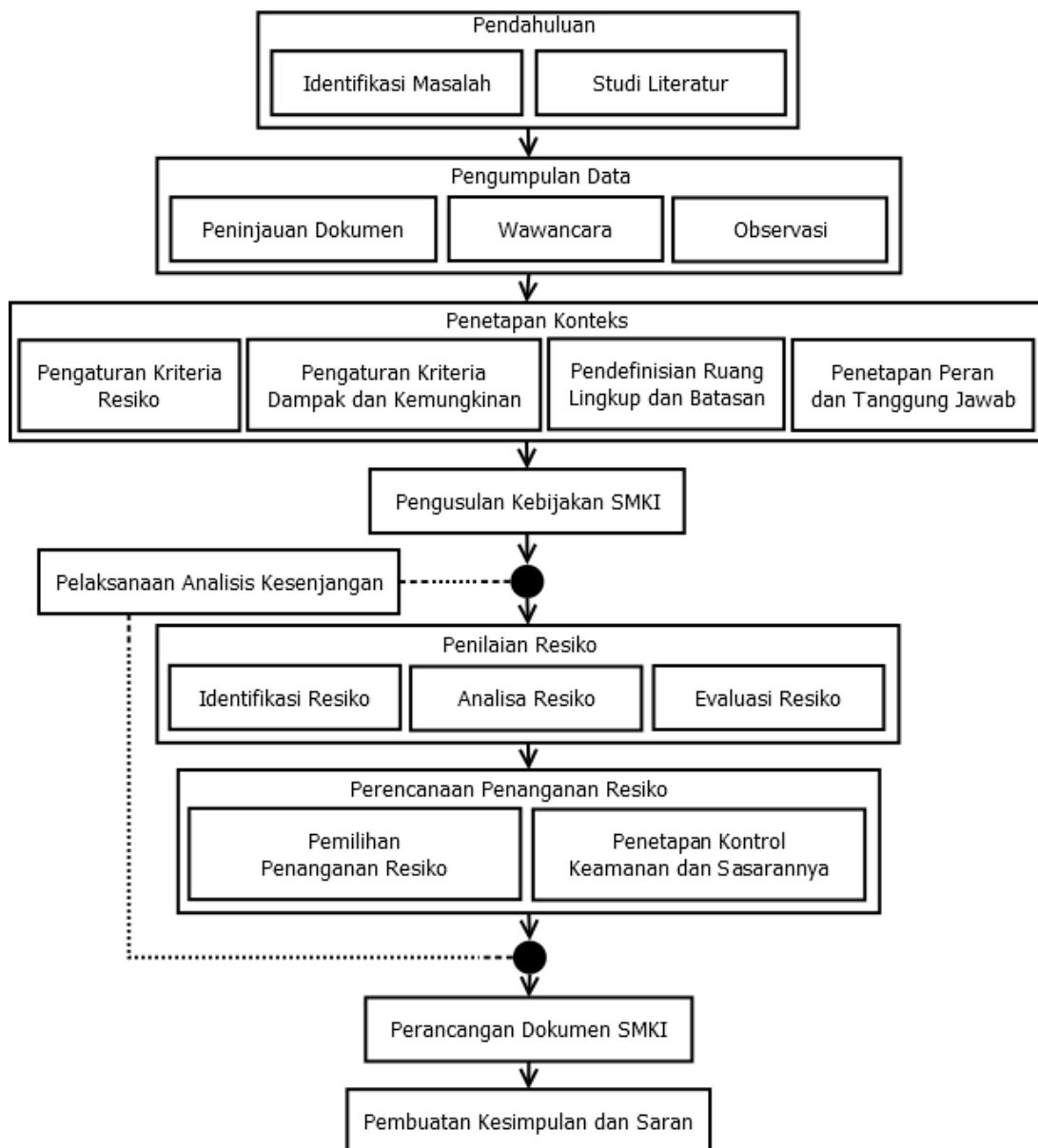
Aset, pemilik aset dan pemilik resiko yang akan diidentifikasi pada penelitian ini adalah yang berkaitan dengan *website server* dan *email* ITS. Jadi kalau nanti terdapat aset lain yang ada di DPTSI-ITS tapi tidak berkaitan dengan *website server* dan *email* ITS, aset tersebut tidak akan diidentifikasi meskipun sama-sama menggunakan perangkat jaringan dan *server*, serta dikelola oleh DPTSI-ITS. Contoh aset yang tidak berkaitan adalah *Digital Library*, SIM Kepegawaian, Integra ITS dan lainnya.

*Halaman ini sengaja dikosongkan*

### BAB III

## METODE PENELITIAN

BAB ini membahas tentang metode yang digunakan untuk menyelesaikan permasalahan penelitian seperti yang digambarkan pada Gambar 3.1. Data contoh akan diberikan pada aktifitas penilaian resiko dan perencanaan penanganan resiko untuk menggambarkan bagaimana metode akan dijalankan ketika penelitian.



Gambar 3.1 Alur Tahapan Penelitian



### **3.1. Pendahuluan**

#### **3.1.1. Identifikasi Masalah**

Identifikasi masalah dilakukan untuk mengidentifikasi dan memahami permasalahan yang dihadapi organisasi sebagai acuan bagi penelitian ini, serta mencari solusi yang akan dilakukan untuk mengatasi masalah yang ada. Dalam mengidentifikasi masalah diperlukan penjelasan masalah yang dihadapi organisasi yang tersaji dalam bentuk latar belakang dan rumusan masalah, serta solusi atas masalah yang dihadapi yang tersaji dalam bentuk tujuan dan manfaat. Kesemua hal tersebut dibatasi dengan batasan masalah agar penelitian tetap fokus namun berbobot terhadap masalah yang dibahas. Hasil dari identifikasi masalah sudah tertuang pada BAB I.

#### **3.1.2. Studi Literatur**

Studi literatur dilakukan untuk menambah pemahaman terhadap permasalahan yang diangkat melalui pengumpulan dan pembelajaran dari berbagai macam sumber literatur. Sumber yang digunakan dalam penelitian ini didapat melalui *internet* (jurnal, artikel, laporan, pedoman, *e-book*) maupun perpustakaan (penelitian ilmiah, pedoman dan buku). Pedoman utama penelitian ini adalah dokumen SNI ISO/IEC 27001:2013 (BSN, 2013a), SNI ISO/IEC 27002:2014 (BSN, 2014b), dan SNI ISO/IEC 27005:2013 (BSN, 2013c) serta sumber-sumber lainnya. Hasil dari studi literatur sudah tertuang pada BAB II.

### **3.2. Pengumpulan Data**

#### **3.2.1. Peninjauan Dokumen**

Peninjauan dokumen dilakukan untuk memahami tentang organisasi secara mendalam melalui pengumpulan dan pembelajaran dokumen yang diperlukan milik organisasi. Hal pertama yang dilakukan adalah memahami organisasi secara umum melalui peninjauan informasi berupa profil, visi, misi dan struktur organisasi, dimana informasi ini sudah tertuang pada BAB II dibagian 2.1. Setelah itu memahami kondisi keamanan informasi di organisasi melalui peninjauan dokumen pendukung berupa

kebijakan, prosedur, instruksi kerja, hukum/peraturan yang berlaku, *website* organisasi, topologi jaringan, rencana penerapan keamanan informasi, dan audit/laporan manajemen resiko keamanan informasi sebelumnya.

### **3.2.2. Wawancara**

Wawancara dilakukan untuk memahami suatu kejadian atau fakta melalui tanya jawab kepada narasumber yang terpercaya. Wawancara untuk mengetahui kondisi dan kebutuhan keamanan informasi di organisasi dilakukan saat aktifitas penetapan konteks, penetapan kebijakan SMKI, pelaksanaan analisis kesenjangan dan penilaian resiko.

### **3.2.3. Observasi**

Observasi dilakukan untuk memperoleh gambaran kondisi saat ini melalui pengamatan secara langsung terhadap aktifitas bisnis, aset dan kontrol keamanan dilingkungan organisasi yang berada pada ruang lingkup SMKI. Observasi juga dilakukan untuk mengklarifikasi dan melengkapi beberapa informasi yang didapat dari hasil aktifitas peninjauan dokumen dan wawancara.

## **3.3. Penetapan Konteks**

### **3.3.1. Pengaturan Kriteria Resiko**

Aktifitas ini dilakukan untuk menyusun kriteria resiko yang sesuai dengan kebutuhan organisasi melalui wawancara dengan pihak manajemen tentang pendefinisian beberapa batasan nilai level resiko. Kriteria resiko yang disusun mendefinisikan skala nilai level resiko yang tidak dapat diterima dan yang dapat diterima. Contoh dari kriteria resiko dapat dilihat pada Tabel 2.8.

### **3.3.2. Pengaturan Kriteria Dampak dan Kemungkinan**

Aktifitas ini dilakukan untuk menetapkan skala nilai berdasarkan kriteria dampak dan kemungkinan yang sesuai dengan kebutuhan organisasi melalui

wawancara dengan pihak manajemen. Contoh dari skala nilai dampak dapat dilihat pada Tabel 2.14 dan skala nilai kemungkinan dapat dilihat pada Tabel 2.15.

### **3.3.3. Pendefinisian Ruang Lingkup dan Batasan**

Aktifitas ini dilakukan untuk menggambarkan secara jelas ruang lingkup SMKI melalui wawancara dengan pihak manajemen dan peninjauan dokumen. Yang akan didefinisikan pada ruang lingkup SMKI adalah karakteristik atau proses bisnis organisasi, departemen/unit fungsional yang terlibat, topologi jaringan yang digunakan, lokasi dimana ruang lingkup berada, dan yang tidak termasuk didalam ruang lingkup.

### **3.3.4. Penetapan Peran dan Tanggung Jawab**

Aktifitas ini dilakukan untuk menentukan siapa yang berperan dan bertanggung jawab untuk mengelola SMKI melalui penetapan tim pengelola SMKI. Susunan tim pengelola SMKI ditetapkan melalui wawancara dengan pihak manajemen serta pemetaan struktur tim pengelola SMKI yang dibutuhkan SNI ISO/IEC 27001 dengan struktur organisasi yang berlaku di organisasi.

### **3.4. Pengusulan Kebijakan SMKI**

Aktifitas ini dilakukan untuk mengusulkan kebijakan SMKI yang nantinya akan menjadi acuan untuk tahapan selanjutnya. Yang didefinisikan pada kebijakan SMKI adalah hasil wawancara dengan pihak manajemen (seperti sasaran SMKI serta hasil yang diharapkan), kriteria resiko yang sudah diatur, ruang lingkup SMKI yang sudah didefinisikan, serta peran dan tanggung jawab yang sudah ditetapkan.

### **3.5. Pelaksanaan Analisis Kesenjangan**

Aktifitas ini dilakukan untuk mengetahui seberapa jauh tingkat kesenjangan keamanan informasi (baik sebelum maupun sesudah) pada organisasi terhadap SNI ISO/IEC 27001. Aktifitas yang dilakukan saat analisis kesenjangan adalah menentukan kesesuaian/kepatuhan organisasi terhadap setiap kontrol keamanan yang

ada pada *Annex A* didalam SNI ISO/IEC 27001 melalui aktifitas pengumpulan data. Yang perlu diperhatikan adalah tidak semua kontrol keamanan pada *Annex A* dapat diterapkan oleh organisasi dikarenakan ruang lingkup dan batasan yang telah didefinisikan, ataupun perbedaan proses bisnis yang dilakukan di organisasi. Contoh topik pertanyaan yang dapat digunakan saat analisis kesenjangan yang berasal dari kontrol keamanan pada *Annex A* dapat dilihat pada Tabel 3.1.

Tabel 3.1 Contoh Topik Pertanyaan Analisis Kesenjangan dari *Annex A*

| Kontrol Keamanan                                   | Ekstrasi Pertanyaan                                                                                                                                                                                                                                              |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.8.1.2<br>Kepemilikan asset                       | <b>Deskripsi:</b> Setiap aset yang dikelola pada inventaris harus dimiliki.<br><b>Pertanyaan:</b> Apakah setiap aset yang dikelola pada inventaris terdapat pemiliknya?                                                                                          |
| A.12.1.1<br>Mendokumentasikan prosedur operasional | <b>Deskripsi:</b> Prosedur operasional harus didokumentasikan dan dibuat tersedia bagi seluruh pengguna yang membutuhkan.<br><b>Pertanyaan:</b> Apakah prosedur operasional didokumentasikan dan dibuat tersedia bagi seluruh seluruh pengguna yang membutuhkan? |
| A.13.1.1<br>Kontrol jaringan                       | <b>Deskripsi:</b> Jaringan harus dimanajemen dan dikontrol untuk melindungi informasi pada sistem dan aplikasi.<br><b>Pertanyaan:</b> Apakah jaringan dimanajemen dan dikontrol untuk melindungi informasi pada sistem dan aplikasi?                             |

Sumber: BSN, 2013a; Candiwan, 2014

Jawaban dari setiap topik pertanyaan pada Tabel 3.1 bisa didapat melalui hasil wawancara dengan narasumber (baik jawaban yang berasal dari topik pertanyaan atau tidak), peninjauan dokumen dan/atau hasil temuan dari aktifitas observasi. Jumlah pertanyaan bisa juga bertambah untuk konfirmasi tambahan dan memperjelas jawaban yang didapat. Setelah itu menentukan kondisi organisasi menggunakan klasifikasi tingkat kepatuhan pada Tabel 3.2 terhadap setiap kontrol keamanan yang ada pada *Annex A*.

Tabel 3.2      Klasifikasi Tingkat Kepatuhan terhadap SNI ISO/IEC 27001

| <b>Klasifikasi</b>         | <b>Keterangan</b>                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <i>Compliant</i>           | Organisasi patuh secara keseluruhan dengan area tertentu pada SNI ISO/IEC 27001.                                         |
| <i>Partially compliant</i> | Organisasi telah melakukan berbagai cara untuk patuh, namun masih memerlukan pekerjaan tambahan yang harus dijalankan.   |
| <i>Non-compliant</i>       | Organisasi tidak memiliki beberapa kontrol keamanan ditempat untuk memenuhi beberapa persyaratan dari SNI ISO/IEC 27001. |
| <i>Not applicable</i>      | Organisasi telah ditinjau dan diidentifikasi bahwa kontrol keamanan tidak dapat diterapkan.                              |

Sumber: Deloitte, 2009

Setelah itu dilakukan perhitungan penjumlahan terhadap kontrol keamanan pada *Annex A* yang diklasifikasikan telah *compliant*, *partially compliant*, *non-compliant* dan *not applicable*, lalu perhitungan persentase untuk menghasilkan seberapa besar tingkat kesenjangan yang ada. Yang perlu diperhatikan adalah analisis kesenjangan tidak mengukur keefektifan kontrol keamanan terhadap resiko, dimana untuk mengukur keefektifan kontrol keamanan hanya bisa menggunakan aktifitas manajemen resiko. Jadi bisa saja terdapat kontrol keamanan yang sudah *compliant* namun tidak efektif terhadap resiko dan perlu dilakukan rekomendasi. Aktifitas analisis kesenjangan dilakukan dua kali, yaitu sebelum penilaian resiko dan setelah perencanaan penanganan resiko.

### **3.6. Penilaian Resiko**

#### **3.6.1. Identifikasi Resiko**

Identifikasi resiko dilakukan untuk mengidentifikasi semua resiko yang dihadapi oleh organisasi didalam ruang lingkup SMKI. Identifikasi resiko yang akan dilakukan terdiri dari beberapa tahapan, yaitu:

## **1. Identifikasi aset**

Hal pertama yang dilakukan adalah mengidentifikasi semua aset kritis yang berfungsi sebagai pengolah, pengirim maupun media/penyimpanan informasi didalam ruang lingkup SMKI. Kritis dapat diartikan mengganggu proses bisnis jika terdapat gangguan/hambatan/ancaman pada aset tersebut. Berikut ini adalah pertanyaan saat mengidentifikasi aset:

- Apa saja aset kritis yang dimiliki oleh grup/departemen/unit fungsional anda?
- Siapakah pemilik aset dan pemilik resiko dari masing-masing aset tersebut?
- Berada dimanakah lokasi aset tersebut berada?

Jawaban dari pertanyaan disusun kedalam daftar inventaris aset beserta data tipe dari aset tersebut. Untuk beberapa aset tertentu akan dikelompokkan jika terlihat identik dan tidak perlu untuk diidentifikasi secara individual. Pemilik aset adalah orang yang memiliki tanggung jawab terhadap aset, sedangkan pemilik resiko adalah orang yang memiliki akuntabilitas untuk mengelola resiko yang muncul dari aset tersebut. Contoh hasil identifikasi aset dapat dilihat pada Tabel 3.3.

Tabel 3.3 Contoh Daftar Inventaris Aset

| Nomor Aset | Tipe Aset       | Aset                     | Pemilik Aset                | Pemilik Resiko | Lokasi              |
|------------|-----------------|--------------------------|-----------------------------|----------------|---------------------|
| AS1        | Informasi       | Data pengembangan produk | Staf R&D                    | Ketua R&D      | Departemen R&D      |
| AS2        | Perangkat keras | Komputer                 | Staf TIK                    | Ketua TIK      | Semua ruangan kerja |
| AS3        | Fasilitas fisik | Pusat data               | <i>Administrator server</i> | Ketua TIK      | Lantai 2            |
| ...        | ...             | ...                      | ...                         | ...            | ...                 |

Sumber: Contoh

## 2. Identifikasi ancaman

Setelah identifikasi aset, selanjutnya adalah mengidentifikasi semua ancaman yang mengganggu aspek keamanan informasi seperti *confidentiality*, *integrity* dan *availability* terhadap aset yang telah teridentifikasi. Berikut ini adalah pertanyaan saat mengidentifikasi ancaman:

- Apa saja ancaman/gangguan/hambatan terhadap aset tersebut yang anda ketahui atau yang anda curigai terjadi?

Jawaban dari pertanyaan disusun kedalam daftar ancaman beserta data aset yang terganggu, sumber ancamannya, dan aspek keamanan informasi yang terganggu (seperti *confidentiality*, *integrity*, dan/atau *availability*). Contoh hasil identifikasi ancaman dapat dilihat pada Tabel 3.4.

Tabel 3.4 Contoh Daftar Ancaman

| Nomor Ancaman | Sumber Ancaman           | Ancaman                   | Aspek CIA | Aset yang Terganggu |
|---------------|--------------------------|---------------------------|-----------|---------------------|
| AN1           | Bencana Alam             | Kebakaran                 | A         | AS2                 |
| AN2           | Ketidaksengajaan manusia | Penyebaran <i>malware</i> | C + I + A | AS1                 |
| AN3           |                          | Penyingkapan informasi    | C         | AS3                 |
| ...           | ...                      | ...                       | ...       | ...                 |

Sumber: Contoh

## 3. Identifikasi kontrol keamanan yang ada

Setelah identifikasi ancaman, selanjutnya adalah identifikasi kontrol keamanan pada ketiga area seperti *administrative*, *physical*, dan *technical* yang melindungi aset organisasi dari ancaman. Selain melakukan peninjauan dokumen, wawancara, dan observasi untuk mengidentifikasi kontrol keamanan, akan ditanyakan juga:

- Apa saja perangkat/prosedur/kebijakan/tindakan yang melindungi aset tersebut dari ancaman yang teridentifikasi?



Beberapa informasi yang didapat disusun kedalam daftar kontrol keamanan yang dikelompokkan kedalam ketiga area berikut deskripsi/keterangannya. Contoh hasil identifikasi kontrol keamanan dapat dilihat pada Tabel 3.5.

Tabel 3.5 Contoh Daftar Kelompok Kontrol Keamanan Saat Ini

| Kode                  | Kontrol Keamanan                    | Keterangan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Administrative</i> |                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| A1                    | Kebijakan Keamanan TIK (Lampiran B) | <ul style="list-style-type: none"> <li>• Tata cara penggunaan <i>password</i> (larangan memberikan ke pihak lain dan persyaratan minimum <i>password</i>).</li> <li>• Pelarangan penggunaan fasilitas TIK selain pekerjaan kantor.</li> <li>• Pelarangan dan ketentuan penyebaran data/informasi perusahaan.</li> <li>• Pelarangan dan ketentuan pemasangan perangkat lunak lain.</li> <li>• Ketentuan penggunaan media penyimpanan elektronik.</li> <li>• Menyebut sangsi jika tidak mematuhi kebijakan.</li> </ul> |
| A2                    | Prosedur jika terjadi kebakaran     | Tata cara bagaimana jika terjadi kebakaran, mulai dari penggunaan alat pemadam api sampai pelaporan ke petugas pemadam kebakaran.                                                                                                                                                                                                                                                                                                                                                                                    |
| A3                    | <i>Background check</i>             | Proses memastikan kesesuaian <i>curriculum vitae</i> pelamar beserta kelengkapannya (KTP/paspor, SKCK, sertifikat akademis/profesional). Selain itu dinilai juga kemampuan karyawan melalui wawancara dan tes tertulis.                                                                                                                                                                                                                                                                                              |
| <i>Physical</i>       |                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| P1                    | APAR                                | APAR (Alat Pemadam Api Ringan) yang berfungsi sebagai perangkat pemadam api <i>mobile</i> yang dipasang didalam ruangan pusat data maupun dibeberapa tempat didalam kantor.                                                                                                                                                                                                                                                                                                                                          |

|                  |                           |                                                                                                                                                 |
|------------------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| P2               | Perangkat pendeteksi asap | Perangkat yang dipasang didinding atau dilangit-langit sebagai pendeteksi asap yang akan berbunyi ( <i>alarm</i> ) jika terdapat indikasi asap. |
| <i>Technical</i> |                           |                                                                                                                                                 |
| T1               | <i>Anti-virus XYZ</i>     | Perangkat lunak yang dipasang disemua komputer yang memiliki fitur pencegah <i>virus</i> , <i>worm</i> , <i>spyware</i> .                       |
| T2               | <i>Firewall XYZ</i>       | Perangkat keras yang dipasang untuk mencegah gangguan dari luar bagi komputer dan <i>server</i> yang terhubung kedalam jaringan.                |
| ..               | ..                        | ...                                                                                                                                             |

Sumber: Contoh

#### 4. Identifikasi kerentanan

Setelah identifikasi kontrol keamanan, selanjutnya adalah identifikasi kerentanan pada keamanan informasi yang dapat dieksploitasi oleh ancaman, baik yang terdapat pada kebijakan, prosedur, desain, penerapan, dan kontrol keamanan lainnya didalam organisasi. Selain menggunakan hasil peninjauan dokumen, wawancara, dan observasi untuk mengidentifikasi kerentanan, akan ditanyakan juga:

- Apa saja penyebab/celah/kerentanan yang dapat menimbulkan terjadinya ancaman terhadap aset yang ada?

Beberapa informasi yang didapat disusun kedalam daftar kerentanan. Contoh hasil identifikasi kerentanan dapat dilihat pada Tabel 3.6.

Tabel 3.6 Contoh Daftar Kerentanan

| Kode | Kerentanan                                              | Keterangan                                                                                                                                                                                                                                                                                                |
|------|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V1   | Kurangnya perhatian terhadap informasi rahasia/sensitif | <ul style="list-style-type: none"> <li>• Dokumen/media penyimpanan elektronik yang berisi informasi rahasia/sensitif dibuang begitu saja.</li> <li>• Dokumen/media penyimpanan elektronik yang berisi informasi rahasia/sensitif ditaruh ditempat yang bisa dijangkau orang yang tidak berhak.</li> </ul> |

|     |                                                        |                                                                                                                                                                                               |
|-----|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V2  | <i>Anti-virus</i> yang ada tidak lagi efektif          | Masa aktif <i>anti-virus</i> yang dipasang pada beberapa komputer sudah kadaluarsa sehingga tidak bisa melindungi komputer dari <i>malware</i> .                                              |
| V3  | Perangkat lunak tidak ter- <i>patch</i> secara berkala | Beberapa sistem operasi dan perangkat lunak lain yang terpasang memiliki versi lama dibanding dengan versi terbaru yang dirilis vendor.                                                       |
| V4  | Kurangnya perhatian terhadap perangkat kebakaran       | Tidak ada yang melakukan pemeriksaan perangkat pendeteksi dan pemadam kebakaran secara rutin.                                                                                                 |
| V5  | Tidak adanya program kesadaran keamanan                | Pelatihan tentang keamanan informasi secara berkala tidak pernah diadakan. Pelatihan yang dilakukan hanya mencakup penggunaan sistem informasi untuk bekerja.                                 |
| V6  | Kesalahan pemberian hak akses                          | Terdapat hak akses yang diberikan karyawan bukan staf TIK pada beberapa komputer bersifat <i>administrator</i> .                                                                              |
| V7  | Tidak adanya perencanaan jika terjadi bencana          | Tidak tersedianya <i>disaster recovery plan</i> untuk mengembalikan kondisi kekeadaan semula dan <i>business continuity plan</i> untuk tetap menjalankan proses bisnis meski terjadi bencana. |
| ... | ...                                                    | ...                                                                                                                                                                                           |

Sumber: Contoh

### 3.6.2. Analisis Resiko

Analisis resiko dilakukan untuk menganalisis resiko yang telah teridentifikasi menggunakan metodologi kualitatif, dimana nilai yang diberikan pada dampak dan kemungkinan menggunakan sistem pemeringkatan. Analisis resiko yang akan dilakukan terdiri dari beberapa tahapan, yaitu:

#### 1. Penilaian dampak dan kemungkinan

Hal pertama yang dilakukan adalah menentukan nilai dampak dan nilai kemungkinan dari suatu resiko. Nilai dampak adalah besarnya kerusakan/kerugian jika ancaman terjadi pada aset, sedangkan nilai kemungkinan adalah besarnya

kemungkinan terjadinya ancaman tersebut. Berikut ini adalah pertanyaan saat menilai dampak dan kemungkinan:

- Menurut anda seberapa besar nilai dampak yang diterima jika ancaman tersebut terjadi berdasarkan skala nilai dampak?
- Menurut anda seberapa besar nilai kemungkinan dari ancaman tersebut berdasarkan skala nilai kemungkinan?

Saat penilaian dampak, perlu dipertimbangkan peringkat nilai dampak dari ancaman, apakah *very low* (1), *low* (2), *medium* (3), *high* (4) atau *very high* (5) berdasarkan skala nilai dampak. Begitu juga saat penilaian kemungkinan, perlu dipertimbangkan peringkat nilai kemungkinan terjadinya ancaman, apakah *rare* (1), *unlikely* (2), *possible* (3), *likely* (4), *certain* (5) berdasarkan skala nilai kemungkinan.

## **2. Menentukan level resiko**

Setelah penilaian dampak dan kemungkinan, selanjutnya adalah menentukan level resikonya menggunakan metode perkalian antara nilai dampak dengan nilai kemungkinan. Misalnya resiko penyingkapan informasi yang memiliki nilai dampak 4 dan nilai kemungkinan 3, maka level resikonya adalah 12. Setelah itu memetakan keseluruhan hasil identifikasi resiko dan analisis resiko yang saling berhubungan kedalam lembar kerja penilaian resiko yang dapat dilihat pada Tabel 3.7.

Tabel 3.7 Contoh Lembar Kerja Penilaian Resiko

| Kode | Aset | Ancaman | Kontrol Keamanan | Kerentanan     | Aspek CIA | Probabilitas | Dampak | Level Resiko |
|------|------|---------|------------------|----------------|-----------|--------------|--------|--------------|
| R1   | AS1  | AN3     | A2, A3           | V1, V5         | C         | 4            | 3      | 12           |
| R2   | AS2  | AN2     | A2, T1, T2       | V2, V3, V5, V6 | CIA       | 4            | 5      | 20           |
| R3   | AS3  | AN1     | A3, P1, P2       | V4, V7         | A         | 5            | 1      | 5            |
| ...  | ...  | ...     | ...              | ...            | ...       | ...          | ...    | ...          |

Sumber: Contoh

### 3.6.3. Evaluasi Resiko

Evaluasi resiko dilakukan untuk membuat keputusan tindakan kedepan, seperti resiko mana yang perlu ditangani serta prioritas dari keputusan tersebut. Dalam aktifitas ini, dilakukan perbandingan level resiko pada masing-masing resiko pada lembar kerja penilaian resiko dengan kriteria resiko yang sudah ditetapkan, lalu dibuat keputusan apakah resiko diterima atau tidak diterima. Misalnya resiko penyingkapan informasi yang memiliki level resiko 12 tidak dapat diterima dan harus ditangani. Sedangkan resiko kebakaran yang memiliki level resiko 4 dapat diterima organisasi tanpa perlakuan apapun. Untuk penentuan prioritas, bisa saja terdapat beberapa resiko yang memiliki ancaman yang sama dan level resiko yang sama namun berbeda aset yang terkena resiko. Jika hal ini terjadi, maka resiko tersebut dikelompokkan menjadi satu untuk penomoran prioritasnya. Tabel 3.8 berisikan contoh evaluasi resiko yang sudah diurutkan berdasarkan prioritas menggunakan contoh kriteria resiko pada Tabel 2.8.

Tabel 3.8 Contoh Evaluasi Resiko

| Prioritas | No Resiko | Resiko                    | Level Resiko |                | Keputusan      |
|-----------|-----------|---------------------------|--------------|----------------|----------------|
| 1         | R2        | Penyebaran <i>malware</i> | 20           | <i>Extreme</i> | Tidak diterima |
| 2         | R1        | Penyingkapan informasi    | 12           | <i>High</i>    | Tidak diterima |
| 3         | R3        | Kebakaran                 | 5            | <i>Low</i>     | Diterima       |
| ...       | ...       | ...                       | ...          | ...            | ...            |

Sumber: Contoh

## 3.7. Perencanaan Penanganan Resiko

### 3.7.1. Pemilihan Penanganan Resiko

Aktifitas ini dilakukan untuk memilih penanganan keseluruhan resiko berdasarkan hasil evaluasi resiko pada Tabel 3.6. Pemilihan kontrol keamanan

mengacu pada *Annex A* didalam SNI ISO/IEC 27001:2013, dimana setiap kontrol keamanan yang dipilih untuk menangani resiko disesuaikan dengan sasaran kontrol keamanan dan deskripsi kontrol keamanan tersebut. Hal yang harus diperhatikan adalah bisa saja terdapat suatu resiko memerlukan beberapa kontrol keamanan untuk penanganan risikonya.

Selain memilih kontrol keamanan, terdapat juga pilihan lain untuk menangani resiko, seperti menghindari resiko dengan cara menghindari aktifitas atau kondisi yang dapat menimbulkan resiko, membagi resiko dengan cara mengkontrak pihak ketiga yang mampu menangani resiko, atau menerima resiko tanpa melakukan tindakan lebih lanjut. Contoh pemilihan penanganan resiko yang sudah diurutkan berdasarkan prioritas besarnya level resiko dapat dilihat pada Tabel 3.9.

Tabel 3.9 Contoh Pemilihan Penanganan Resiko

| No Resiko | Resiko                                                                                                                                                                                                                                                                                                                                       | Pemilihan Penanganan     |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| R2        | Penyebaran <i>malware</i>                                                                                                                                                                                                                                                                                                                    | <i>Risk Modification</i> |
|           | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.2.1. Kontrol terhadap <i>malware</i>.</li> <li>• A.12.6.1. Manajemen kerentanan teknis.</li> </ul> |                          |
| R1        | Penyingkapan informasi                                                                                                                                                                                                                                                                                                                       | <i>Risk Modification</i> |
|           | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.8.2.1. Klasifikasi informasi.</li> <li>• A.8.3.2. Pembuangan media.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> </ul>                        |                          |

|     |           |                       |
|-----|-----------|-----------------------|
| R3  | Kebakaran | <i>Risk Retention</i> |
| ... | ...       | ...                   |

Sumber: Contoh

### 3.7.2. Penetapan Kontrol Keamanan dan Sasarannya

Aktifitas ini dilakukan untuk menguraikan lebih jelas beberapa kontrol keamanan yang sudah dipilih untuk menangani resiko. Hal yang dapat diuraikan seperti kebijakan, prosedur, perangkat keras/lunak, dan kontrol keamanan lainnya yang dibutuhkan sesuai panduan SNI ISO/IEC 27002:2013. Selain itu sasaran keamanan informasi juga diuraikan disetiap kontrol keamanan yang ada. Contoh penetapan kontrol keamanan beserta sasaran keamanan informasi dapat dilihat pada Tabel 3.10.

Tabel 3.10 Contoh Penetapan Kontrol Keamanan dan Sasaran Keamanan Informasi

| No<br><i>Annex</i> | Kontrol Keamanan                                                                                                                                                                                      | Sasaran Keamanan Informasi                                                      |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
|                    | Kontrol Keamanan yang Ditetapkan                                                                                                                                                                      |                                                                                 |
| A.5.1.1            | Kebijakan keamanan informasi                                                                                                                                                                          | Semua kebijakan tersedia dan disosialisasikan keseluruh pihak yang terkait.     |
|                    | <b><i>Administrative:</i></b> <ul style="list-style-type: none"> <li>• Pembuatan kebijakan Klasifikasi Informasi (A.8.2.1).</li> <li>• Pembaharuan dokumen Kebijakan Keamanan TIK.</li> </ul>         |                                                                                 |
| A.7.2.2            | Kepedulian, pendidikan dan pelatihan keamanan informasi                                                                                                                                               | Semua karyawan didalam ruang lingkup sudah mengikuti program kesadaran keamanan |
|                    | <b><i>Administrative:</i></b> <ul style="list-style-type: none"> <li>• Melakukan sosialisasi terhadap kebijakan dan prosedur tentang keamanan informasi yang ada dan yang akan diterapkan.</li> </ul> |                                                                                 |



|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>• Menjadwalkan dan melaksanakan program kesadaran keamanan secara berkala setidaknya 6 bulan sekali.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                       |
| A.8.2.1  | Klasifikasi informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Semua aset bertipe informasi sudah diklasifikasikan berdasarkan bentuk dan kesensitifannya.           |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Mendokumentasikan klasifikasi kerahasiaan informasi berdasarkan tingkatan publik, internal dan rahasia untuk setiap data yang diolah sistem informasi (<i>database</i>), data yang dibuat sistem (<i>log, backup, file konfigurasi, ID login</i>), maupun data yang diolah manual baik berbentuk <i>file (worksheet, spreadsheet)</i> atau dokumen kertas.</li> </ul>                                                                                                                                                                                                                                                                                                    |                                                                                                       |
| A.8.3.2  | Pembuangan media                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Semua informasi sensitif berbentuk dokumen dan <i>file</i> elektronik dibuang sesuai dengan prosedur. |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Membuang informasi berbentuk dokumen dan <i>file</i> elektronik sesuai prosedur dan perangkat yang tersedia.</li> <li>• Mendokumentasikan prosedur pembuangan informasi yang berisikan langkah-langkah dalam pembuangan informasi sensitif baik yang berbentuk dokumen maupun tersimpan pada media penyimpanan elektronik.</li> </ul> <p><b>Physical:</b></p> <ul style="list-style-type: none"> <li>• Membeli perangkat penghancur/<i>shedder</i> kertas.</li> </ul> <p><b>Technical:</b></p> <ul style="list-style-type: none"> <li>• Memasang perangkat lunak <i>file shedder</i> untuk menghapus informasi secara aman pada media penyimpanan elektronik.</li> </ul> |                                                                                                       |
| A.12.1.1 | Mendokumentasikan prosedur operasional                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Semua prosedur tersedia dan disosialisasikan keseluruh karyawan yang terkait.                         |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Pembuatan prosedur Pembuangan Informasi (A.8.3.2).</li> <li>• Pembuatan prosedur Manajemen Kerentanan Teknis (A.12.1.2).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                       |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                   |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| A.12.2.1 | Kontrol terhadap <i>malware</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Menurunkan jumlah insiden <i>malware</i> sebanyak 50% dibanding tahun sebelumnya. |
|          | <b>Technical:</b> <ul style="list-style-type: none"> <li>• Membeli lisensi <i>anti-virus</i> baru untuk komputer yang sudah memasuki masa kadaluarsa atau menggunakan <i>anti-virus</i> yang berlisensi <i>freeware</i> agar tidak ada masalah lisensi lagi.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                   |
| A.12.6.1 | Manajemen kerentanan teknis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Versi perangkat lunak harus sama dengan versi rilis terbaru.                      |
|          | <b>Administrative:</b> <ul style="list-style-type: none"> <li>• Mengawasi kerentanan baru berdasarkan klasifikasi melalui forum/<i>website</i> keamanan informasi (seperti NIST National Vulnerability Database di <a href="https://nvd.nist.gov/">https://nvd.nist.gov/</a>, Offensive Security's Exploit Database Archive di <a href="https://www.exploit-db.com/">https://www.exploit-db.com/</a>, atau CVE di <a href="http://www.cvedetails.com/">http://www.cvedetails.com/</a>) dan mengawasi rilis terbaru <i>patch/update</i> dari <i>website</i> vendor perangkat lunak secara berkala dan terjadwal.</li> <li>• Menguji perbaharuan <i>patch</i> yang ada. Jika terdapat masalah maka menggunakan versi lama dan melakukan , jika tidak maka akan dipasang kedalam sistem.</li> <li>• Melakukan perekaman riwayat aktifitas pemasangan <i>patch</i> yang dilakukan baik yang berhasil maupun yang tidak berhasil.</li> <li>• Mendokumentasikan prosedur manajemen kerentanan teknis yang berisikan langkah-langkah dalam manajemen <i>patch</i> mulai dari identifikasi sampai pengujian <i>patch</i> yang akan dipasang dan penyediaan informasi untuk manajemen insiden (termasuk kerentanan yang telah teridentifikasi namun belum memenuhi penanganan yang tepat).</li> </ul> <b>Technical:</b> <ul style="list-style-type: none"> <li>• Memasang sistem manajemen <i>patch</i> untuk mengelola pemasangan <i>patch</i> pada semua sistem.</li> </ul> |                                                                                   |
| ..       | ...                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                   |

Sumber: Contoh

Contoh hubungan antara beberapa resiko yang tidak diterima dengan domain kontrol keamanan yang dipilih untuk menangani masing-masing resiko tersebut dapat dilihat pada Tabel 3.11.

Tabel 3.11 Hubungan Kelompok Resiko dengan Domain Kontrol Keamanan SNI ISO/IEC 27001

| No Annex | Domain Kontrol Keamanan      | Kelompok Resiko                                                                                                   |
|----------|------------------------------|-------------------------------------------------------------------------------------------------------------------|
| A.5      | Kebijakan keamanan informasi | • Semua resiko                                                                                                    |
| A.7      | Keamanan sumber daya manusia | <ul style="list-style-type: none"> <li>• Penyebaran <i>malware</i>.</li> <li>• Penyingkapan informasi.</li> </ul> |
| A.8      | Manajemen aset               | • Penyingkapan informasi.                                                                                         |
| A.12     | Keamanan operasional         | <ul style="list-style-type: none"> <li>• Penyebaran <i>malware</i>.</li> <li>• Penyingkapan informasi.</li> </ul> |

Sumber: Contoh

### 3.8. Perancangan Dokumen SMKI

Setelah penanganan resiko, selanjutnya melakukan perancangan dokumen SMKI yang berada dicakup proses *plan* pada proses *PDCA*. Beberapa dokumen SMKI yang dibuat adalah ruang lingkup SMKI, kebijakan SMKI, proses penilaian resiko, proses penanganan resiko, *statement of applicability*, dan sasaran keamanan informasi. Dokumen SMKI yang dibuat bersumber dari beberapa aktifitas yang dilakukan sebelumnya.

### 3.9. Pembuatan Kesimpulan dan Saran

Aktifitas ini dilakukan untuk memberikan kesimpulan dari hasil penelitian yang dilakukan, serta memberikan saran untuk penelitian selanjutnya dan perbaikan terhadap penelitian yang dibahas.

### 3.10. Rencana dan Jadwal Kerja Penelitian

Dalam penyusunan penelitian ini, direncanakan waktu yang diperlukan sekitar 4 bulan. Rincian aktifitas beserta jadwal dalam penelitian ini dapat dilihat pada Tabel 3.12.

Tabel 3.12 Rencana dan Jadwal Kerja Penelitian

| Kegiatan                                   | Bulan I |  |  |  | Bulan II |  |  |  | Bulan III |  |  |  | Bulan IV |  |  |  |
|--------------------------------------------|---------|--|--|--|----------|--|--|--|-----------|--|--|--|----------|--|--|--|
| Pendahuluan                                |         |  |  |  |          |  |  |  |           |  |  |  |          |  |  |  |
| Pengumpulan data                           |         |  |  |  |          |  |  |  |           |  |  |  |          |  |  |  |
| Penetapan konteks                          |         |  |  |  |          |  |  |  |           |  |  |  |          |  |  |  |
| Pengusulan kebijakan SMKI                  |         |  |  |  |          |  |  |  |           |  |  |  |          |  |  |  |
| Pelaksanaan analisis kesenjangan (sebelum) |         |  |  |  |          |  |  |  |           |  |  |  |          |  |  |  |
| Penilaian resiko                           |         |  |  |  |          |  |  |  |           |  |  |  |          |  |  |  |
| Perencanaan penanganan resiko              |         |  |  |  |          |  |  |  |           |  |  |  |          |  |  |  |
| Pelaksanaan analisis kesenjangan (sesudah) |         |  |  |  |          |  |  |  |           |  |  |  |          |  |  |  |
| Perancangan dokumen SMKI                   |         |  |  |  |          |  |  |  |           |  |  |  |          |  |  |  |
| Pembuatan kesimpulan dan saran             |         |  |  |  |          |  |  |  |           |  |  |  |          |  |  |  |

Sumber: Penelitian

*Halaman ini sengaja dikosongkan*

## **BAB IV**

### **HASIL PENELITIAN**

BAB ini membahas tentang hasil dari penelitian yang dilakukan menggunakan setiap tahapan pada metode penelitian yang sudah dijelaskan sebelumnya. Beberapa tahapan yang menghasilkan dokumen yang lebih detail akan ditempatkan pada bagian lampiran.

#### **4.1. Pengumpulan Data**

##### **4.1.1. Peninjauan Dokumen**

Hasil peninjauan dokumen yang didapatkan pada penelitian ini digunakan untuk menunjang aktifitas pelaksanaan analisis kesenjangan. Dokumen yang dikumpulkan adalah kebijakan yang terkait dengan penelitian dan berada didalam ruang lingkup SMKI, prosedur dan instruksi kerja yang berada didalam dokumen ISO 9000 milik DPTSI-ITS, *website* DPTSI-ITS (<https://dptsi.its.ac.id/>), topologi jaringan, *user guide*, *developer guide*, dan lainnya.

##### **4.1.2. Wawancara**

Hasil wawancara yang didapatkan pada penelitian ini digunakan untuk menunjang aktifitas penetapan konteks, pengusulan kebijakan SMKI, pelaksanaan analisis kesenjangan, dan penilaian resiko. Untuk aktifitas penetapan konteks dan pengusulan kebijakan SMKI, narasumber yang dipilih adalah Direktur DPTSI-ITS. Sedangkan untuk aktifitas pelaksanaan analisis kesenjangan, narasumber yang dipilih adalah pihak yang terkait dengan topik pertanyaan analisis kesenjangan pada SNI ISO/IEC 27001:2013 berdasarkan dengan tugas dan jabatan yang diemban di DPTSI-ITS. Narasumber yang dipilih berasal dari masing-masing Subdit di DPTSI-ITS, semua Kasubdit di DPTSI-ITS, Direktur DPTSI-ITS, Direktorat Sarana dan Prasarana (untuk masalah kabel), dan Direktorat SDM dan Organisasi (untuk masalah SDM).

Hasil wawancara untuk pelaksanaan analisis kesenjangan berikut pertanyaannya dapat dilihat pada Lampiran C

Untuk aktifitas penilaian resiko, narasumber yang dipilih untuk menilai resiko pada aset adalah Kasubdit dari masing-masing Subdit, sedangkan untuk aset orang (SDM) adalah Direktur DPTSI-ITS. Penilaian resiko yang ada pada aset di Subdit Infrastruktur & Keamanan Teknologi Informasi dilakukan oleh bapak Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D., penilaian resiko yang ada pada aset di Subdit Pengembangan Sistem Informasi dilakukan oleh ibu Anny Yuniarti, S.Kom., M.Comp.Sc., penilaian resiko yang ada pada aset di Subdit Pelayanan Teknologi dan Sistem Informasi dilakukan oleh Hanim Maria Astuti, S.Kom., M.Sc., dan penilaian resiko yang ada pada aset orang dilakukan oleh Dr.Eng. Febriliyan Samopa, S.Kom., M.Kom. Hasil wawancara untuk penilaian resiko dapat dilihat pada Lampiran I.

#### **4.1.3. Observasi**

Hasil observasi yang didapatkan pada penelitian ini digunakan untuk menunjang aktifitas pelaksanaan analisis kesenjangan. Semua bukti dari hasil observasi dapat dilihat pada beberapa gambar di Lampiran F. Observasi yang sudah dilakukan adalah mengklarifikasi dan melengkapi beberapa informasi yang didapat dari hasil aktifitas peninjauan dokumen dan wawancara. Contohnya observasi yang dilakukan berdasarkan hasil wawancara dengan bapak Satriyo Wicaksono, S.Kom. dari Subdirektorat Infrastruktur & Keamanan Teknologi Informasi yang menyatakan terdapatnya perlindungan berlapis pada jaringan yang menggunakan CISCO ASA Firewall (A.13.1.1). Untuk membuktikan adanya CISCO ASA Firewall dari hasil wawancara dilakukan observasi secara langsung yang dapat dilihat pada Gambar F.124 dan Gambar F.125 di Lampiran F.

Namun tidak semua hasil peninjauan dokumen dan wawancara memerlukan aktifitas observasi. Hal ini bisa dikarenakan hasil peninjauan dokumen dan wawancara bersifat prosedural yang tidak terekam pelaksanaannya, tidak terdapat kontrol keamanan yang dimaksud, atau tidak mungkin dilakukan observasi secara langsung

(baik disebabkan masalah privasi atau tingkat kesulitannya). Berikut ini adalah beberapa contoh tersebut:

1. Contoh untuk yang bersifat prosedural yang tidak terekam pelaksanaannya berdasarkan hasil wawancara dengan bapak Satriyo Wicaksono, S.Kom. dari Subdirektorat Infrastruktur & Keamanan Teknologi Informasi yang menyatakan terdapatnya diskusi ilmu tentang analisa dan penanganan insiden keamanan informasi untuk mengurangi dampak dan kemungkinan insiden kedepan (A.16.1.6). Karena DPTSI-ITS tidak merekam setiap aktifitas tersebut atau sudah terekam tapi tidak bisa ditemukan ketika dibutuhkan, maka hal ini tidak bisa diobservasi.
2. Contoh untuk tidak terdapatnya kontrol keamanan yang dimaksud berdasarkan hasil wawancara dengan ibu Widiyaningsih, S.Kom. dari Direktorat Pelayanan Teknologi dan Sistem Informasi yang menyatakan tidak adanya daftar aset yang perlu dijaga hak kekayaan intelektualnya di DPTSI-ITS (A.18.1.2).
3. Contoh untuk tidak memungkinkan dilakukan observasi berdasarkan hasil wawancara dengan bapak Ardi Purwono dari Direktorat Sarana dan Prasarana yang menyatakan bahwa jalur kabel dilindungi oleh U-Ditch (A.11.2.3). Hal ini tidak bisa diklarifikasikan secara langsung apakah setiap jalur kabel memang dilindungi oleh U-Ditch, jika tidak dilakukan penggalian pada jalur kabel tersebut. Untuk masalah konfigurasi jaringan, konfigurasi sistem di *server*, atau yang terkait kontrak dengan pihak ketiga tidak bisa observasi dikarenakan privasi dari pihak DPTSI-ITS.

## **4.2. Penetapan Konteks**

### **4.2.1. Pengaturan Kriteria Resiko**

Kriteria resiko merupakan alat bantu yang berisikan beberapa batasan dengan sasaran level resiko untuk membantu aktifitas evaluasi resiko nantinya. Berdasarkan hasil wawancara dengan Direktur DPTSI-ITS, kriteria resiko yang disesuaikan dengan kebutuhan DPTSI-ITS dapat dilihat pada Tabel 4.1.



Tabel 4.1 Kriteria Resiko

| Level Resiko |               | Kegiatan                                                                 |
|--------------|---------------|--------------------------------------------------------------------------|
| 1 – 3        | <i>Low</i>    | Menerima resiko, dimana tidak perlu dilakukan rencana tindakan perbaikan |
| 4 – 6        | <i>Medium</i> | Tidak menerima resiko, dimana perlu dilakukan rencana tindakan perbaikan |
| 7 - 9        | <i>High</i>   |                                                                          |

Sumber: Penelitian

#### 4.2.2. Pengaturan Kriteria Dampak dan Kemungkinan

Skala nilai berdasarkan kriteria dampak dan kemungkinan merupakan alat bantu yang berisikan tingkatan nilai dan kriteria untuk membantu aktifitas penilaian resiko nantinya. Berdasarkan hasil wawancara dengan Direktur DPTSI-ITS, skala nilai dampak dan kemungkinan yang disesuaikan dengan kebutuhan DPTSI-ITS dapat dilihat pada Tabel 4.2 dan Tabel 4.3.

Tabel 4.2 Skala Nilai Dampak

| Nilai |               | Kriteria Dampak                   |
|-------|---------------|-----------------------------------|
| 1     | <i>Low</i>    | Gangguan layanan $\leq$ 2 hari.   |
| 2     | <i>Medium</i> | Gangguan layanan 3 - 6 hari.      |
| 3     | <i>High</i>   | Gangguan layanan $\geq$ 1 minggu. |

Sumber: Penelitian

Tabel 4.3 Skala Nilai Kemungkinan

| Nilai |                 | Kriteria Kemungkinan                                                                                                                                   |
|-------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | <i>Unlikely</i> | Kejadian dapat terjadi pada suatu waktu.                                                                                                               |
| 2     | <i>Possible</i> | <ul style="list-style-type: none"> <li>• Telah terjadi di masa lalu.</li> <li>• Kejadian mungkin kerap terjadi (berulang) pada suatu waktu.</li> </ul> |
| 3     | <i>Likely</i>   | Kejadian akan terjadi (berulang) pada sebagian besar keadaan.                                                                                          |

Sumber: Penelitian

Dampak yang ada di DPTSI-ITS jika terjadi insiden adalah lebih kearah gangguan layanan berdasarkan Tabel 4.2. Hal ini dikarenakan DPTSI-ITS merupakan unit pendukung dan fungsi utamanya adalah menyediakan layanan TIK dan pendukungnya didalam lingkungan ITS. Sedangkan untuk dampak finansial, DPTSI-ITS tidak menghitungnya dan merasakannya. Misalnya terdapat kerusakan perangkat jaringan akibat terjadi gangguan listrik dan memerlukan pembelian perangkat baru, maka semua urusan dialihkan ke ULP-ITS untuk urusan pengadaan dan BAUK-ITS untuk urusan pendanaan pengadaan. Jadi tidak ada dampak finansial atau dampak lainnya yang diterima oleh DPTSI-ITS.

#### 4.2.3. Pendefinisian Ruang Lingkup dan Batasan

Ruang lingkup SMKI merupakan parameter yang mendefinisikan cakupan dan batasan dari SMKI yang akan dibuat. Seperti yang dijelaskan sebelumnya bahwa ruang lingkup SMKI pada penelitian ini hanya mencakup layanan *email* yang dikelola oleh DPTSI-ITS. Ruang lingkup tidak mencakup untuk layanan *email* yang bekerjasama dengan Google (<https://mail2.its.ac.id>) dan Microsoft (<https://login.microsoftonline.com>). Spesifikasi dan konfigurasi yang digunakan pada *server* yang digunakan untuk Webmail ITS dapat dilihat pada Tabel 4.4.

Tabel 4.4 Spesifikasi dan Konfigurasi *Server* untuk Webmail ITS

| Spesifikasi            | Keterangan                                                                                                                    |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <i>Processor</i>       | Intel Xeon dengan 4 <i>core</i> @ 2,6 Ghz                                                                                     |
| <i>Memory</i>          | 3 GB ( <i>triple-channel</i> )                                                                                                |
| <i>Hardisk</i>         | 1 TB (konfigurasi <i>RAID</i> )                                                                                               |
| Sistem Operasi         | Linux Debian                                                                                                                  |
| Sistem Webmail ITS     | SquirrelMail (berjalan di Apache <i>HTTP Server</i> )                                                                         |
| Bahasa Pemrograman     | <i>HTML, CSS, PHP, JavaScript</i>                                                                                             |
| Halaman <i>website</i> | <a href="https://webmail.its.ac.id">https://webmail.its.ac.id</a>                                                             |
| <i>IP address</i>      | 202.46.129.20                                                                                                                 |
| Kuota <i>email</i>     | <ul style="list-style-type: none"> <li>• 200 MB untuk karyawan atau dosen.</li> <li>• 1 GB untuk karyawan teknisi.</li> </ul> |

Sumber: Penelitian

Berdasarkan hasil wawancara dengan pihak manajemen dan peninjauan dokumen, ruang lingkup SMKI yang disesuaikan dengan kebutuhan DPTSI-ITS adalah sebagai berikut:

1. Karakteristik atau proses bisnis yang terlibat didalam ruang lingkup SMKI adalah sebagai berikut:
  - DPTSI-ITS bertugas untuk mengelola, mengordinasikan, mengendalikan, dan mengembangkan berbagai fasilitas TIK disekitar lingkungan universitas Institut Teknologi Sepuluh Nopember.
  - Layanan *email* ITS digunakan dosen, mahasiswa dan karyawan untuk keperluan berkirim pesan, serta sebagai alat autentikasi ketika menggunakan fasilitas *internet* di aera kampus dan berbagai sistem informasi terpadu yang disediakan oleh DPTSI-ITS.
  - DPTSI-ITS memiliki 3 bentuk layanan *email* yaitu layanan *email* mandiri dari DPTSI-ITS (<https://webmail.its.ac.id>) yang khusus untuk karyawan dan dosen saja, layanan *email* yang bekerjasama dengan Google

(<https://mail2.its.ac.id>), dan layanan *email* yang bekerjasama dengan Microsoft (<https://login.microsoftonline.com>) yang khusus untuk pimpinan saja seperti Kasubag/Kasubdit sampai keatas. Karyawan dan dosen dapat memilih untuk migrasi ke layanan *email* yang bekerjasama dengan Google.

Home > Webmail ITS

### Login Webmail ITS

**Perhatian !**  
Mohon mengabaikan segala macam email yang meminta username dan password Anda yang mengatasnamakan Administrator ITS

Anda harus login terlebih dahulu untuk membaca atau mengirim email. Masukkan alamat email dan password anda.

Email: furqon14 @ mhs.mmt.its.ac.id

Password: .....

Login

#### Info Webmail

Seperti halnya aparat penegak hukum negara kita yang senantiasa mengajak masyarakat untuk turut serta menjaga keamanan lingkungan, kami juga mengajak para pengguna email (email ITS atau email yang lain) untuk selalu menjaga keamanan *account* masing-masing.

Setidaknya, kita dapat turut aktif menjaga keamanan *account* masing-masing dengan cara:

1. **Jangan pernah** menggunakan nama *account* anda sebagai kata sandi!
2. Jaga kerahasiaan kata sandi anda.
3. Secara rutin, ubahlah kata sandi anda.
4. Gunakan kata sandi yang sulit ditebak.

Ingat, tidak sepatutnya kita menuntut petugas HANSIP di kampung halaman bila rumah anda kemalingan saat anda tidur **tanpa mengunci pintu rumah** dengan baik. Hal yang sama berlaku juga untuk email anda :)

Beberapa fasilitas tambahan yang dapat anda gunakan dalam webmail ITS adalah:

1. **Lupa Login & Password** — Fasilitas ini bekerja layaknya permainan tebak-kata. Anda dapat memasukkan beberapa pertanyaan pada menu yang disediakan untuk kemudian ditanyakan kembali pada anda ketika anda kehilangan *password* anda. Bila anda memasukkan jawaban yang tepat, maka *password* anda akan di-*reset* [info]
- Mahasiswa aktif dapat pula melakukan perubahan *password* menggunakan NRP dan *password* FRS online. Gunakan fasilitas ini melalui *link* yang ada di sebelah kanan.
2. **html\_mail** — Mengirim email dalam format HTML [info]
3. **to-do reminder** — Daftar tugas yang harus anda selesaikan [info]

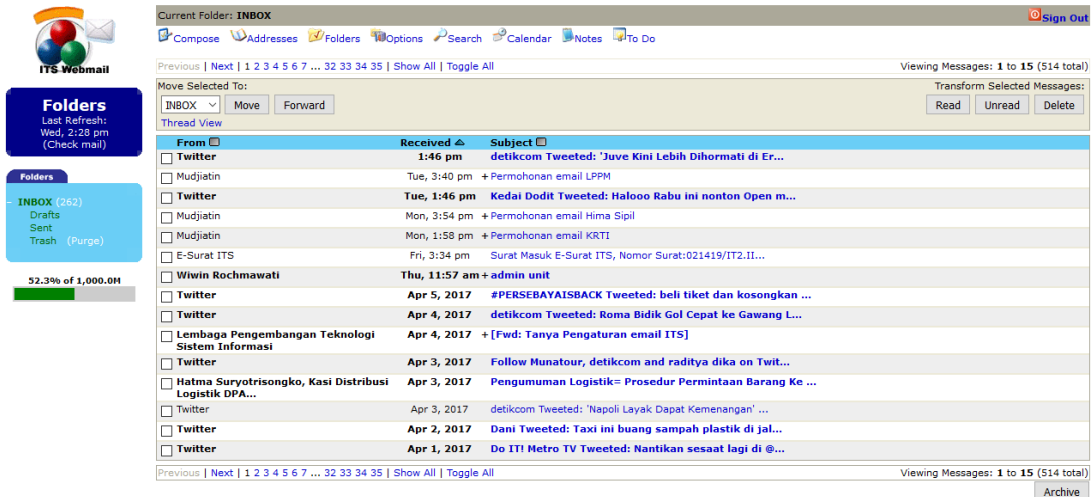
#### Layanan Lain

- Web ITS
- Web LPTSI
- Portal Google Apps For Edu
- Portal Software Lisensi ITS
- Portal Software GPL ITS
- Mirror ITS
- Direktori ITS

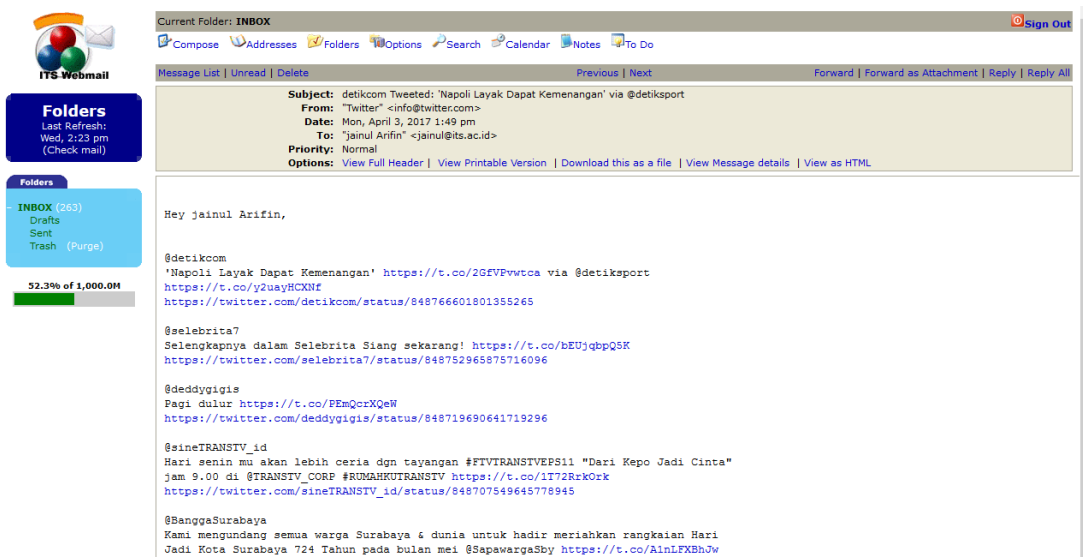
#### Informasi Email ITS

- Info Webmail
- Pendaftaran Mahasiswa
- Lupa Login & Password
- Ketentuan Layanan
- Domain Email
- Penggunaan Mail Client

Gambar 4.1 Halaman *Login* untuk Layanan *Email* Mandiri



Gambar 4.2 Halaman Awal untuk Layanan *Email* Mandiri



Gambar 4.3 Halaman Buka *Email* untuk Layanan *Email* Mandiri

2. Selain dari pihak manajemen, departemen/unit fungsional yang terlibat dalam ruang lingkup SMK I adalah sebagai berikut:

- Subdirektorat Infrastruktur & Keamanan Informasi yang bertugas terhadap jaringan dan koneksi antara klien/pengguna dengan *server* yang digunakan untuk *email* ITS.

- Subdirektorat Pelayanan Teknologi dan Sistem Informasi yang bertugas terhadap administrasi akun *email* ITS, seperti membuat akun, merubah *password* atau data akun, dan menghapus akun.
  - Subdirektorat Pengembangan Sistem Informasi yang bertugas terhadap pengembangan sistem dan antarmuka Webmail ITS.
3. Topologi jaringan yang ada di DPTSI-ITS dapat dilihat pada Gambar 4.4.

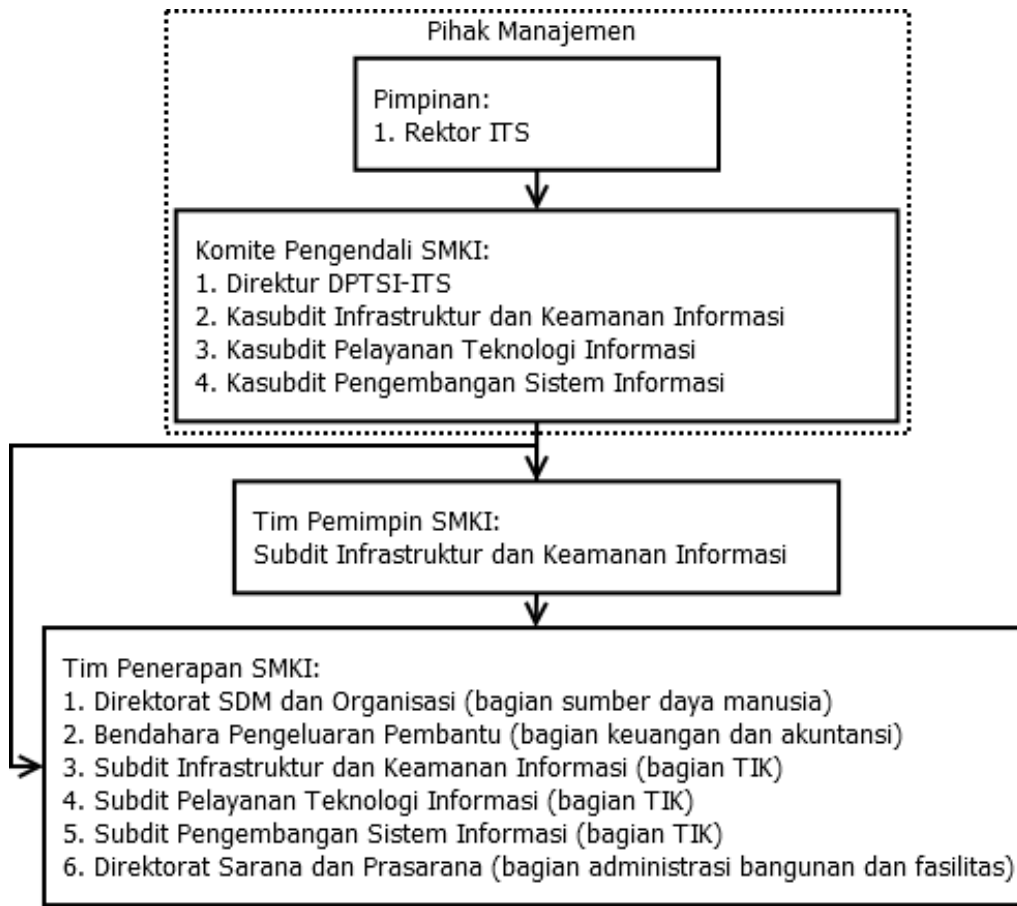


4. Lokasi tempat ruang lingkup berada adalah Direktorat Pengembangan Teknologi dan Sistem Informasi di gedung ITS *Research Center*, lantai 3, Sukolilo, Surabaya 60111.
5. Yang tidak termasuk kedalam ruang lingkup SMKI adalah:
  - Layanan *email* yang dikelola mandiri oleh jurusan/unit lain di ITS ataupun layanan *email* yang bekerjasama dengan Google dan Microsoft.
  - *Server* yang dikelola oleh DPTSI-ITS yang tidak berkaitan dengan *email* ITS, misalnya *website* ITS (<https://its.ac.id>), *website* DPTSI-ITS (<https://dptsi.its.ac.id>), *Integra* ITS (<https://integra.its.ac.id>), *LPSE* (<https://lpse.its.ac.id>) untuk pengadaan barang/layanan secara elektronik yang dimiliki oleh ULP-ITS, *E-Aset* (<https://e-aset.its.ac.id>) untuk inventaris aset BMN yang dimiliki oleh BAUK-ITS, *Umpan Balik/E-Tiket* (<https://umpanbalik.its.ac.id>) untuk pelaporan keluhan yang dimiliki oleh Subdit Pelayanan, portal unduh perangkat lunak (<https://unduh.its.ac.id>), dan lainnya.
  - Perangkat jaringan, *server*, komputer dan aset informasi lainnya yang berada diluar kantor DPTSI-ITS, misalnya yang dipasang disetiap jurusan/unit.

#### **4.2.4. Penetapan Peran dan Tanggung Jawab**

Peran dan tanggung jawab akan keseluruhan aktifitas SMKI maupun proses manajemen resiko keamanan informasi nantinya dilakukan oleh tim pengelola SMKI. Berdasarkan hasil wawancara dengan Direktur DPTSI-ITS dan pemetaan struktur tim pengelola SMKI yang dibutuhkan SNI ISO/IEC 27001 dengan struktur organisasi, tim pengelola SMKI yang dibutuhkan DPTSI-ITS dapat dilihat pada Gambar 4.5.





Gambar 4.5 Tim Pengelola SMKI

Didalam tim penerapan SMKI, pihak yang berperan dan bertanggung jawab sebagai pihak manajemen resiko dapat dirangkap pada tim pemimpin SMKI, dan auditor dapat dilakukan oleh auditor eksternal. Berikut ini adalah penjelasan tanggung jawab dari masing-masing tim pengelola SMKI berdasarkan Gambar 4.10:

1. Pimpinan bertanggung jawab dalam memastikan kesesuaian kebijakan dan sasaran keamanan informasi dengan arah strategis organisasi, serta tersedianya sumber daya yang dibutuhkan SMKI. Selain itu mengkomunikasikan pentingnya kepatuhan dan mendukung kontribusi setiap pemangku kepentingan terhadap SMKI.
2. Komite pengendali SMKI bertanggung jawab untuk memastikan dan meninjau kesesuaian penerapan dan peningkatan SMKI. Selain itu menyediakan arahan yang jelas pada strategi SMKI organisasi dalam mengelola keamanan

informasi dan mendukung pimpinan untuk mencapai sasaran strategis organisasi.

3. Tim pemimpin SMKI bertanggung jawab dalam merencanakan, mengerakkan, dan mengatur aktifitas yang berkaitan dengan SMKI. Selain itu mengelola resiko dan beberapa dokumen terkait SMKI.
4. Tim penerapan SMKI bertanggung jawab untuk melakukan dan menerapkan semua aktifitas SMKI yang direncanakan oleh tim pemimpin SMKI.

#### **4.3. Pengusulan Kebijakan SMKI**

Kebijakan SMKI merupakan sumber acuan untuk setiap aktifitas didalam SMKI. Berdasarkan hasil wawancara dengan pihak manajemen dan hasil dari aktifitas sebelumnya, kebijakan SMKI yang disesuaikan dengan kebutuhan DPTSI-ITS adalah sebagai berikut:

1. Sasaran dari penerapan SMKI adalah melindungi aset informasi yang dikelola oleh DPTSI-ITS dari segala resiko terkait keamanan informasi yang ada dan mendukung proses bisnis di ITS.
2. Hasil yang diharapkan melalui penerapan SMKI adalah sebagai berikut:
  - Terlindunginya aspek *confidentiality*, *integrity* dan *availability* dari keseluruhan aset informasi yang dikelola oleh DPTSI-ITS.
  - Meningkatkan keamanan, kepercayaan dan kenyamanan pemangku kepentingan di DPTSI-ITS.
3. Kriteria resiko yang digunakan terdiri dari 3 tingkatan, yaitu *high* yang bernilai antara 7-9, *medium* yang bernilai antara 4-6, dan *low* yang bernilai antara 1-3. Kriteria resiko dapat dilihat sebelumnya pada Tabel 4.1.
4. Ruang lingkup SMKI hanya mencakup beberapa aset yang terkait *email* ITS dan *website server* yang dikelola DPTSI-ITS.
5. Peran dan tanggung jawab dalam aktifitas SMKI dilakukan oleh tim pengelola SMKI yang terdiri dari pimpinan, komite pengendali SMKI, tim pemimpin

SMKI dan tim penerapan SMKI. Selain itu pemilik ataupun pengguna aset bertanggung jawab juga terhadap *confidentiality*, *integrity* dan *avalability* pada masing-masing aset.

#### **4.4. Pelaksanaan Analisis Kesenjangan (Sebelum)**

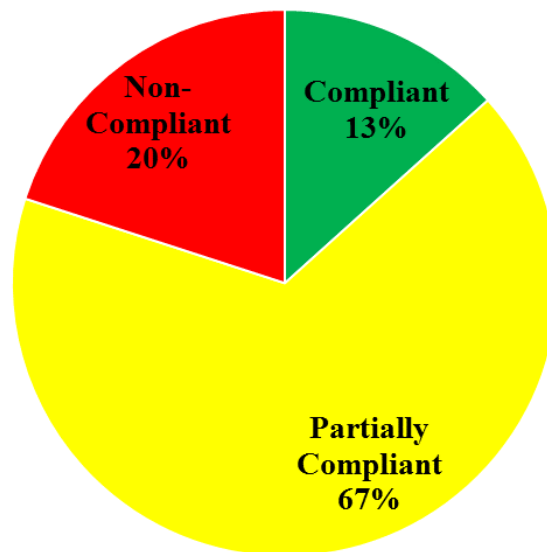
Analisis kesenjangan sebelum dilakukan untuk melihat seberapa besar kesenjangan antara kondisi DPTSI-ITS saat ini dengan SNI ISO/IEC 27001. Hasil lengkap analisis kesenjangan sebelum di DPTSI-ITS dapat dilihat pada Lampiran D. Tabel 4.5 dibawah merupakan perhitungan jumlah hasil akhir tingkat kesenjangan yang datanya merujuk pada Tabel D.2 di Lampiran D.

Tabel 4.5 Hasil Analisis Kesenjangan (Sebelum)

| No<br><i>Annex</i>              | Domain Kontrol Keamanan                                        | Jumlah  |                  |       |                            |       |                      |       |                       |
|---------------------------------|----------------------------------------------------------------|---------|------------------|-------|----------------------------|-------|----------------------|-------|-----------------------|
|                                 |                                                                | Kontrol | <i>Compliant</i> | %     | <i>Partially Compliant</i> | %     | <i>Non-Compliant</i> | %     | <i>Not Applicable</i> |
| A.5                             | Kebijakan keamanan informasi                                   | 2       | 0                | 0     | 1                          | 50    | 1                    | 50    | 0                     |
| A.6                             | Organisasi untuk keamanan informasi                            | 7       | 0                | 0     | 4                          | 57.14 | 3                    | 42.86 | 0                     |
| A.7                             | Keamanan SDM                                                   | 6       | 1                | 16.67 | 4                          | 66.67 | 1                    | 16.67 | 0                     |
| A.8                             | Manajemen aset                                                 | 10      | 0                | 0     | 7                          | 70    | 2                    | 20    | 1                     |
| A.9                             | Kontrol akses                                                  | 14      | 3                | 21.43 | 10                         | 71.43 | 1                    | 7.143 | 0                     |
| A.10                            | Kriptografi                                                    | 2       | 0                | 0     | 1                          | 50    | 1                    | 50    | 0                     |
| A.11                            | Keamanan fisik dan lingkungan                                  | 15      | 1                | 6.667 | 12                         | 80    | 2                    | 13.33 | 0                     |
| A.12                            | Keamanan operasional                                           | 14      | 1                | 7.143 | 10                         | 71.43 | 3                    | 21.43 | 0                     |
| A.13                            | Keamanan komunikasi                                            | 7       | 3                | 42.86 | 3                          | 42.86 | 1                    | 14.29 | 0                     |
| A.14                            | Akuisisi, pengembangan dan pemeliharaan sistem                 | 13      | 1                | 7.692 | 6                          | 46.15 | 2                    | 15.38 | 4                     |
| A.15                            | Relasi dengan vendor                                           | 5       | 2                | 40    | 2                          | 40    | 0                    | 0     | 1                     |
| A.16                            | Manajemen insiden keamanan informasi                           | 7       | 1                | 14.29 | 5                          | 71.43 | 1                    | 14.29 | 0                     |
| A.17                            | Aspek keamanan informasi akan manajemen keberlangsungan bisnis | 4       | 0                | 0     | 2                          | 50    | 2                    | 50    | 0                     |
| A.18                            | Kepatuhan                                                      | 8       | 1                | 12.5  | 3                          | 37.5  | 1                    | 12.5  | 3                     |
| Hasil Jumlah                    |                                                                | 114     | 14               | 12.28 | 70                         | 61.4  | 21                   | 18.42 | 9                     |
| Hasil Akhir Tingkat Kesenjangan |                                                                | 105     | 14 dari 105      | 13.33 | 70 dari 105                | 66.67 | 21 dari 105          | 20    | 105                   |

Sumber: Penelitian

Berdasarkan Tabel 4.5 terlihat bahwa tidak semua domain kontrol keamanan yang patuh (*compliant*). Rincian dari hasil analisis kesenjangan adalah 14 kontrol keamanan yang patuh, 70 kontrol keamanan yang hanya sebagian patuh (*partially compliant*), 21 kontrol keamanan yang tidak patuh (*non-compliant*), dan 9 kontrol keamanan yang tidak dapat diterapkan (*not applicable*). Persentasi jumlah tingkat kesenjangan sebelum yang datanya merujuk pada Tabel 4.5 dapat dilihat pada Gambar 4.6.



Gambar 4.6 Persentasi Jumlah Tingkat Kesenjangan (Sebelum)

## 4.5. Penilaian Resiko

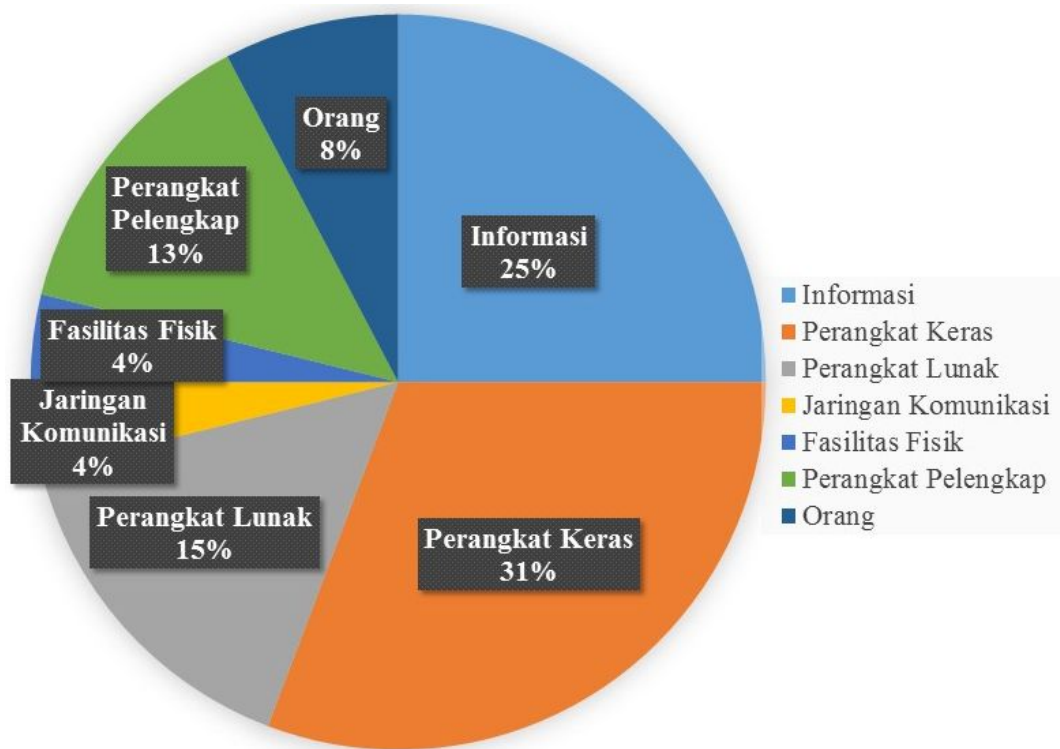
### 4.5.1. Identifikasi Resiko

Identifikasi resiko merupakan aktifitas mengenali semua resiko yang dihadapi oleh DPTSI-ITS didalam ruang lingkup SMKI. Berikut ini adalah hasil dari beberapa tahapan dalam identifikasi resiko yang telah dilakukan:

#### 1. Identifikasi aset

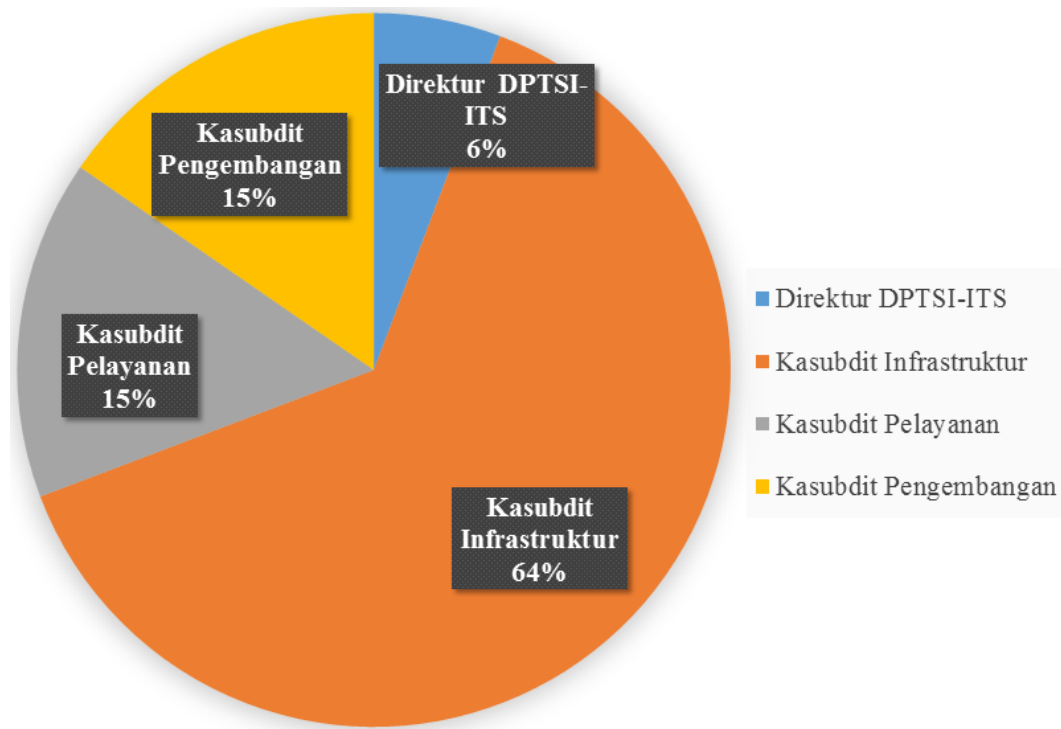
Hal pertama yang dilakukan adalah mengidentifikasi semua aset kritis yang berfungsi sebagai pengolah, pengirim maupun media/penyimpanan informasi didalam ruang lingkup SMKI. Berdasarkan hasil wawancara dengan pihak manajemen, jumlah

aset yang diidentifikasi adalah 52 aset yang terdiri dari 13 aset informasi, 16 aset perangkat keras, 8 aset perangkat lunak, 2 aset jaringan komunikasi, 2 aset fasilitas fisik, 7 aset perangkat pelengkap dan 4 aset orang. Hasil lengkap dari identifikasi aset yang kritis di DPTSI-ITS dapat dilihat pada Tabel I.3 di Lampiran I. Persentasi jumlah aset berdasarkan tipenya yang datanya merujuk pada Tabel I.3 di Lampiran I dapat dilihat pada Gambar 4.7.



Gambar 4.7 Persentasi Jumlah Aset Berdasarkan Tipe Aset

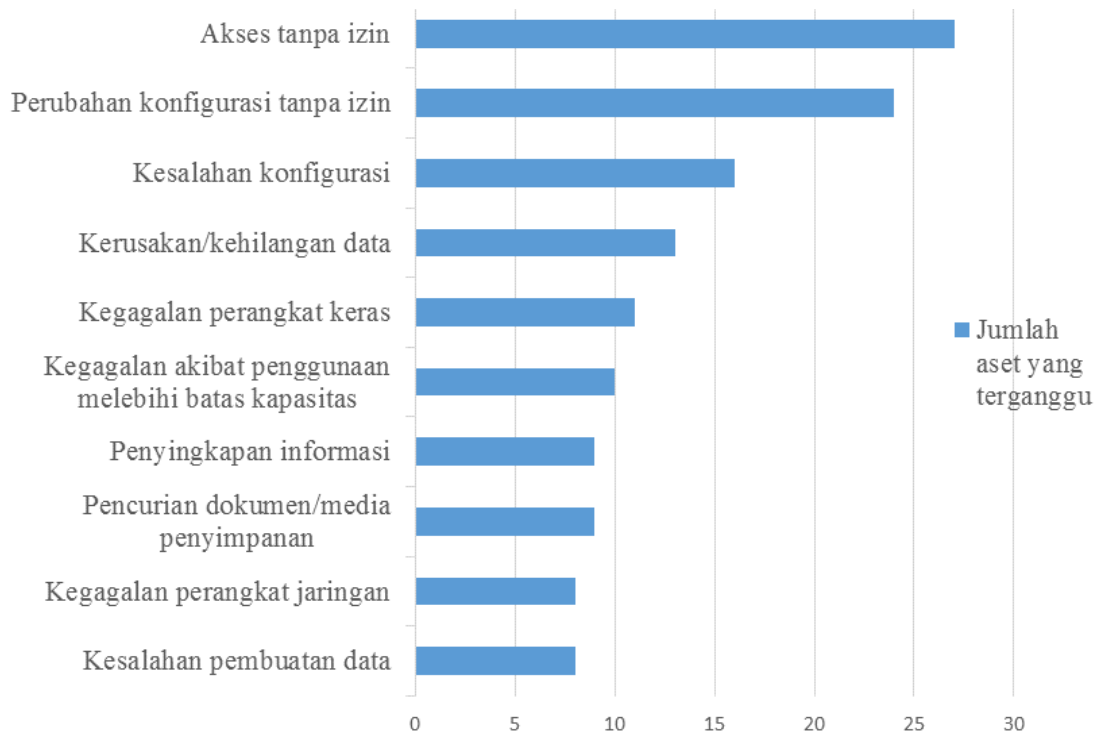
Beberapa aset yang teridentifikasi seperti *server*, Sangfor Internet Access Management, *core switch*, *distribution switch*, Cisco ASA Firewall, kabel *fiber optic*, kabel listrik, karyawan Subdit Infrastruktur, karyawan Subdit Pengembangan, pengguna Webmail ITS, dan lainnya. Selain itu jumlah aset berdasarkan pemilik resiko adalah 3 aset untuk Direktur DPTSI-ITS, 33 aset untuk Kasubdit Infrastruktur, 8 aset untuk Kasubdit Pelayanan, dan 8 aset untuk Kasubdit Pengembangan. Persentasi jumlah aset berdasarkan pemilik resikonya yang datanya merujuk pada Tabel I.3 di Lampiran I dapat dilihat pada Gambar 4.8.



Gambar 4.8 Persentasi Jumlah Aset Berdasarkan Pemilik Resiko

## 2. Identifikasi ancaman

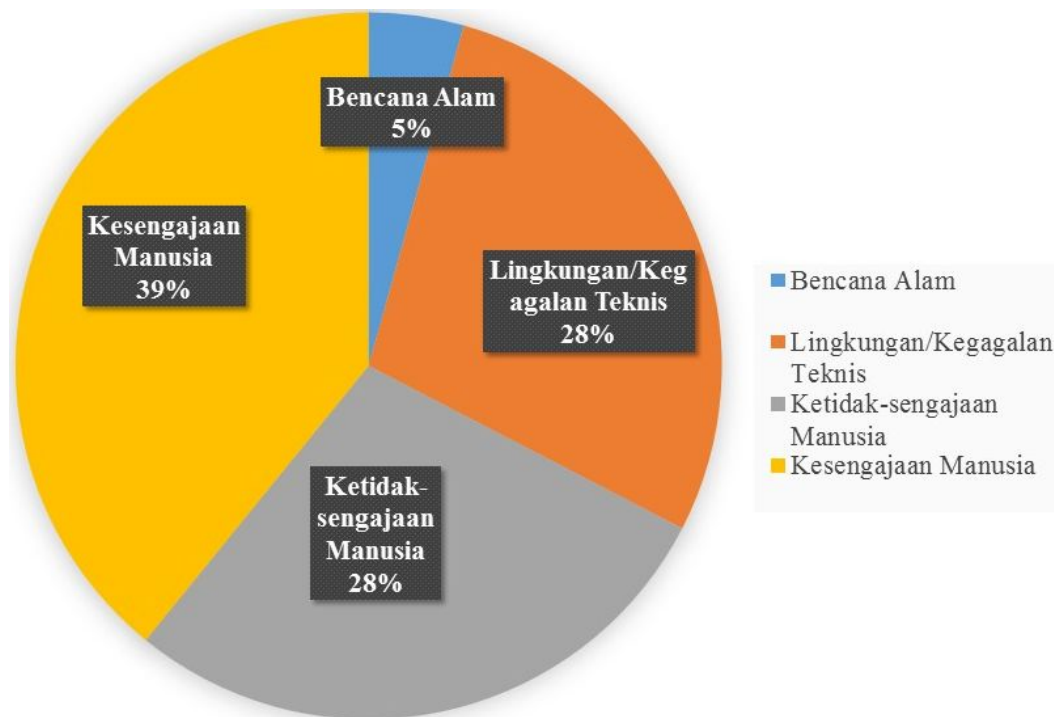
Setelah identifikasi aset, selanjutnya adalah mengidentifikasi semua ancaman yang mengganggu aspek keamanan informasi seperti *confidentiality*, *integrity* dan *availability* terhadap aset yang telah teridentifikasi. Berdasarkan hasil wawancara dengan pihak manajemen, hasil ancaman yang teridentifikasi adalah akses tanpa izin, perubahan konfigurasi tanpa izin, kesalahan konfigurasi, terkena aktifitas *social engineering*, penurunan kondisi media penyimpanan, absensi karyawan, kerusakan kabel, *denial of service*, penyalahgunaan hak akses dan tindakan ilegal lainnya, dan lainnya. Hasil lengkap dari identifikasi ancaman di DPTSI-ITS dapat dilihat pada Tabel I.4 di Lampiran I. Ancaman terbanyak yang terdapat pada aset yang datanya merujuk pada Tabel I.4 di Lampiran I dapat dilihat pada Gambar 4.9.



Gambar 4.9 Ancaman Terbanyak pada Aset

Jumlah ancaman yang diidentifikasi adalah 46 ancaman. Berdasarkan sumber ancamannya, dari 46 ancaman terdapat 2 ancaman untuk bencana alam, 13 ancaman untuk lingkungan/kegagalan teknis, 13 ancaman untuk ketidak-sengajaan manusia dan 18 ancaman untuk kesengajaan manusia. Persentasi jumlah ancaman berdasarkan sumber ancamannya yang datanya merujuk pada Tabel I.4 di Lampiran I dapat dilihat pada Gambar 4.10.



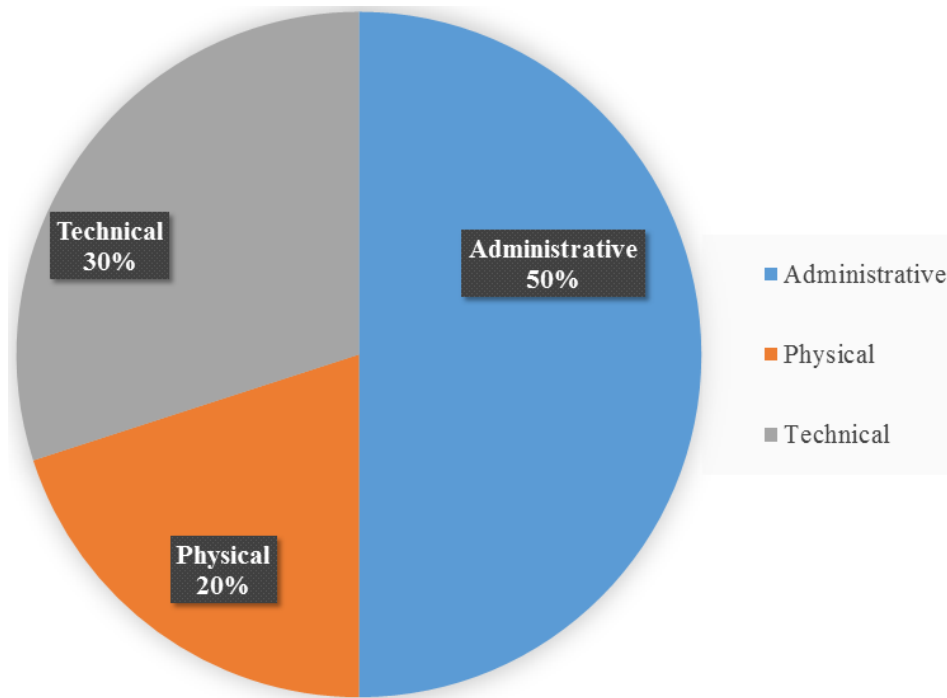


Gambar 4.10 Persentasi Jumlah Ancaman Berdasarkan Sumber Ancamannya

### 3. Identifikasi kontrol keamanan yang ada

Setelah identifikasi ancaman, selanjutnya adalah identifikasi kontrol keamanan pada ketiga area seperti *administrative*, *physical*, dan *technical* yang melindungi aset organisasi dari ancaman. Berdasarkan hasil wawancara dengan pihak manajemen, peninjauan dokumen dan observasi, hasil identifikasi kontrol keamanan adalah menghubungi vendor (A3), menghubungi unit lain di ITS (A4), menghubungi *forum* (A5), *background check* (A7), program kesadaran keamanan (A11), pelatihan kerja (A13), prosedur manajemen perubahan (A36), prosedur *backup* (A38), pemasangan *patch* (A40), prosedur pengawasan jaringan (A41), peninjauan layanan vendor (A51), prosedur penanganan insiden (A53), *service desk* (A54), pintu dengan kunci analog ataupun *fingerprint* (P1-P2), *CCTV* (P5), ruangan pusat data (P6), Cacti (T10), SIEM AlienVault (T15), Cisco ASA Firewall (T17), Tsubame (T19), Nagios (T22), ITS Web Monitoring System (T23), layanan keamanan *ISP* (T24), *server backup* (T24), *data recovery center* (T32), komponen redundan (T34), cadangan komponen atau perangkat (T35), dan lainnya.

Hasil lengkap dari identifikasi kontrol keamanan di DPTSI-ITS dapat dilihat pada Tabel I.5 di Lampiran I. Jumlah kelompok kontrol keamanan berdasarkan areanya adalah 60 kontrol keamanan *administrative*, 24 kontrol keamanan *physical*, dan 36 kontrol keamanan *technical*. Persentasi jumlah kelompok kontrol keamanan berdasarkan ketiga area yang datanya merujuk pada Tabel I.5 di Lampiran I dapat dilihat pada Gambar 4.11.



Gambar 4.11 Persentasi Jumlah Kelompok Kontrol Keamanan Berdasarkan Ketiga Area

#### 4. Identifikasi kerentanan

Setelah identifikasi kontrol keamanan, selanjutnya adalah identifikasi kerentanan pada keamanan informasi yang dapat dieksploitasi oleh ancaman. Berdasarkan hasil wawancara dengan pihak manajemen, peninjauan dokumen dan observasi, hasil identifikasi kerentanan di DPTSI-ITS adalah kurangnya pengelolaan forum yang dikunjungi (V4), kurangnya program kesadaran keamanan bagi karyawan baru (V9), kurangnya kualifikasi yang dimiliki karyawan (V11), kurang terencana dan terukurnya program kesadaran keamanan (V12), kurang lengkapnya aturan penggunaan untuk perangkat yang ada (V16), tidak adanya penyerapan ilmu yang

dimiliki karyawan (V19), kurangnya prosedur penanganan aset (V22), kurangnya penjadwalan dan pencatatan perawatan perangkat (V54), kurangnya pembaharuan dokumen ISO 9000 (V61), kurangnya rencana manajemen kapasitas (V63), kurangnya manajemen kerentanan teknis (V74), tidak adanya aturan pertukaran informasi (V77), kurangnya cadangan komponen dan perangkat (V99), kurangnya audit keamanan informasi (V101), kurangnya peninjauan kepatuhan teknis pada sistem (V103), dan lainnya. Hasil lengkap dari kerentanan di DPTSI-ITS dapat dilihat pada Tabel I.6 di Lampiran I.

#### 4.5.2. Analisis Resiko

Analisis resiko merupakan aktifitas memetakan aset, ancaman, kontrol keamanan, kerentanan dan dampak pada aspek *CIA*. Selain itu dilakukan perhitungan nilai dampak dan kemungkinannya berdasarkan hasil wawancara dengan pihak manajemen untuk menentukan level resiko dengan menggunakan metode perkalian. Jumlah resiko yang didapatkan adalah 228 resiko yang dapat dilihat pada Tabel I.7, Tabel I.8, Tabel I.9 dan Tabel I.10 di Lampiran I. Berikut ini adalah sebagian dari hasil analisis resiko yang didapatkan:

1. Resiko kegagalan perangkat jaringan untuk aset Frey Internet Router (IK39), Sangfor Internet Access Management (IK45), *core switch* (IK51), *distribution switch* (IK57) dan Cisco ASA Firewall (IK76) terdapat kontrol keamanan seperti menghubungi vendor untuk perbaikan perangkat jika masih dalam masa garansi (A3), menghubungi unit ULP-ITS untuk pengadaan perangkat baru jika perangkat diluar masa garansi dan tidak bisa diperbaiki lagi (A4), menghubungi *forum* di *internet* untuk proses *troubleshooting* (A5), pemasangan *patch* untuk memperbaiki masalah yang mungkin dapat menyebabkan *error* (A40), prosedur pengawasan jaringan yang dilakukan secara berkala oleh Subdit Infrastruktur menggunakan Cacti dan Nagios (untuk aset *core switch* dan *distribution switch*) (A41, T10 dan T22), prosedur penanganan insiden yang mencakup perbaikan komponen rusak dan pemasangan perangkat jaringan yang rusak (A53), *circuit breaker* untuk

melindungi perangkat dari gangguan listrik (P16), *AC* untuk menjaga temperatur berlebih dari perangkat (P17), dan lainnya. Nilai resiko yang didapatkan tinggi yaitu 9. Hal ini dikarenakan terdapat kerentanan seperti kurangnya penjadwalan dan pencatatan perawatan perangkat (V54), kurangnya manajemen kerentanan teknis untuk pemasangan *patch* baik secara prosedural maupun kebijakan (V74), kurangnya cadangan komponen dan perangkat (dimana perangkat Frey Internet Router, Sangfor Internet Access Management, *core switch*, dan Cisco ASA Firewall terlalu mahal untuk disiapkan perangkat cadangannya) (V99), dan lainnya.

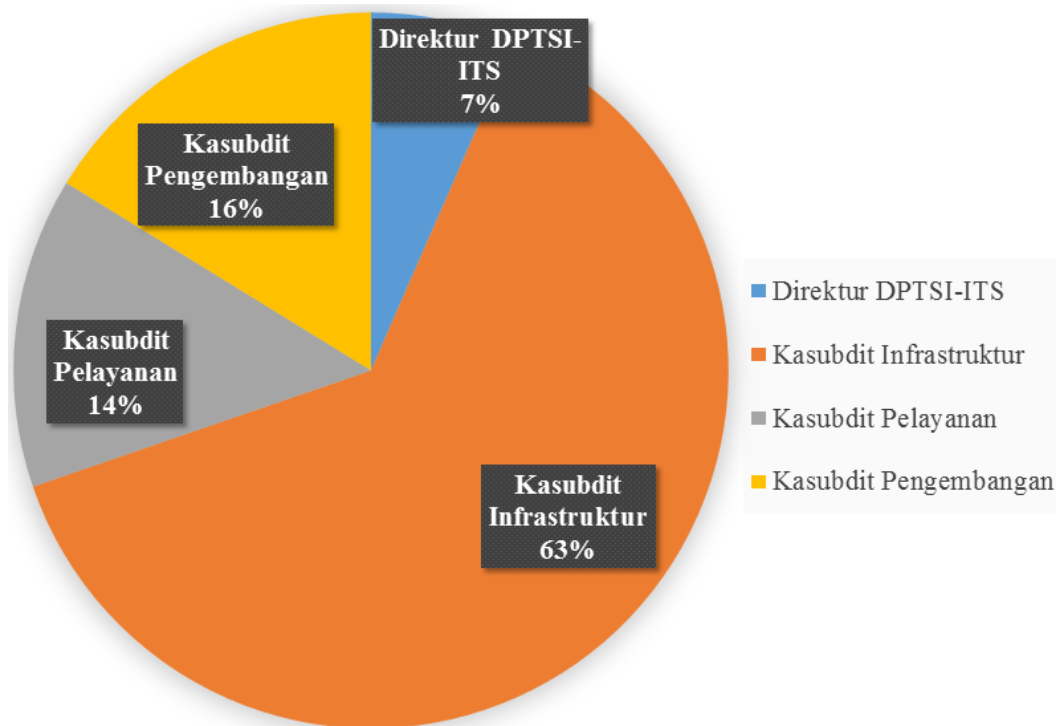
2. Resiko kesalahan konfigurasi pada aset Sangfor Internet Access Management (IK46), *core switch* (IK52), *distribution switch* (IK58) dan Cisco ASA Firewall (IK77) terdapat kontrol keamanan menghubungi *forum* untuk melihat konfigurasi yang benar (A5), *background check* untuk mengecek kualifikasi karyawan dalam melakukan pekerjaannya sesuai dokumen Kompetisi Sumber Daya sebelum penerimaan kerja (A7 dan A8), pelatihan kerja yang dinyatakan pada dokumen Matriks Kebutuhan Pelatihan SDM untuk meningkatkan kemampuan karyawan dalam mengkonfigurasi (A13 dan A14), prosedur manajemen perubahan untuk melakukan perubahan pada konfigurasi (A36), dan prosedur *backup* untuk mem-*backup* data konfigurasi jaringan kedalam *server backup* (A38 dan T13). Nilai resiko yang didapatkan tinggi yaitu 9. Hal ini dikarenakan terdapat kerentanan seperti kurangnya pengelolaan *forum* yang dikunjungi oleh karyawan (V4), kurangnya kualifikasi yang dimiliki karyawan dimana tidak semua karyawan memiliki kualifikasi untuk melakukan konfigurasi perangkat tertentu (V11), tidak adanya penyerapan ilmu yang dimiliki karyawan (V19), dan kurangnya pembaharuan dokumen ISO 9000 (dimana didalamnya terdapat dokumen Matriks Kebutuhan Pelatihan SDM yang berisikan pelatihan kerja untuk karyawan dan belum terbaharui) (V61).
3. Resiko terkena aktifitas *social engineering* pada aset Subdit Pelayanan (D15) terdapat kontrol keamanan seperti program kesadaran keamanan yang dilakukan secara berkala (A11), dan saran penggunaan *password* yang aman

pada halaman *login* Webmail ITS dan Integra ITS (A29). Nilai resiko yang didapatkan tinggi yaitu 9. Hal ini dikarenakan terdapat kerentanan seperti kurangnya pengarahan keamanan sebelum diberikan akses (V8), tidak adanya panduan ekspektasi keamanan informasi (V9), kurang terencana dan terukurnya program kesadaran keamanan (V12), kurang lengkapnya aturan penggunaan perangkat yang ada (V16), kurangnya prosedur penanganan aset (V22), tidak adanya prosedur tentang *removable media* (V23), tidak adanya aturan pemasangan perangkat lunak (V73), tidak adanya aturan pertukaran informasi yang aman (V77), dan lainnya. Namun untuk resiko terkena aktifitas *social engineering* pada aset Subdit Infrastruktur (D5) dan Subdit Pengembangan (D10), nilai resiko yang didapatkan lebih rendah yaitu 6. Hal ini bisa dikarenakan *background* dari karyawan Subdit Infrastruktur dan Subdit Pengembangan lebih menjurus ke TIK dan lebih paham masalah TIK.

4. Resiko *denial of service* pada aset *server* (IK25) terdapat kontrol keamanan seperti menghubungi vendor *ISP* untuk memblokir *IP address* yang melakukan *DDoS* (A3), menghubungi *forum* untuk penyelesaian masalah (misalnya perbaikan konfigurasi dan pencarian *patch* yang benar)(A5), pemasangan *patch* untuk menambal kerentanan yang ada (A40), prosedur pengawasan jaringan menggunakan, perangkat pengawas jaringan (Cacti, SIEM AlienVault, ITS Web Monitoring System) (A41, T10, T15, T23), peninjauan layanan vendor untuk meninjau apakah layanan yang diberikan sesuai dengan kontrak (A51), Cisco ASA Firewall untuk memblokir aktifitas dan *port* yang tidak diinginkan (T17), Tsubame untuk pemberi peringatan ancaman *hack* atau *malware* di jaringan (T19), layanan keamanan *ISP* yang menyediakan *anti-DDoS* (T24), cadangan infrastruktur jika terjadi masalah pada *server* (seperti terdapat *data recovery center* untuk Webmail ITS dan *server* redundan) (T32 dan T33), dan lainnya. Nilai resiko yang didapatkan cukup tinggi yaitu 6. Hal ini dikarenakan terdapat kerentanan seperti Kurangnya aturan dan prosedur manajemen perubahan (V62), kurangnya rencana manajemen kapasitas yang memproyeksikan kebutuhan kapasitas kedepan (V63), kurangnya manajemen kerentanan teknis untuk menambal kerentanan yang ada baik secara prosedural

maupun kebijakan (V74), kurangnya audit keamanan informasi untuk melihat kontrol apa saja yang kurang dalam penerapannya (V101), kurangnya peninjauan kepatuhan teknis pada sistem untuk melihat kerentanan dan kehandalan sistem (V103), dan lainnya.

Jumlah resiko berdasarkan pemilik resiko adalah 15 resiko dimiliki oleh Direktur DPTSI-ITS, 144 resiko dimiliki oleh Kasubdit Infrastruktur, 32 resiko dimiliki oleh Kasubdit Pelayanan, dan 37 resiko dimiliki oleh Kasubdit Pengembangan. Persentasi jumlah resiko berdasarkan pemilik resikonya yang datanya merujuk pada Tabel I.7, Tabel I.8, Tabel I.9 dan Tabel I.10 di Lampiran I dapat dilihat pada Gambar 4.12.

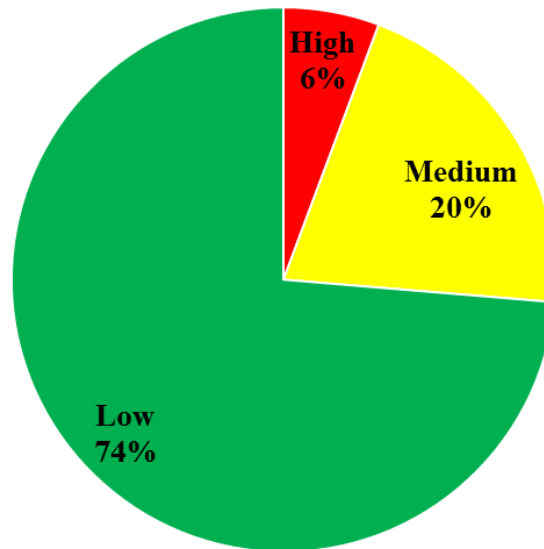


Gambar 4.12 Persentasi Jumlah Resiko Berdasarkan Pemilik Resiko

#### 4.5.3. Evaluasi Resiko

Evaluasi resiko merupakan tindakan keputusan kedepan, seperti resiko mana yang perlu ditangani serta prioritasnya. Hasil dari evaluasi resiko di DPTSI-ITS didapat dari perbandingan level resiko pada Tabel I.7, Tabel I.8, Tabel I.9 dan Tabel I.10 di Lampiran I dengan kriteria resiko pada Tabel 4.1. Hasil ini dapat dilihat pada

Tabel I.11 di Lampiran I. Berdasarkan evaluasi resiko, 13 resiko memiliki level resiko *high*, 47 resiko memiliki level resiko *medium* dan 168 resiko memiliki level resiko *low*. Persentasi jumlah pengelompokkan level resiko yang datanya merujuk pada Tabel I.11 di Lampiran I dapat dilihat pada Gambar 4.13.



Gambar 4.13 Persentasi Jumlah Pengelompokkan Level Resiko

Berdasarkan hasil evaluasi resiko yang diurutkan secara prioritas, 5 kelompok resiko dengan level resiko *high* adalah kegagalan perangkat jaringan, kesalahan konfigurasi, terkena aktifitas *social engineering*, penurunan kondisi media penyimpanan, dan kegagalan perangkat keras. Sedangkan 5 kelompok resiko dengan level resiko *medium* adalah kegagalan akibat penggunaan melebihi batas kapasitas, absensi karyawan, terkena aktifitas *social engineering*, kerusakan kabel, dan kerusakan/kehilangan data. Selain itu 5 kelompok resiko dengan level resiko *low* adalah pencurian perangkat keras, kegagalan perangkat keras, penyalahgunaan hak akses dan tindakan ilegal lainnya, pencurian perangkat jaringan, dan kegagalan perangkat jaringan. Berikut ini adalah sebagian kelompok resiko yang resikonya tidak diterima berdasarkan hasil analisis resiko sebelumnya dapat dilihat pada Tabel 4.6.

Tabel 4.6 Sebagian Kelompok Resiko yang Tidak Diterima

| Nomor resiko | Resiko                                      | Aset                               |
|--------------|---------------------------------------------|------------------------------------|
| IK39         | Kegagalan perangkat jaringan                | Frey Internet Router               |
| IK45         |                                             | Sangfor Internet Access Management |
| IK51         |                                             | <i>Core switch</i>                 |
| IK57         |                                             | <i>Distribution switch</i>         |
| IK76         |                                             | Cisco ASA Firewall                 |
| IK46         | Kesalahan konfigurasi                       | Sangfor Internet Access Management |
| IK52         |                                             | <i>Core switch</i>                 |
| IK58         |                                             | <i>Distribution switch</i>         |
| IK77         |                                             | Cisco ASA Firewall                 |
| D10          | Terkena aktifitas <i>social engineering</i> | Subdit Pelayanan                   |
| D5           | Terkena aktifitas <i>social engineering</i> | Subdit Infrastruktur               |
| D15          |                                             | Subdit Pengembangan                |
| IK25         | <i>Denial of service</i>                    | <i>Server</i>                      |

Sumber: Penelitian

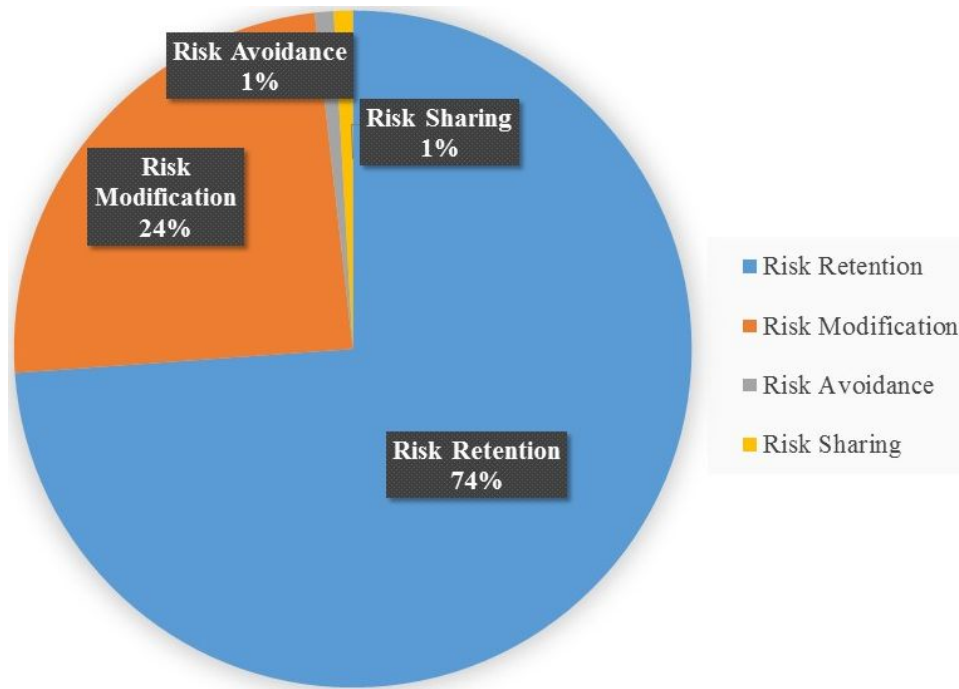
## 4.6. Perencanaan Penanganan Resiko

### 4.6.1. Pemilihan Penanganan Resiko

Pemilihan penanganan resiko merupakan aktifitas memilih penanganan keseluruhan resiko yang ada, apakah dilakukan modifikasi resiko dengan mengacu SNI ISO/IEC 27002:2013 (*risk modification*), menghindari resiko (*risk avoidance*), membagi resiko (*risk sharing*) atau menerima resiko (*risk retention*). Hasil dari pemilihan penanganan resiko di DPTSI-ITS yang sudah diurutkan berdasarkan prioritas besarnya level resiko dapat dilihat pada Tabel J.1 di Lampiran J. Dari 60 resiko yang tidak diterima, terdapat 58 resiko yang dilakukan *risk modification*, 1 resiko yang dilakukan *risk avoidance* dan 1 resiko yang dilakukan *risk sharing*. Semua kelompok resiko yang terdapat pada Tabel 4.6 dilakukan penanganan *risk modification*,



sedangkan untuk resiko *denial of service* dilakukan penanganan *risk sharing* dengan menyewa pihak ketiga yang ahli dalam penanganan *DDoS*. Persentasi jumlah pemilihan penanganan resiko yang datanya merujuk pada Tabel J.1 di Lampiran J dapat dilihat pada Gambar 4.14.



Gambar 4.14 Persentasi Jumlah Pemilihan Penanganan Resiko

#### 4.6.2. Penetapan Kontrol Keamanan dan Sasarannya

Beberapa hubungan antara kelompok resiko yang dipetakan dengan domain kontrol keamanan yang dipilih untuk menangani masing-masing resiko dapat dilihat pada Tabel 4.7. Hasil lengkapnya dapat dilihat pada Tabel J.3 di Lampiran J.

Tabel 4.7 Beberapa Hubungan Kelompok Resiko dengan Domain Kontrol Keamanan SNI ISO/IEC 27001

| No Annex | Domain Kontrol Keamanan                                        | Kelompok Resiko                                                                                                                                                                           |
|----------|----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.5      | Kebijakan keamanan informasi                                   | <ul style="list-style-type: none"> <li>• Kegagalan perangkat jaringan.</li> <li>• Terkena aktifitas <i>social engineering</i>.</li> <li>• Penurunan kondisi media penyimpanan.</li> </ul> |
| A.7      | Keamanan sumber daya manusia                                   | <ul style="list-style-type: none"> <li>• Terkena aktifitas <i>social engineering</i>.</li> <li>• Kesalahan konfigurasi.</li> </ul>                                                        |
| A.8      | Manajemen aset                                                 | <ul style="list-style-type: none"> <li>• Kegagalan perangkat jaringan.</li> <li>• Penurunan kondisi media penyimpanan.</li> <li>• Kesalahan konfigurasi.</li> </ul>                       |
| A.11     | Keamanan fisik dan lingkungan                                  | <ul style="list-style-type: none"> <li>• Kegagalan perangkat jaringan.</li> <li>• Penurunan kondisi media penyimpanan.</li> </ul>                                                         |
| A.12     | Keamanan operasional                                           | <ul style="list-style-type: none"> <li>• Kegagalan perangkat jaringan.</li> </ul>                                                                                                         |
| A.17     | Aspek keamanan informasi akan manajemen keberlangsungan bisnis | <ul style="list-style-type: none"> <li>• Kegagalan perangkat jaringan.</li> <li>• Penurunan kondisi media penyimpanan.</li> </ul>                                                         |

Sumber: Penelitian

Penetapan kontrol keamanan merupakan aktifitas menguraikan lebih jelas beberapa kontrol keamanan yang sudah dipilih untuk menangani resiko serta sasaran penerapannya. Beberapa hasil dari penetapan kontrol keamanan beserta sasaran keamanan informasi di DPTSI-ITS dapat dilihat pada Tabel 4.8. Hasil lengkapnya dapat dilihat pada Tabel J.2 di Lampiran J.

Tabel 4.8 Penetapan Kontrol Keamanan dan Sasaran Keamanan Informasi

| No<br><i>Annex</i> | Kontrol Keamanan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Sasaran Keamanan Informasi                                                                                                                                              |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | Kontrol Keamanan yang Ditetapkan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                         |
| A.5.1.1            | Kebijakan keamanan infor-masi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Semua kebijakan tersedia dan disosialisasikan keseluruh pihak yang terkait                                                                                              |
|                    | <b><i>Administrative:</i></b> <ul style="list-style-type: none"> <li>• Pembuatan kebijakan Klasifikasian Informasi (A.8.2.1).</li> <li>• Pembuatan kebijakan Manajemen Perubahan (A.12.1.2).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                         |
| A.7.2.2            | Kepedulian, pendidikan dan pelatihan keamanan infor-masi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Semua dosen, mahasiswa dan karyawan di ITS, sudah mengikuti program kesadaran keamanan, dan 30% karyawan DPTSI-ITS sudah mengikuti pelatihan kerja sesuai pekerjaannya. |
|                    | <b><i>Administrative:</i></b> <ul style="list-style-type: none"> <li>• Mengadakan program kesadaran keamanan sekaligus memberitahukan kebijakan dan prosedur tentang keamanan informasi yang terkait kepada karyawan yang baru masuk baik PNS, non-PNS ataupun magang.</li> <li>• Menjadwalkan secara matriks dan mengadakan program kesadaran keamanan secara berkala terkait keamanan informasi, seperti peserta (internal DPTSI-ITS atau pengguna sistem), waktu, materi/topik, narasumber dan jenis pelatihan (seminar, madding ITS, publikasi <i>website</i>, atau pembaharuan <i>screensaver</i>).</li> <li>• Mengadakan pelatihan atau sertifikasi kerja bagi karyawan seperti Ms. SQL Server, CISCO, dan lainnya sesuai bidangnya secara merata dan rutin.</li> <li>• Memperbaharui dokumen Matriks Kebutuhan Pelatihan SDM yang ada.</li> </ul> <b><i>Technical:</i></b> <ul style="list-style-type: none"> <li>• Memasang <i>screensaver</i> pada setiap komputer atau laptop dinas yang digunakan karyawan di DPTSI-ITS yang berisikan petunjuk, pengingat dan isu keamanan informasi.</li> </ul> |                                                                                                                                                                         |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                     |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|         | <ul style="list-style-type: none"> <li>• Pengujian tingkat kesadaran terhadap keamanan informasi melalui Integra ITS. Setiap pemangku kepentingan selama 6 bulan sekali sebelum mengakses Integra <i>ITS</i> diharuskan menjawab pertanyaan tentang keamanan informasi untuk mengukur seberapa besar tingkat kesadarannya. Pertanyaan berisikan tentang isu-isu keamanan informasi, membedakan mana yang baik dan buruk pada aktifitas penggunaan TIK, kontrol keamanan apa yang harusnya dipasang di komputer atau perangkat <i>mobile</i> yang digunakan, dan lainnya.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                     |
| A.8.1.1 | Inventaris aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Semua aset informasi disetiap Subdit sudah didokumentasikan.                        |
|         | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Mendokumentasikan aset informasi yang dibuat, dikelola atau digunakan oleh masing-masing Subdit dan karyawan DPTSI-ITS lainnya kedalam dokumen Daftar Inventaris Aset Informasi. Dokumen ini disusun berdasarkan Daftar Inventaris Aset, Daftar Inventaris SIM dan Daftar Rekaman Mutu berikut data/informasi yang ada, seperti yang diolah sistem informasi (<i>database</i>), yang dibuat sistem (<i>log, backup, file konfigurasi</i>), maupun yang diolah manual baik berbentuk <i>file (word, spreadsheet)</i> atau dokumen. Dokumen ini berisikan nomor aset, nama aset, jenis aset (informasi, perangkat keras, perangkat lunak, dan lainnya sesuai dengan penelitian ini), bentuk aset (<i>fisik/nyata/hardcopy</i> atau <i>logic/tidak nyata/softcopy</i>), lokasi aset, pemilik aset.</li> <li>• Pencatatan perangkat keras didalam Daftar Inventaris Aset harus menyertakan informasi yang tepat terutama jumlah perangkat cadangan, dan yang sedang digunakan berikut tanggal garansi habis untuk masing-masing perangkat agar memudahkan dalam penyiapan perangkat cadangannya.</li> </ul> |                                                                                     |
| A.8.1.2 | Kepemilikan aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Semua aset informasi disetiap Kasubdit sudah didokumentasikan siapa pemilik asetnya |
|         | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Mendokumentasikan siapa yang bertanggung jawab terhadap aset (pemilik aset) pada masing-masing aset secara lengkap dan jelas. Contohnya perangkat <i>AC</i> dan <i>UPS</i> pemilik asetnya adalah bapak Bustari, atau materi pelatihan dan dokumen ISO 9000 pemilik asetnya adalah ibu Widiyaningsih.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                     |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                             |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| A.8.1.4  | Pengembalian aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Setiap karyawan mengisikan 5 ilmu yang dimiliki kedalam sistem <i>knowledge management</i>  |
|          | <b>Technical:</b> <ul style="list-style-type: none"> <li>• Menerapkan sistem <i>knowledge management</i> untuk mendokumentasikan ilmu-ilmu yang dimiliki karyawan selama bekerja di DPTSI-ITS.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                             |
| A.8.2.1  | Klasifikasi informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Semua aset bertipe informasi sudah diklasifikasikan berdasarkan bentuk dan kesensitifannya. |
|          | <b>Administrative:</b> <ul style="list-style-type: none"> <li>• Mendokumentasikan klasifikasi kerahasiaan informasi berdasarkan tingkatan publik, internal dan rahasia untuk setiap data yang diolah sistem informasi (<i>database</i>), data yang dibuat sistem (<i>log, backup, file konfigurasi, ID login</i>), maupun data yang diolah manual baik berbentuk <i>file (worksheet, spreadsheet)</i> atau dokumen kertas.</li> </ul>                                                                                                                                                           |                                                                                             |
| A.11.2.4 | Pemeliharaan perlengkapan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Semua perangkat sudah dilakukan pemeliharaan perangkat sesuai dengan prosedur.              |
|          | <b>Administrative:</b> <ul style="list-style-type: none"> <li>• Melakukan pemeriksaan dan perawatan <i>server</i>. Selain itu dilakukan perekaman setiap riwayat pemeriksaan dan perawatan yang dilakukan menggunakan <i>checklist</i> waktu, nama perangkat dan tanggal pemeriksaan/perawatan.</li> <li>• Mendokumentasikan prosedur Perawatan <i>Server</i> untuk perawatan perangkat secara berkala.</li> <li>• Merekam semua riwayat perbaikan pada perangkat yang berisikan semua kesalahan sebenarnya atau yang diperkirakan, dan semua tindakan pencegahan atau perbaikannya.</li> </ul> |                                                                                             |
| A.12.1.1 | Mendokumentasikan prosedur operasional                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Semua prosedur tersedia dan disosialisasikan keseluruh karyawan yang terkait.               |
|          | <b>Administrative:</b> <ul style="list-style-type: none"> <li>• Pembuatan prosedur Perawatan <i>Server</i> (A.11.2.4).</li> <li>• Pembuatan prosedur Pemulihan dari Kegagalan Perubahan (A.12.1.2).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                             |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                              |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>• Pembuatan prosedur Manajemen Perubahan (A.12.1.2).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                              |
| A.12.1.2 | Manajemen perubahan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Semua perubahan dilakukan sesuai dengan prosedur yang ada.                   |
|          | <b><i>Administrative:</i></b> <ul style="list-style-type: none"> <li>• Mengklasifikasikan apa saja aktifitas perubahan yang memerlukan persetujuan formal ataupun yang tidak memerlukannya, dan yang memerlukan penilaian dampak/isu keamanan.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                              |
|          | <ul style="list-style-type: none"> <li>• Melakukan identifikasi dan pendokumentasian setiap perubahan yang dilakukan untuk semua Subdit di DPTSI-ITS. Dokumen tersebut berisikan waktu perubahan, petugas yang terlibat dalam perubahan, apa yang dirubah, dokumen pendukung (seperti konfigurasi atau perencanaan), dan hasil perubahan.</li> <li>• Melakukan penilaian dampak/isu keamanan yang berpotensi jika terjadi perubahan berdasarkan klasifikasi perubahan, contohnya <i>server</i> dan perangkat jaringan yang berhubungan dengan proses bisnis tertentu.</li> <li>• Mendokumentasikan kebijakan manajemen perubahan yang berisikan aturan dalam perubahan, klasifikasi perubahan, pengujian dan penilaian dampak pada perubahan, cara mengkomunikasikan perubahan, dan lainnya.</li> <li>• Mendokumentasikan prosedur pemulihan perubahan untuk mengembalikan kondisi sistem ke keadaan semula jika terjadi kegagalan dalam penerapan perubahan baru.</li> <li>• Mendokumentasikan prosedur manajemen perubahan umum yang digunakan untuk semua perubahan baik pada perangkat keras/lunak/jaringan, organisasi, proses bisnis dan lainnya.</li> </ul> |                                                                              |
| A.17.2.1 | Ketersediaan dari fasilitas pemrosesan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Setiap perangkat keras atau jaringan sudah memiliki cadangan dan komponennya |
|          | <b><i>Administrative:</i></b> <ul style="list-style-type: none"> <li>• Mendefinisikan beberapa perangkat keras/jaringan atau komponennya yang dirasakan kritis untuk segera disediakan cadangannya dengan mempertimbangkan proses bisnis yang terlibat.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                              |

|  |                                                                                                                                                                                                                                                                                                                                                                                   |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | <p><b>Technical:</b></p> <ul style="list-style-type: none"> <li>• Menyiapkan cadangan perangkat (<i>firewall, core switch, distribution switch</i> dan lainnya) ataupun komponen (<i>processor, memory, hardisk, dan lainnya</i>), jika suatu perangkat atau komponen perangkat didefinisikan kritis, sedang digunakan/beroperasional dan sudah melewati umur garansi.</li> </ul> |
|--|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Sumber: Penelitian

#### 4.7. Pelaksanaan Analisis Kesenjangan (Sesudah)

Analisis kesenjangan sesudah dilakukan untuk melihat seberapa besar kesenjangan antara kondisi DPTSI-ITS dengan SNI ISO/IEC 27001 setelah dilakukan aktifitas perencanaan penanganan resiko. Hasil analisis kesenjangan sesudah di DPTSI-ITS dapat dilihat pada Lampiran E. Tabel 4.9 dibawah merupakan perhitungan jumlah hasil akhir tingkat kesenjangan yang datanya merujuk pada Tabel E.2 di Lampiran E.

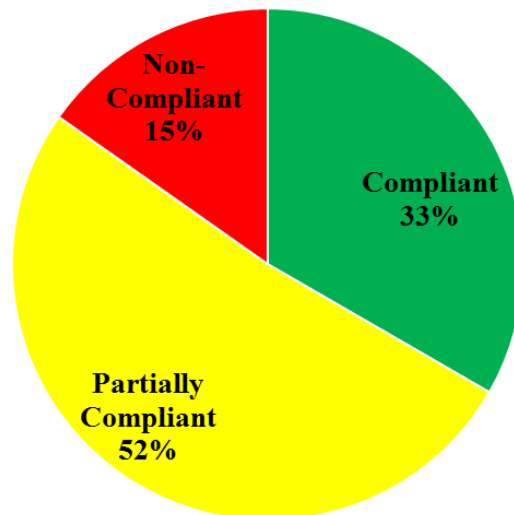
Tabel 4.9 Hasil Analisis Kesenjangan (Sesudah)

| No<br><i>Annex</i>              | Domain Kontrol Keamanan                                        | Jumlah  |                  |       |                            |       |                      |       |                       |
|---------------------------------|----------------------------------------------------------------|---------|------------------|-------|----------------------------|-------|----------------------|-------|-----------------------|
|                                 |                                                                | Kontrol | <i>Compliant</i> | %     | <i>Partially Compliant</i> | %     | <i>Non-Compliant</i> | %     | <i>Not Applicable</i> |
| A.5                             | Kebijakan keamanan informasi                                   | 2       | 1                | 50    | 1                          | 50    | 0                    | 0     | 0                     |
| A.6                             | Organisasi untuk keamanan informasi                            | 7       | 1                | 14.29 | 3                          | 42.86 | 3                    | 42.86 | 0                     |
| A.7                             | Keamanan SDM                                                   | 6       | 2                | 33.33 | 3                          | 50    | 1                    | 16.67 | 0                     |
| A.8                             | Manajemen aset                                                 | 10      | 3                | 30    | 4                          | 40    | 2                    | 20    | 1                     |
| A.9                             | Kontrol akses                                                  | 14      | 4                | 28.57 | 9                          | 64.29 | 1                    | 7.143 | 0                     |
| A.10                            | Kriptografi                                                    | 2       | 0                | 0     | 1                          | 50    | 1                    | 50    | 0                     |
| A.11                            | Keamanan fisik dan lingkungan                                  | 15      | 6                | 40    | 8                          | 53.33 | 1                    | 6.667 | 0                     |
| A.12                            | Keamanan operasional                                           | 14      | 7                | 50    | 5                          | 35.71 | 2                    | 14.29 | 0                     |
| A.13                            | Keamanan komunikasi                                            | 7       | 3                | 42.86 | 3                          | 42.86 | 1                    | 14.29 | 0                     |
| A.14                            | Akuisisi, pengembangan dan pemeliharaan sistem                 | 13      | 3                | 23.08 | 6                          | 46.15 | 0                    | 0     | 4                     |
| A.15                            | Relasi dengan vendor                                           | 5       | 2                | 40    | 2                          | 40    | 0                    | 0     | 1                     |
| A.16                            | Manajemen insiden keamanan informasi                           | 7       | 1                | 14.29 | 5                          | 71.43 | 1                    | 14.29 | 0                     |
| A.17                            | Aspek keamanan informasi akan manajemen keberlangsungan bisnis | 4       | 1                | 25    | 1                          | 25    | 2                    | 50    | 0                     |
| A.18                            | Kepatuhan                                                      | 8       | 1                | 12.5  | 3                          | 37.5  | 1                    | 12.5  | 3                     |
| Hasil Jumlah                    |                                                                | 114     | 35               | 30.7  | 54                         | 47.37 | 16                   | 14.04 | 9                     |
| Hasil Akhir Tingkat Kesenjangan |                                                                | 105     | 35 dari 105      | 33.33 | 54 dari 105                | 51.43 | 16 dari 105          | 15.24 | 105                   |

Sumber: Penelitian

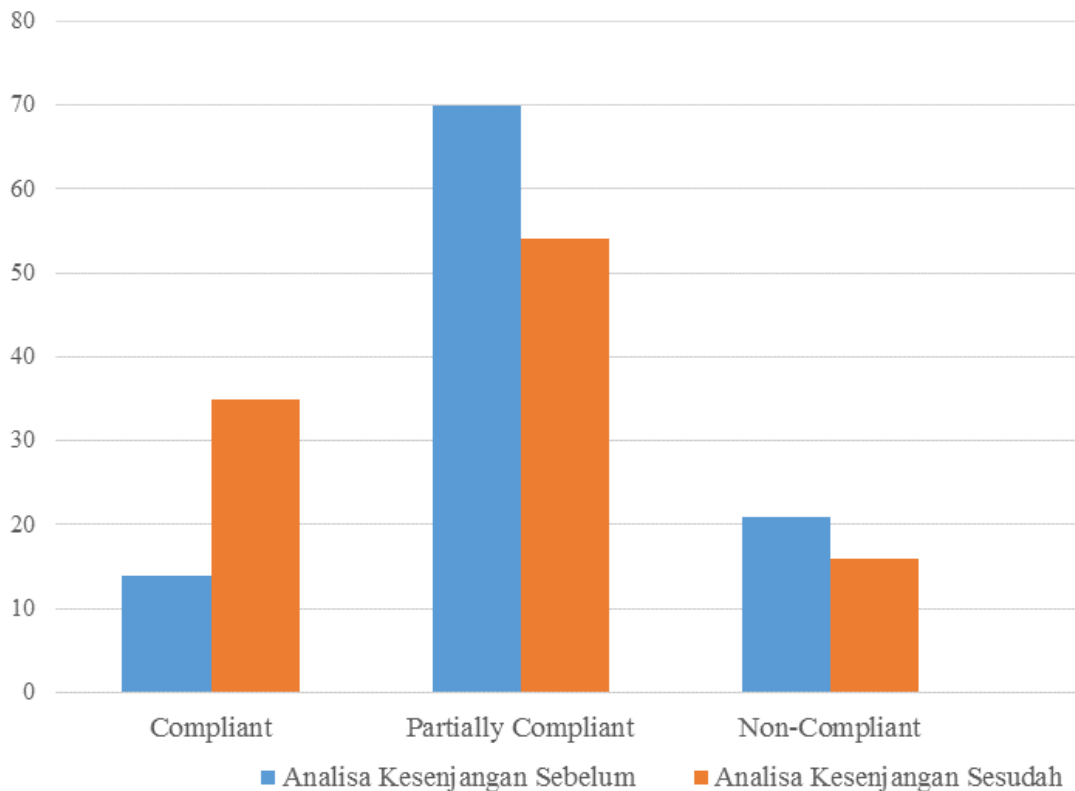


Berdasarkan Tabel 4.9 terlihat bahwa tidak semua domain kontrol keamanan yang *compliant*. Rincian dari hasil analisis kesenjangan sesudah adalah 35 kontrol keamanan yang *compliant*, 54 kontrol keamanan yang *partially compliant*, 16 kontrol keamanan yang *non-compliant*, dan 9 kontrol keamanan yang *not applicable*. Persentasi jumlah tingkat kesenjangan sesudah yang datanya merujuk pada Tabel 4.9 dapat dilihat pada Gambar 4.15.



Gambar 4.15 Persentasi Jumlah Tingkat Kesenjangan (Sesudah)

Berdasarkan perbandingan dari hasil analisis kesenjangan sebelum dengan hasil analisis kesenjangan sesudah, ditemukan sebesar 13% penambahan pada kontrol keamanan yang *compliant*, 6% pengurangan pada kontrol keamanan yang *partially compliant* dan 7% pengurangan pada kontrol keamanan yang *non-compliant*. Perbandingan persentasi jumlah tingkat kesenjangan sebelum dan sesudah dapat dilihat pada Gambar 4.16.



Gambar 4.16 Perbandingan Persentasi Jumlah Tingkat Kesenjangan Sebelum dan Sesudah

#### 4.8. Perancangan Dokumen SMKI

Berdasarkan keseluruhan aktifitas pada penelitian ini, beberapa dokumen SMKI yang berada dicakupan proses *plan* pada proses *PDCA* sudah selesai dirancang. Beberapa dokumen SMKI tersebut adalah dokumen ruang lingkup SMKI yang dapat dilihat pada Lampiran G, dokumen kebijakan SMKI yang dapat dilihat pada Lampiran H, dokumen proses penilaian resiko yang dapat dilihat pada Lampiran I, dokumen proses penanganan resiko yang dapat dilihat pada Lampiran J, dokumen *statement of applicability* yang dapat dilihat pada Lampiran K, dan dokumen sasaran keamanan informasi yang dapat dilihat pada Lampiran L.

*Halaman ini sengaja dikosongkan*

## **BAB V**

### **KESIMPULAN DAN SARAN**

BAB ini membahas mengenai kesimpulan dari penelitian perancangan SMKI berdasarkan SNI ISO/IEC 27001:2013 dan SNI ISO/IEC 27005:2015 di DPTSI-ITS. Bagian ini juga membahas mengenai saran yang membangun untuk penelitian atau pengembangan dari SMKI kedepannya.

#### **5.1. Kesimpulan**

Berikut ini adalah beberapa saran yang diberikan untuk penelitian tentang perancangan SMKI ini:

1. Jumlah resiko di DPTSI-ITS yang berhasil diidentifikasi adalah 228, dimana sebesar 168 resiko merupakan resiko yang diterima dan 60 resiko merupakan resiko yang tidak diterima.
2. Resiko yang menempati urutan 5 besar berdasarkan level resiko pada resiko yang tidak diterima adalah kegagalan perangkat jaringan, kesalahan konfigurasi, terkena aktifitas *social engineering*, penurunan kondisi media penyimpanan, dan kegagalan perangkat keras. Sedangkan resiko yang menempati urutan 5 besar berdasarkan level resiko pada resiko yang diterima adalah pencurian perangkat keras, kegagalan perangkat keras, penyalahgunaan hak akses dan tindakan ilegal lainnya, pencurian perangkat jaringan, dan kegagalan perangkat jaringan. Persentase jumlah resiko yang berada pada tingkat *high* adalah 6%, *medium* adalah 20%, dan *low* adalah 74%.
3. Dari 60 resiko yang tidak diterima, terdapat 58 resiko yang dilakukan *risk modification*, 1 resiko yang dilakukan *risk avoidance*, dan 1 resiko yang dilakukan *risk sharing*.
4. Berdasarkan 60 resiko yang tidak diterima sebelum dilakukan perencanaan penanganan resiko, hasil analisis kesenjangan sebelum yang didapatkan adalah 14 kontrol keamanan *compliant*, 70 kontrol keamanan yang *partially*

*compliant*, 21 kontrol keamanan yang *non-compliant*. Setelah resiko yang tidak diterima dilakukan perencanaan penanganan resiko, hasil analisis kesenjangan sesudah yang didapatkan adalah 35 kontrol keamanan yang *compliant*, 54 kontrol keamanan yang *partially compliant*, 16 kontrol keamanan yang *non-compliant*.

5. Berdasarkan perbandingan dari hasil analisis kesenjangan sebelum dengan hasil analisis kesenjangan sesudah, ditemukan sebesar 13% penambahan pada kontrol keamanan yang *compliant*, 6% pengurangan pada kontrol keamanan yang *partially compliant* dan 7% pengurangan pada kontrol keamanan yang *non-compliant*.
6. Rancangan tata kelola keamanan informasi berdasarkan SNI ISO/IEC 27001:2013 yang dibuat adalah dokumen ruang lingkup SMKI, dokumen kebijakan SMKI, dokumen proses penilaian resiko, dokumen proses penanganan resiko, dokumen *statement of applicability*, dan dokumen sasaran keamanan informasi. Dokumen SMKI tersebut dapat dilihat pada Lampiran G sampai Lampiran L.
7. Penggunaan SNI ISO/IEC 27001:2013 pada penelitian ini dapat dilihat dari aktifitas penetapan konteks yang menghasilkan dokumen ruang lingkup SMKI, aktifitas pengusulan kebijakan SMKI konteks yang menghasilkan dokumen kebijakan SMKI, aktifitas pelaksanaan analisis kesenjangan (baik sesudah maupun sebelum) yang dapat dilihat pada Lampiran D dan E, dan aktifitas perencanaan penanganan resiko yang menghasilkan dokumen *statement of applicability* dan dokumen sasaran keamanan informasi. Sedangkan penggunaan SNI ISO/IEC 27005:2013 pada penelitian ini dapat dilihat pada aktifitas penetapan konteks yang menghasilkan dokumen ruang lingkup SMKI, aktifitas penilaian resiko yang menghasilkan dokumen proses penilaian resiko, dan aktifitas perencanaan penanganan resiko yang menghasilkan dokumen proses penanganan resiko. Dokumen ruang lingkup SMKI berdasarkan SNI ISO/IEC 27001:2013 dan SNI ISO/IEC 27005:2013 yang dihasilkan pada penelitian ini tidaklah berbeda.

## 5.2. Saran

Berikut ini adalah beberapa saran yang diberikan untuk penelitian tentang perancangan SMKI ini:

1. DPTSI-ITS dapat memperluas area ruang lingkup SMKI untuk perlindungan yang lebih luas dan lengkap.
2. DPTSI-ITS disarankan melakukan proses manajemen resiko keamanan informasi secara berkala maupun ketika terjadinya perubahan fungsional besar-besaran pada organisasi agar resiko yang ada dapat ditangani dan diantisipasi secara tepat dan cepat.
3. Perancangan SMKI pada penelitian ini dapat dilanjutkan setelah proses *plan* dalam proses *Plan-Do-Check-Act (PDCA)* bagi DPTSI-ITS maupun peneliti atau kalangan akademik untuk penelitian selanjutnya.

*Halaman ini sengaja dikosongkan*

## GLOSARIUM

| Istilah                             | Pengertian                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Advanced Encryption Standard</i> | <i>AES</i> adalah algoritma kriptografi yang dapat digunakan untuk melindungi data elektronik, dimana <i>AES</i> menggunakan <i>chipper block</i> yang simetris yang dapat mengenkripsi dan mendekripsi informasi (Kissel, 2013).                                                                                                                                                                                                          |
| <i>Advanced Persistent Threats</i>  | <i>APT</i> memiliki beberapa pengertian, seperti mendekati korban terus menerus selama periode waktu tertentu, adaptasi untuk bertahan dari usaha pengamanan, atau menentukan untuk menjaga level interaksi yang dibutuhkan untuk melaksanakan tujuannya (Kissel, 2013).                                                                                                                                                                   |
| Ancaman                             | Penyebab potensial suatu insiden keamanan informasi yang tidak dikehendaki, yang dapat membahayakan suatu sistem atau organisasi (BSN, 2014a).                                                                                                                                                                                                                                                                                             |
| Apache HTTP Server                  | <i>HTTP server</i> atau bisa disebut <i>website server</i> merupakan perangkat lunak yang memetakan permintaan <i>URL</i> dari <i>browser</i> ke sumber yang akan menangani permintaan dan mengembalikan responnya ke <i>browser</i> . Apache sendiri merupakan proyek open source yang mengembangkan dan memelihara <i>website server</i> Apache (Rouse, 2012).                                                                           |
| AS/NZS 4360                         | <i>The Australian/New Zeland Standard for Risk Management</i> adalah standar yang menyediakan kerangka kerja umum untuk proses manajemen resiko yang dibagi menjadi sub-proses, seperti menetapkan konteks, identifikasi resiko, analisis resiko, evaluasi resiko dan menangani resiko. Standar ini tidak hanya digunakan untuk manajemen resiko keamanan informasi, tapi bisa sebagai pendekatan manajemen resiko lainnya (Ionita, 2013). |
| Audit                               | Proses yang sistematis, berdiri sendiri dan terdokumentasi untuk menemukan bukti-bukti/ <i>audit evidence</i> dan dievaluasi secara objektif untuk menentukan ditingkat manakah kriteria audit yang telah terpenuhi (BSN, 2014a).                                                                                                                                                                                                          |
| <i>Audit trail</i>                  | Rekaman yang menunjukkan siapa yang telah mengakses sistem TIK dan aktifitas apa yang telah dilakukan selama periode tertentu (Kissel, 2013).                                                                                                                                                                                                                                                                                              |



|                        |                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Autentikasi            | Proses untuk membuktikan/verikasi identitas atau atribut lainnya yang diklaim oleh atau diterima entitas (pengguna, proses atau perangkat), atau untuk membuktikan sumber dan <i>integrity</i> dari data (Kissel, 2013).                                                                                                                                            |
| Autentikasi dua faktor | Praktik yang menuntut sekurangnya dua bentuk informasi autentikasi dari pengguna sebelum mengkonfirmasi identitas pengguna (Landoll, 2011). Contoh faktornya adalah <i>something you know</i> ( <i>password, pattern</i> , kombinasi gambar), <i>something you have</i> (kartu elektronik), <i>something you are</i> (retina, wajah, sidik jari).                   |
| <i>Backbone</i>        | Bagian dari infrastruktur jaringan komputer yang saling berhubungan antar jaringan yang berbeda dan menyediakan jalur untuk pertukaran data antara jaringan yang berbeda tersebut (Microsoft, 2017). <i>Backbone</i> berfungsi untuk saling menghubungkan antar sub jaringan atau <i>LAN</i> yang berbeda baik hubungan didalam, atau antar kantor/kampus/bangunan. |
| <i>Backdoor</i>        | Penggunaan mekanisme perangkat lunak/keras tersembunyi yang tidak diizinkan untuk mengelabui kontrol keamanan (Kissel, 2013).                                                                                                                                                                                                                                       |
| <i>Backup</i>          | Salinan dokumen dan perangkat lunak yang dibuat untuk memudahkan pemulihan jika dibutuhkan (Kissel, 2013).                                                                                                                                                                                                                                                          |
| Badan sertifikasi      | Pihak ketiga yang menilai dan mensertifikasi SMKI milik organisasi klien dengan mematuhi standar SMKI yang diterbitkan dan setiap dokumen tambahan yang dibutuhkan didalam sistem (CSM, 2013).                                                                                                                                                                      |
| <i>Botnet</i>          | Jaringan komputer yang saling terhubung yang terinfeksi oleh <i>malware</i> tanpa sepengetahuan pengguna dan dikendalikan oleh <i>hacker</i> . <i>Botnet</i> umumnya menggunakan pengiriman <i>spam</i> , penyebaran <i>virus</i> dan tindakan kejahatan lainnya (Kaspersky, 2016).                                                                                 |
| <i>Browser</i>         | Perangkat lunak yang berfungsi menampilkan dan melakukan interaksi dengan dokumen-dokumen yang disediakan oleh server (Nugroho, 2013).                                                                                                                                                                                                                              |
| <i>Brute force</i>     | Metode untuk mengakses perangkat penghalang melalui percobaan beberapa kombinasi <i>password</i> numerik dan/atau alpha numerik (Kissel, 2013).                                                                                                                                                                                                                     |

|                                   |                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BSN                               | Badan Standarisasi Nasional adalah badan pembantu presiden untuk menyelenggarakan pengembangan dan pembinaan dibidang standarisasi sesuai undang-undang yang berlaku (BSN, 2005).                                                                                                                                           |
| <i>Business Continuity Plan</i>   | <i>BCP</i> merupakan proses (otomatis maupun manual) yang dirancang untuk mengurangi ancaman terhadap fungsi-fungsi penting organisasi, sehingga menjamin keberlangsungan layanan bagi operasi yang penting (Wibowo, 2006).                                                                                                 |
| <i>Business impact analysis</i>   | Metode mengukur penilaian dampak terhadap operasional bisnis dari kejadian bencana. Langkahnya adalah memprioritaskan sistem mana yang akan ditangani ketika terjadi bencana dan alokasi sumber yang tepat untuk sistem tersebut selama terjadi bencana (Landoll, 2011).                                                    |
| <i>Checksum</i>                   | Nilai perhitungan komputasi pada data untuk mendeteksi kesalahan atau manipulasi (Kissel, 2013).                                                                                                                                                                                                                            |
| <i>CSIRT</i>                      | <i>Computer Incident Response Team</i> merupakan grup atau individual yang terdiri dari analis keamanan yang terorganisasi untuk membangun, merekomendasi dan mengkoordinasikan penanganan secara langsung untuk pengkarantinaan, pembasmian, dan pemulihan yang dihasilkan dari insiden keamanan informasi (Kissel, 2013). |
| CSS                               | <i>Cascading Style Sheet</i> merupakan kumpulan kode program yang digunakan untuk mendesain atau mempercantik tampilan halaman <i>HTML</i> , seperti mengubah desain dari tulisan, warna, gambar dan latar belakang (Erudeye, 2015).                                                                                        |
| <i>Data Definition Language</i>   | Kumpulan perintah <i>SQL</i> yang dipakai dalam pembuatan, perubahan dan penghapusan data pada <i>database</i> , seperti tabel, <i>indeks</i> , <i>trigger</i> , fungsi dan lainnya (Teori Komputer, 2015).                                                                                                                 |
| <i>Data Manipulation Language</i> | Kumpulan perintah yang berfungsi untuk memanipulasi data pada tabel dalam <i>database</i> , seperti menambah/ <i>insert</i> , merubah/ <i>update</i> dan menghapus/ <i>delete</i> data pada tabel (Teori Komputer, 2015).                                                                                                   |
| <i>Database</i>                   | Kumpulan data item yang saling terhubung, terkelola menjadi satu unit. <i>Database</i> merupakan data yang disimpan didalam komputer secara sistematis. Data tersebut dapat                                                                                                                                                 |

|                                |                                                                                                                                                                                                                                                                                                        |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | diolah/dimanipulasi dengan menggunakan perangkat lunak untuk menghasilkan informasi (Temukan Pengertian, 2013a).                                                                                                                                                                                       |
| <i>Demilitarized zone</i>      | <i>DMZ</i> merupakan konfigurasi arsitektur jaringan yang aman dalam akses layanan publik yang terpisah dari sebagian jaringan dengan menggunakan teknologi <i>firewall</i> (Landoll, 2011).                                                                                                           |
| <i>Denial of Service</i>       | <i>DoS</i> adalah pencegahan akses tanpa izin atau mengganggu aktifitas yang kritis terhadap waktu. Sedangkan <i>Distributed DoS (DDoS)</i> adalah teknik yang menggunakan banyak sistem untuk melakukan penyerangan (Kissel, 2013).                                                                   |
| <i>Digital signature</i>       | Verifikasi kriptografi pada <i>file</i> dan pesan yang dibuat atau dikirim oleh pengguna atau entitas tertentu (Landoll, 2011).                                                                                                                                                                        |
| <i>Disaster Recovery Plan</i>  | Ketika <i>business continuity plan</i> sedang berlangsung, maka juga dimulailah langkah-langkah untuk penyelamatan terhadap fasilitas TIK dan sistem informasi. Dapat dikatakan bahwa <i>DRP</i> merupakan bagian atau subset dari <i>BCP</i> (Wibowo, 2006).                                          |
| <i>Eavesdropping</i>           | Serangan dimana pelakunya mendengarkan secara pasif (tidak merubah data) pada protokol yang terautentikasi untuk menangkap informasi yang dapat digunakan serangan aktif berikutnya seperti <i>masquerading</i> (Kissel, 2013).                                                                        |
| <i>Email client</i>            | <i>Mail User Agent (MUA)</i> adalah aplikasi <i>desktop</i> di komputer pengguna sendiri yang dapat digunakan oleh pengguna untuk membaca dan mengirim <i>email</i> tanpa menggunakan fasilitas <i>website email</i> yang ada, contohnya Microsoft Outlook atau Mozilla Thunderbird (DPTSI-ITS, 2017). |
| Enkripsi                       | Pengubahan dari <i>plaintext</i> (informasi belum terenkripsi) ke <i>ciphertext</i> (informasi dalam bentuk terenkripsi) melalui penggunaan algoritma kriptografi (Kissel, 2013).                                                                                                                      |
| Fasilitas pemrosesan informasi | Segala macam sistem, layanan atau infrastruktur, atau lokasi fisik (yang menempatkan) pemrosesan informasi (BSN, 2014a).                                                                                                                                                                               |
| <i>Firewall</i>                | Perangkat keras/lunak yang mampu membatasi akses antara jaringan dan/atau sistem sesuai dengan kebijakan yang spesifik (Kissel, 2013).                                                                                                                                                                 |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Forensik            | Praktik untuk mengumpulkan, menahan dan menganalisis data yang berhubungan dengan komputer untuk tujuan penyelidikan (Kissel, 2013).                                                                                                                                                                                                                                                                                                                   |
| Formulir            | Lembar isian atau surat isian (Kamus Besar Bahasa Indonesia). Formulir dalam standar ISO merupakan bukti penerapan standar dan selalu diisi setiap sebuah kegiatan atau aktifitas dilakukan (Djarmiko, 2015).                                                                                                                                                                                                                                          |
| <i>Freeware</i>     | Lisensi ini biasanya ditemui pada perangkat lunak yang bersifat mendukung atau memberikan fasilitas tambahan (contohnya <i>plug-in</i> Eye Candy di Adobe Photoshop). Selain itu terdapat pula lisensi <i>Non Commercial Use</i> yang sifatnya tidak komersial, biasanya gratis tetapi dengan batasan penggunaan tertentu dan diperuntukkan untuk kalangan pendidikan atau yayasan tertentu dibidang sosial (contohnya Star Office) (Totaltren, 2015). |
| <i>Full version</i> | Lisensi yang dibuat untuk kepentingan komersial, dimana pengguna yang ingin menggunakannya harus membeli atau mendapatkan ijin penggunaan dari pemegang hak cipta (Totaltren, 2015). Umumnya lisensi ini bisa bersifat <i>no-perpetual</i> dimana lisensi harus diperbarui setiap tahunnya atau <i>perpetual</i> dimana lisensi tidak harus melakukan pembaharuan setiap tahunnya (DPTSI-ITS, 2017).                                                   |
| <i>Hacker</i>       | Pengguna tanpa izin yang mencoba mendapatkan akses ke sistem informasi (Kissel, 2013).                                                                                                                                                                                                                                                                                                                                                                 |
| <i>Hardening</i>    | Mengatur sistem operasi dan perangkat lunak pada sistem untuk mengurangi kelemahan keamanannya (Kissel, 2013).                                                                                                                                                                                                                                                                                                                                         |
| <i>Honeypot</i>     | Sistem komputer yang dipasang sebagai pemikat/umpan untuk memancing serangan <i>cyber</i> , serta untuk mendeteksi, menangkap atau menganalisa percobaan untuk mendapatkan akses tanpa izin ke sistem informasi (Rouse, 2016).                                                                                                                                                                                                                         |
| <i>HTML</i>         | Bahasa dasar pembuatan <i>website</i> yang bukan merupakan bahasa pemrograman, tetapi bahasa <i>markup</i> . Bahasa <i>PHP</i> dan JavaScript dapat digunakan untuk memanipulasi kode <i>HTML</i> . <i>HTML</i> menampilkan berbagai informasi didalam <i>browser</i> dan pemformatan <i>hypertext</i> sederhana yang ditulis dalam berkas format <i>ASCII</i> ( <i>American Standard Code for Information</i>                                         |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | <i>Interchange</i> ) agar dapat menghasilkan tampilan wujud yang terintegrasi (Erudeye, 2015).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IEC                               | <i>International Electrotechnical Commission</i> adalah badan internasional yang mempunyai kewenangan dan tanggung jawab atas pengembangan dan konsensus standar internasional dibidang elektronik dan telekomunikasi di dunia yang mencakup mutu keselamatan, unjuk kerja dan penggunaan bahan yang selaras dengan lingkungan (BSN, 2005).                                                                                                                                                                                                                                                                                                                    |
| IMAP                              | <i>Internet Message Access Protocol</i> merupakan protokol yang sama seperti <i>POP3</i> , namun pengguna dapat <i>login</i> ke banyak <i>email client</i> karena <i>email</i> disimpan pada <i>server</i> sampai pengguna menghapusnya (How-To Geek, 2014).                                                                                                                                                                                                                                                                                                                                                                                                   |
| Indeks KAMI                       | Indeks KAMI (Keamanan Informasi) adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001 (KEMENKOMINFO, 2011b). |
| Insiden keamanan informasi        | Satu atau serangkaian kejadian keamanan informasi yang memiliki peluang signifikan terhadap pelanggaran pada aktifitas bisnis dan mengancam keamanan informasi (BSN, 2014a).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Instruksi kerja                   | Penjelasan lebih rinci cara melakukan tiap pekerjaan dan urutan pekerjaan sehingga setiap karyawan dapat bekerja dengan jelas dan fokus (Djatkiko, 2015).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <i>Intrusion detection system</i> | Perangkat keras/lunak yang mengumpulkan dan menganalisa informasi dari berbagai area dalam komputer atau jaringan untuk mengidentifikasi kemungkinan pelanggaran keamanan baik diluar maupun didalam organisasi (Kissel, 2013).                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <i>IP address</i>                 | Alamat yang secara unik mengidentifikasi setiap perangkat pada <i>internet</i> yang dipresentasikan dalam bilangan desimal                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                  | dengan format "titik-desimal" (contohnya 192.168.0.1) (Lammle, 2007).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ISO              | <i>International Organization for Standardization</i> adalah organisasi non-pemerintahan yang terdiri dari 148 negara yang berbasis atas satu anggota/lembaga pernegara dimana anggotanya tidak seperti PBB. Namun ISO menempati posisi khusus diantara sektor publik dan swasta karena banyak anggotanya merupakan bagian dari struktur pemerintahan di negaranya maupun sektor swasta yang telah diatur asosiasi-asosiasi industri. Karena itu ISO dapat bertindak sebagai organisasi penghubung dimana konsensus dapat dicapai sebagai solusi yang memenuhi persyaratan bisnis dan kebutuhan masyarakat luas (BSN, 2005). |
| ISO/IEC 17021    | ISO - <i>Conformity Assessment Requirement for Bodies Providing Audit and Certification of Management Systems</i> adalah standar yang berisikan dasar dan persyaratan untuk kompetensi, konsistensi, kejujuran badan penyedia audit dan sertifikasi untuk semua tipe sistem manajemen (ISO, 2015).                                                                                                                                                                                                                                                                                                                           |
| JavaScript       | Bahasa skrip yang populer di <i>internet</i> dan dapat bekerja disebagian besar <i>browser</i> . Bahasa ini bersifat <i>client side programming language</i> yang artinya proses dilakukan oleh <i>browser/client</i> (Erudeye, 2015).                                                                                                                                                                                                                                                                                                                                                                                       |
| Kebijakan        | Ketentuan/prinsip yang menggambarkan komitmen, tekad atau rencana manajemen terhadap suatu masalah tertentu yang dinyatakan secara formal oleh pihak manajemen dan menjadi landasan kerja organisasi (KEMENKOMINFO, 2011b).                                                                                                                                                                                                                                                                                                                                                                                                  |
| Kerentanan       | Kelemahan pada aset atau kontrol keamanan yang dapat dimanfaatkan satu atau lebih ancaman (BSN, 2014a).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Ketidak-sesuaian | <i>Non-conformity</i> adalah tidak memenuhi persyaratan, seperti dokumen SMKI menyimpang dari persyaratan SNI ISO/IEC 27001, atau penerapan SMKI menyimpang daripernyataan yang didokumentasikan (UCISA, 2015).                                                                                                                                                                                                                                                                                                                                                                                                              |
| Keylogger        | Perangkat lunak yang didesain untuk merekam ketikan tombol <i>keyboard</i> yang digunakan untuk mengambil <i>password</i> atau kunci dari kriptografi dan melewati tindakan pengamanan lainnya (Kissel, 2013).                                                                                                                                                                                                                                                                                                                                                                                                               |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kontrol keamanan    | Proses, alat, praktik, kebijakan atau tindakan apapun yang memodifikasi resiko (BSN, 2014a).                                                                                                                                                                                                                                                                                                                                                                     |
| Kriptografi         | Ilmu atau seni mengenai prinsip, cara dan metode untuk mengubah informasi yang tidak bisa dimengerti dan untuk mengembalikan informasi yang terenkripsi ke bentuk yang bisa dimengerti (Kissel, 2013).                                                                                                                                                                                                                                                           |
| <i>Malware</i>      | Perangkat lunak yang dimasukkan diam-diam kesistem dengan maksud melanggar <i>confidentiality</i> , <i>integrity</i> , atau <i>availability</i> dari data korban, perangkat lunak/sistem operasi, ataupun yang mengganggu atau mengacaukan lainnya (Kissel, 2013).                                                                                                                                                                                               |
| <i>Masquerading</i> | Ketika orang/entitas tanpa hak mengaku identitas orang/entitaslain (Kissel, 2013).                                                                                                                                                                                                                                                                                                                                                                               |
| NIST SP800-30       | <i>National Institute of Standards and Technology - Risk Management Guide for Information Technology Systems</i> adalah standar yang memberikan panduan dan identifikasi detail apa yang harus dipertimbangkan dalam manajemen resiko dan penilaian resiko dalam keamanan komputer. Terdapat daftar centang, gambar (termasuk diagram alir) dan formula matematika yang sebagian besar merujuk pada terbitan peraturan pemerintah Amerika Serikat (ENISA, 2006). |
| <i>NTP</i>          | <i>Network time protocol</i> merupakan protokol sinkronisasi waktu dalam jaringan antar dua komputer atau lebih. <i>NTP</i> bertujuan untuk mensinkronisasi semua komputer yang terhubung dalam beberapa milidetik dari <i>Coordinated Universal Time (UTC)</i> serta dapat mempertahankan akurasi hingga puluhan milidetik melalui <i>internet</i> publik, bisa mencapai akurasi kurang dari satu milidetik pada jaringan lokal (Utama, 2016).                  |
| <i>Open source</i>  | Lisensi yang membebaskan penggunaanya untuk menjalankan, menggandakan, menyebarluaskan, mempelajari, mengubah dan meningkatkan kinerja perangkat lunak (Totaltren, 2015).                                                                                                                                                                                                                                                                                        |
| Panduan             | Rekomendasi tindakan yang dianjurkan dapat dilakukan untuk mencapai suatu sasaran (KEMENKOMINFO, 2011b).                                                                                                                                                                                                                                                                                                                                                         |
| <i>Patch</i>        | Pembaharuan pada sistem operasi atau perangkat lunak lainnya yang diterbitkan untuk memperbaiki masalah tertentu (Kissel, 2013).                                                                                                                                                                                                                                                                                                                                 |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>PHP</i>                    | <i>PHP: Hypertext Preprocessor</i> adalah bahasa pemrograman <i>script server-side</i> yang didesain untuk pengembangan <i>website</i> . <i>PHP</i> disebut <i>script server-side</i> karena diproses pada <i>server</i> , berbeda dengan JavaScript yang diproses pada <i>browser/client</i> . <i>PHP</i> bersifat dinamis yang bisa menyesuaikan tampilan konten tergantung situasi, menyimpan data kedalam <i>database</i> , membuat halaman yang berubah-ubah sesuai <i>input</i> dari pengguna atau memproses formulir (Erudeye, 2015). |
| Pemangku kepentingan          | Orang atau organisasi yang dapat mempengaruhi, dipengaruhi oleh, atau merasa mereka menjadi terpengaruh oleh keputusan atau aktifitas (BSN, 2014a).                                                                                                                                                                                                                                                                                                                                                                                          |
| Pemilik proses                | Orang yang bertanggung jawab terhadap pekerjaan dan peningkatan dari salah satu proses yang didefinisikan di organisasi dan sub-proses yang berhubungan (ENISA, 2006).                                                                                                                                                                                                                                                                                                                                                                       |
| Pemindaian kerentanan         | <i>Vulnerability scanning</i> adalah dasar dari tes penetrasi yang mencari beberapa kerentanan yang ada dari antarmuka eksternal dan internal sistem (Landoll, 2011).                                                                                                                                                                                                                                                                                                                                                                        |
| Peninjauan <i>source code</i> | Proses yang menyelidiki secara manual kode pada perangkat lunak yang dikembangkan sesuai kebutuhan untuk mencari kerentanan, seperti praktik pengkodean yang tidak aman dan tersisipnya <i>trojan horse</i> dan <i>backdoor</i> (Landoll, 2011).                                                                                                                                                                                                                                                                                             |
| <i>Phishing</i>               | Menipu individu untuk membuka informasi personal yang sensitif melalui penggunaan alat berbasis komputer yang dapat memperdayai (Kissel, 2013). Kebanyakan penipuan <i>phishing</i> didistribusikan melalui <i>email</i> atau <i>URL</i> pada situs media sosial (Symantec, 2015).                                                                                                                                                                                                                                                           |
| <i>POP3</i>                   | <i>Post Office Protocol</i> merupakan protokol yang digunakan untuk menerima informasi <i>email</i> . Dengan protokol ini, <i>email</i> diunduh ke <i>email client</i> pengguna untuk dibaca secara <i>offline</i> , lalu <i>email</i> dihapus dari <i>server</i> . Versi terbaru dari protokol ini adalah versi ke-3 (How-To Geek, 2014).                                                                                                                                                                                                   |
| Program kesadaran keamanan    | Menjelaskan peraturan yang pantas tentang kebiasaan dalam penggunaan sistem TIK dan informasi. Program ini menyampaikan kebijakan dan prosedur yang harus diikuti (Kissel, 2013).                                                                                                                                                                                                                                                                                                                                                            |



|                            |                                                                                                                                                                                                                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Prosedur                   | Tahapan kegiatan dari suatu proses yang melibatkan satu atau lebih unit kerja dalam suatu organisasi (KEMENKOMINFO, 2011b).                                                                                                                                                                                                                      |
| Protokol                   | Sekumpulan peraturan dan format yang mengizinkan sistem informasi untuk tukar-menukar informasi (Kissel, 2013).                                                                                                                                                                                                                                  |
| <i>RAID</i>                | <i>Redundant Array of Inexpensive Disks</i> adalah teknologi yang digunakan untuk peningkatan performa atau redundansi. Teknologi ini menggabungkan beberapa hardisk dan mengintegrasikan kedalam satu jalur (Kissel, 2013).                                                                                                                     |
| Resiko                     | Kombinasi dari dampak yang disebabkan kejadian yang tidak diinginkan dan kemungkinan terjadinya suatu kejadian (BSN, 2013c).                                                                                                                                                                                                                     |
| Resiko residu              | Sisa resiko yang dirasakan setelah proses penanganan resiko, atau resiko tersebut berada dibawah kriteria penerimaan resiko (Siram, 2012).                                                                                                                                                                                                       |
| Sasaran keamanan informasi | Sesuatu yang diatur organisasi yang konsisten dengan kebijakan untuk mencapai hasil tertentu (BSN, 2014a).                                                                                                                                                                                                                                       |
| Sasaran kontrol keamanan   | Pernyataan yang mendeskripsikan apa yang akan dicapai sebagai hasil dari penerapan kontrol keamanan (BSN, 2014a).                                                                                                                                                                                                                                |
| <i>Secure Socket Layer</i> | <i>SSL</i> adalah protokol yang digunakan untuk melindungi informasi pribadi selama transmisi melalui <i>internet</i> , contohnya alamat <i>website</i> yang dimulai dengan <i>HTTP</i> daripada <i>HTTPS</i> . <i>SSL</i> bekerja menggunakan <i>public key</i> untuk mengenkripsi data yang dikirim melalui koneksi <i>SSL</i> (Kissel, 2013). |
| Sertifikasi                | Aktifitas penilaian kesesuaian/ <i>conformity</i> yang dilakukan oleh badan sertifikasi (CSM, 2013). Setelah melewati audit formal, badan sertifikasi menyerahkan sertifikat SNI ISO/IEC 27001 ke organisasi untuk SMKI-nya yang berlaku selama 3 tahun dan harus disertifikasi ulang setelah itu (GHKSAR, 2015).                                |
| <i>Server</i>              | Perangkat keras/lunak yang menyediakan layanan jaringan untuk pengguna (Lammle, 2007).                                                                                                                                                                                                                                                           |
| <i>SIEM</i>                | <i>Security Information and Event Management</i> merupakan gabungan dari <i>SEM</i> dan <i>SIM</i> . <i>SEM</i> ( <i>Security Event Management</i> ) merupakan sistem penyimpanan dan penterjemah <i>log</i> terpusat dan mampu menganalisa hampir                                                                                               |

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | secara <i>realtime</i> yang dapat membuat karyawan keamanan informasi mengambil tindakan pencegahan lebih cepat. Sedangkan <i>SIM</i> ( <i>Security Information Management</i> ) merupakan sistem yang mengumpulkan data kedalam penyimpanan terpusat untuk analisa trend, pelaporan otomatis untuk kepatuhan dan pelaporan yang terpusat (Rouse, 2014).                                                                                                              |
| SNI                       | Standar Nasional Indonesia adalah standar yang ditetapkan BSN yang diberlakukan diseluruh wilayah Indonesia (BSN, 2005).                                                                                                                                                                                                                                                                                                                                              |
| <i>Sniffing</i>           | Teknik pasif yang mengawasi komunikasi jaringan, membaca protokol dan memeriksa muatan pada informasi yang diminati. <i>Sniffing</i> merupakan teknik meninjau, mengidentifikasi dan menganalisa target (Kissel, 2013).                                                                                                                                                                                                                                               |
| <i>SNMP</i>               | <i>Simple Network Management Protocol</i> merupakan protokol yang populer untuk manajemen jaringan, seperti mengawasi performa jaringan, audit penggunaan jaringan, mendeteksi kesalahan, akses tidak tepat, dan pada beberapa kasus mengkonfigurasi perangkat secara jarak jauh. Protokol ini mengumpulkan informasi dari dan mengkonfigurasi perangkat jaringan, seperti <i>server</i> , <i>printer</i> , <i>hub</i> , <i>switch</i> atau router (Microsoft, 2003). |
| SoA                       | <i>Statement of Applicability</i> merupakan kunci SMKI dalam mendokumentasikan daftar sasaran kontrol keamanan dan kontrol keamanan sebuah organisasi (Carter, 2012).                                                                                                                                                                                                                                                                                                 |
| <i>Social engineering</i> | Usaha mengelabui seseorang untuk memberikan informasi (contohnya <i>password</i> ) yang dapat digunakan untuk menyerang sistem atau jaringan (Kissel, 2013).                                                                                                                                                                                                                                                                                                          |
| <i>Spam</i>               | <i>Email</i> sampah atau penyalahgunaan sistem <i>email</i> untuk mengirim pesan secara tidak pandang bulu yang sebagian besar tidak diinginkan oleh penerima (Kissel, 2013).                                                                                                                                                                                                                                                                                         |
| <i>Spyware</i>            | Perangkat lunak yang mengumpulkan informasi mengenai kebiasaan kunjungan <i>internet</i> pengguna tanpa izin atau sepengetahuan pengguna (Landoll, 2011).                                                                                                                                                                                                                                                                                                             |
| Standar                   | Seperangkat aturan teknis yang berasal dari internal atau eksternal yang wajib dipatuhi suatu organisasi dalam rangka menerapkan suatu kerangka kerja tata kelola TIK. Contoh standar internal yaitu standar perangkat lunak <i>desktop</i> , standar                                                                                                                                                                                                                 |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 | konfigurasi komputer, standar penomoran dokumen, sedangkan contoh standar eksternal yaitu SNI ISO/IEC 27001, SNI ISO/IEC 20000 (KEMENKOMINFO, 2011b).                                                                                                                                                                                                                                                        |
| <i>STARTTLS</i>                 | Cara untuk membuat koneksi yang tidak aman saat ini dan memperbaharunya ke koneksi yang aman menggunakan protokol <i>SSL/TLS</i> (Fast Mail, 2016).                                                                                                                                                                                                                                                          |
| <i>SQL Injection</i>            | Serangan <i>SQL (Structured Query Language) injection</i> terdiri dari penyisipan atau penginjeksian perintah/ <i>query SQL</i> melalui masukan data dari klien ke perangkat lunak. Serangan yang sukses dapat membaca dan memodifikasi data sensitif dari <i>database</i> , atau menjalankan operasi administrasi pada <i>database</i> (seperti mematikan sistem manajemen <i>database</i> ) (OWASP, 2016). |
| SquirrelMail                    | Standar berbasiskan paket <i>website email</i> yang ditulis dengan murni bahasa <i>PHP</i> . Paket ini berlisensi <i>GPL</i> yang mendukung protokol <i>IMAP</i> dan <i>SMTP</i> , dan semua halaman dibuat kedalam murni <i>HTML 4.0</i> (tanpa membutuhkan <i>JavaScript</i> ) untuk kompatibilitas maksimum antar <i>browser</i> (SquirrelMail, 2016).                                                    |
| <i>Teleworking</i>              | Segala bentuk pekerjaan diluar kantor, termasuk lingkungan pekerjaan non-tradisional seperti lingkungan tempat kerja yang fleksibel, pekerjaan jarak jauh/ <i>remote</i> dan pekerjaan <i>virtual</i> (BSN, 2014b).                                                                                                                                                                                          |
| Tes penetrasi                   | <i>Penetration test</i> adalah sebuah metode penyerangan yang terencana pada kontrol keamanan sistem untuk mengetes kecukupan kontrol keamanan yang ada (Landoll, 2011).                                                                                                                                                                                                                                     |
| Topologi jaringan               | Susunan fisik dan logis dari beberapa komponen jaringan (Landoll, 2011).                                                                                                                                                                                                                                                                                                                                     |
| <i>Transport Layer Security</i> | <i>TLS</i> merupakan versi terbaru dari <i>secure socket layers</i> versi 3.0 yang diperkenalkan tahun 1999, dimana <i>TLS</i> dirilis untuk mengacu pada kerentanan dan mendukung algoritma dan teknik enkripsi lebih aman dan kuat (Olenski, 2016).                                                                                                                                                        |
| <i>Trojan horse</i>             | Perangkat lunak yang sepertinya bermanfaat dan/atau tidak berbahaya tetapi sesungguhnya memiliki fungsi merusak (UN-APCICT, 2009).                                                                                                                                                                                                                                                                           |
| <i>URL</i>                      | <i>Uniform Resource Locator</i> adalah cara penamaan alamat <i>file</i> di <i>internet</i> yang terdiri dari serangkaian karakter (huruf, angka,                                                                                                                                                                                                                                                             |

|                                |                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | ataupun simbol) yang sesuai dengan format standar yang sudah ditentukan. <i>URL</i> digunakan untuk menunjukkan alamat suatu sumber yang ada (Temukan Pengertian, 2013b).                                                                                                                                                                                       |
| <i>Virtual Private Network</i> | <i>VPN</i> merupakan jaringan <i>virtual</i> yang dibuat dalam jaringan fisik yang ada dengan menyediakan terowongan/ <i>tunnel</i> komunikasi yang aman untuk data dan informasi lainnya yang ditransmisikan antar jaringan (Kissel, 2013).                                                                                                                    |
| <i>Virtual Private Server</i>  | <i>VPS</i> merupakan <i>server virtual</i> ( <i>server</i> isolasi yang terpisah dari komputer fisik) yang dirasa pengguna sebagai <i>server</i> pribadi/berdiri sendiri meski dipasang pada komputer fisik yang menjalankan beberapa sistem operasi. <i>VPS</i> menyediakan fungsi dan privasi yang sama seperti komputer fisik normal (Techopedia, 2017).     |
| <i>Virus</i>                   | Perangkat lunak yang dapat menyalin dirinya dan menginfeksi komputer tanpa izin dan sepengetahuan pengguna. <i>Virus</i> dapat merusak/menghapus data dan menyebar melalui <i>email</i> (Kissel, 2013).                                                                                                                                                         |
| <i>Work Load Analysis</i>      | Metode yang digunakan untuk menentukan kebutuhan jumlah tenaga kerja berdasarkan beban kerja pada waktu tertentu (Abidin, 2016).                                                                                                                                                                                                                                |
| <i>Worm</i>                    | Perangkat lunak yang menggandakan dan menyebarkan dirinya sendiri dengan menggunakan mekanisme jaringan untuk penyebaran (Kissel, 2013).                                                                                                                                                                                                                        |
| <i>XSS</i>                     | <i>Cross site scripting</i> adalah kerentanan yang mengizinkan <i>hacker</i> untuk memasukkan kode jahat kedalam <i>website</i> lain. Kode tersebut mendapatkan izin dari kode yang dibuat oleh <i>website</i> korban dan dapat mengancam <i>confidentiality</i> dan <i>integrity</i> dari pengiriman data antara <i>website</i> dan pengunjung (Kissel, 2013). |

*Halaman ini sengaja dikosongkan*

## DAFTAR PUSTAKA

- Abidin, Faizal (2016), *Analisis Kebutuhan Jumlah Pegawai Berdasarkan Metode Work Load Analysis dan Work Force Analysis (Studi Kasus Kerajinan Blangkon di Serengan)*, Barchelor Final Report, Universitas Muhammadiyah, Surakarta.
- Albone, Aan (2009), *Perancangan Keamanan Informasi Berdasarkan Penilaian Risiko Keamanan Informasi di PT. Multi Terminal Indonesia*, Master Thesis, Universitas Indonesia, Jakarta.
- Ariefianto, Eko (2006), *Perencanaan Tata Kelola Keamanan Informasi Berdasarkan Information Security Management System (ISMS) ISO 27001 Studi Kasus Pusat Komunikasi Departemen Luar Negeri RI*, Master Thesis, Universitas Indonesia, Jakarta.
- Badan Standarisasi Nasional (2014a), *SNI ISO/IEC 27000:2014 – Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Gambaran Umum dan Kosakata (ISO/IEC 27000:2012, IDT)*, BSN, Bandung.
- Badan Standarisasi Nasional (2014b), *SNI ISO/IEC 27002:2014 – Teknologi Informasi – Teknik Keamanan – Panduan Praktik Kendali Keamanan Informasi (ISO/IEC 27002:2013, IDT)*, BSN, Bandung.
- Badan Standarisasi Nasional (2013a), *SNI ISO/IEC 27001:2013 – Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi (ISO/IEC 27001:2013, IDT)*, BSN, Bandung.
- Badan Standarisasi Nasional (2013b), *SNI ISO/IEC 27003:2013 – Teknologi Informasi – Teknik Keamanan – Panduan Implementasi Sistem Manajemen Keamanan Informasi (ISO/IEC 27003:2010, IDT)*, BSN, Bandung.
- Badan Standarisasi Nasional (2013c), *SNI ISO/IEC 27005:2013 – Teknologi Informasi – Teknik Keamanan – Manajemen Risiko Keamanan Informasi (ISO/IEC 27005:2011, IDT)*, BSN, Bandung.
- Badan Standarisasi Nasional (2005), *Glosarium Standarisasi*, BSN, Jakarta.
- BSI (2013), *Mapping Between the Requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013*, BSI, Milton Keynes.

- Bumgarner, John & Scott Borg (2007), *The US-CCU Cyber-Security Check List*, U.S. Cyber Consequences Unit.
- Candiwan (2014), “Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia”, *Proceedings of the International Conference on Cyber-Crime Investigation and Cyber Security*, Kuala Lumpur.
- Carter, Marty (2012), “ISMS Implementation and Certification Process Overview”, dalam *Free ISO27k Toolkit*, ISO27K Forum, dari [http://www.iso27001security.com/html/iso27k\\_toolkit.html](http://www.iso27001security.com/html/iso27k_toolkit.html), diakses 16/11/2015.
- Cisco (2014), *2014 Annual Security Report*, Cisco, San Jose.
- CS Risk Management (2012), *Information Security Management System (ISMS): ISO27001 Risk Assessment Approach*, CSRM, Berkshire.
- Cyber Security Malaysia (2013), *ISMS Implementation Guideline A Practical Approach*, CSM, Selangor Darul Ehsan.
- Daud, Julia C. (2013), *Pembuatan Disaster Recovery Plan (DRP) Berdasarkan ISO/IEC 24762:2008 di ITS (Studi Kasus di Pusat Data dan Jaringan BTSI)*, Barchelor Final Report, Institut Teknologi Sepuluh Nopember, Surabaya.
- Deloitte (2009), *ISO 27001 Information Security Standard Gap Analysis Executive Summary Report*, Final Internal Audit Report, Deloitte.
- Djarmiko, M. Budi (2015), *Memahami ISO 9001:2008 Secara Menyeluruh bagi Peningkatan Kualitas Perguruan Tinggi*, Workshop Konsep & Aplikasi SPMI Berbasis Teknologi Informasi dalam Rangka Audit Eksternal (AIPT, LAM dan ISO), Jogjakarta.
- Erudeye (2015), *Mengenal HTML, CSS, Javascript dan PHP untuk Web Designer Pemula*, Erudeye, dari <http://www.erudeye.id/blog/mengenal-html-css-javascript-dan-php-untuk-web-designer-pemula/>, diakses 19/03/2017.
- European Union Agency for Network and Information Security (2006), *Risk Management: Implementation Principles and Inventories for Risk Management/Risk Assessment Methods and Tools*, ENISA, Heraklion.
- Fast Mail (2016), *SSL vs TLS vs STARTTLS*, dari <https://www.fastmail.com/help/technical/ssltlsstarttls.html>, diakses 15/03/17.

- Gordas, Vadim (2014), *Implementing Information Security Management System in SMEs and Ensuring Effectiveness in Its Governance*, Technical Report, University of London, London.
- Government of the Hong Kong Special Administrative Region (2015), *An Overview of ISO/IEC 27000 Family of Information Security Management System Standards*, GHKSAR, Hongkong.
- Government of the Hong Kong Special Administrative Region (2012a), *IT Security Guidelines [G3]*, Versi ke-7, GHKSAR, Hongkong.
- Government of the Hong Kong Special Administrative Region (2012b), *Security Risk Assessment & Audit Guidelines [G51]*, Versi ke-5, GHKSAR, Hongkong.
- Hardy, G. Mark (2014), *Risk, Loss and Security Spending in the Financial Sector: A SANS Survey*, SANS Institute, Bethesda.
- Honan, Brian (2010), *ISO27001 in a Windows Environment: The Best Practice Handbook for a Microsoft Windows Environment*, Edisi ke-2, IT Governance Publishing, Cambridgeshire.
- How-To Geek (2014), *Email: What's the Difference Between POP3, IMAP, and Exchange?*, dari <https://www.howtogeek.com/99423/email-whats-the-difference-in-pop3-imap-and-exchange/>, diakses 15/03/17.
- Humphreys, Edward (2007), *Implementing the ISO/IEC 27001 Information Security Management System Standard*, Artech House, Boston.
- International Organization for Standardization & International Electrotechnical Commission (2015), *ISO/IEC 17021-1:2015*, ISO, dari [http://www.iso.org/iso/catalogue\\_detail?csnumber=61651](http://www.iso.org/iso/catalogue_detail?csnumber=61651), diakses 19/11/15.
- International Organization for Standardization & International Electrotechnical Commission (2014), *The ISO Survey of Management System Standard Certifications (2006-2014)*, ISO, dari [http://www.iso.org/iso/iso-survey\\_2014.zip](http://www.iso.org/iso/iso-survey_2014.zip), diakses 11/01/16.
- Ionita, Dan (2013), *Current Established Risk Assessment Methodologies and Tools*, Master Thesis, Universiteit Twente, Enschede.
- Itradat, Awni & Sari Sultan & Maram Al-Junaidi & Rawa'a Qaffaf & Feda'a Mashal & Fatima Daas (2014), "Developing an ISO27001 Information Security



- Management System for an Educational Institute: Hashemite University as a Case Study”, *Jordan Journal of Mechanical and Industrial Engineering*, Vol. 8, No. 2, hal. 102 – 118.
- Kamat, Mohan (2012), “An introduction to ISO27k”, dalam *Free ISO27k Toolkit*, ISO27K Forum, dari [http://www.iso27001security.com/html/iso27k\\_toolkit.html](http://www.iso27001security.com/html/iso27k_toolkit.html), diakses 16/11/2015.
- Kaspersky (2016), *What is a Botnet Attack? - Definition*, Kaspersky, dari <https://usa.kaspersky.com/internet-security-center/threats/botnet-attacks#.WAeyH8kxXIU>, diakses 20/10/16.
- Kaspersky (2014), *IT Security Threats and Data Breaches, Perception versus Reality: Time to Recalibrate*, Kaspersky, Moscow.
- Kementrian Komunikasi dan Informatika Indonesia (2011a), *Hasil Survei Penggunaan Teknologi Informasi dan Komunikasi (TIK) di Sektor Bisnis Indonesia 2011*, KEMENKOMINFO, Jakarta.
- Kementrian Komunikasi dan Informatika Indonesia (2011b), *Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik*, Edisi ke-2, KEMENKOMINFO, Jakarta.
- Kementerian Pemuda dan Olahraga Republik Indonesia (2012), *Bakuan Audit Keamanan Informasi Kemenpora*, KEMENPORA, Jakarta.
- Kissel, Richard (2013), *Glossary of Key Information Security Terms*, Revisi ke-2, National Institute of Standards and Technology, Gaithersburg.
- Komalasari, Rizki & Ilham Perdana (2014), “Audit Keamanan Informasi Bagian Teknologi Informasi PT PLN (Persero) DJBB Menggunakan SNI ISO/IEC 27001: 2009”, *Jurnal Sistem Informasi*, Vol. 9, No. 2, hal. 201-216.
- Kosutic, Dejan (2013), *Risk owners vs. asset owners in ISO 27001:2013*, dari <https://advisera.com/27001academy/knowledgebase/risk-owners-vs-asset-owners-in-iso-270012013/>, diakses 13/03/2017.
- Lammle, Todd (2007), *CCNA: Cisco Certified Network Associate: Fast Pass*, Edisi ke-3, John Wiley & Sons, New Jersey.

- Landoll, Douglas J. (2011), *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments*, Edisi ke-2, Auerbach Publications, Boca Raton.
- Microsoft (2017), *Backbone*, Microsoft, dari [https://technet.microsoft.com/en-us/library/cc776379\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc776379(v=ws.10).aspx), diakses 26/03/2017.
- Microsoft (2003), *What Is SNMP?*, Microsoft, dari [https://technet.microsoft.com/en-us/library/cc776379\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/cc776379(v=ws.10).aspx), diakses 26/03/2017.
- Nugroho, Dika C. (2013), *Pengertian dan Fungsi Browser Beserta Contohnya*, dari <http://sekedarupdate.blogspot.com/2013/09/pengertian-dan-fungsi-browser-beserta.html>, diakses 19/11/2016.
- Olenski, Julie (2016), *SSL vs. TLS - What's the Difference?*, dari <https://www.globalsign.com/en/blog/ssl-vs-tls-difference/>, diakses 14/02/2017.
- Open Web Application Security Project (2016), *SQL Injection*, OWASP, dari [https://www.owasp.org/index.php/SQL\\_Injection](https://www.owasp.org/index.php/SQL_Injection), diakses 20/10/2016.
- Purnomo, Eka P. (2016), *Perancangan Sistem Manajemen Keamanan Informasi Berdasarkan ISO/IEC 27001 (Studi Kasus: PT. Sentra Vidya Utama)*, Master Thesis, Institut Teknologi Sepuluh Nopember, Surabaya.
- Rahmad, Basuki & Suhono H. S. & Jaka Sembiring & Kridanto Surendro (2010), "Threat Scenario Dependency-Based Model of Information Security Risk Analysis", *IJCSNS International Journal of Computer Science and Network Security*, Vol. 10 No. 8, hal. 93-102.
- Ralph, Bob & Gary Hinson & Hamid Nisar (2010), *Information Security Risk Assessment*, Versi ke-3, ISO27K Forum, dari [http://www.iso27001security.com/html/iso27k\\_toolkit.html](http://www.iso27001security.com/html/iso27k_toolkit.html), diakses 16/11/2015.
- Rouse, Margaret (2016), *Honeypot (Honey Pot)*, SearchSecurity, dari <http://searchsecurity.techtarget.com/definition/honey-pot>, diakses 27/03/2017.
- Rouse, Margaret (2014), *Security Information and Event Management (SIEM)*, SearchSecurity, dari <http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM>, diakses 27/03/2017.

- Rouse, Margaret (2012), *Apache HTTP Server Project*, WhatIs, dari <http://whatis.techtarget.com/definition/Apache-HTTP-server-project>, diakses 27/03/2017.
- Salim, Julya & Sri Anna & Meyrisca (2012), *Penilaian Risiko Infrastruktur Teknologi Informasi pada Organisasi Publik dengan Pendekatan ISO 27005 (Studi Kasus: Badan Pengkajian dan Penerapan Teknologi)*, Bachelor Final Report, Universitas Bina Nusantara, Jakarta.
- SANS Institute (2012), *Security Awareness Survey*, SANS Institute, Bethesda.
- Sari, Kartika (2009), *Pembuatan Sistem Manajemen Keamanan Informasi (SMKI) di Biro Administrasi & Akademik Kemahasiswaan (BAAK) Institut Teknologi Sepuluh Nopember Berdasarkan ISO 27001:2005*, Bachelor Final Report, Institut Teknologi Sepuluh Nopember, Surabaya.
- Sarno, Riyanarto & Irsyat Iffano (2009), *Sistem Manajemen Keamanan Informasi Berbasis ISO 27001*, ITS Press, Surabaya.
- Shah, Nafis (2015), *Aset Owners vs Risk Owners*, dari <https://www.scalar.ca/en/blog/aset-owners-vs-risk-owners>, diakses 12/11/16.
- Shuff, Michael (2015), *ISO 27001:2013 - What Has Changed From The 2005 version?*, Cognidox Limited, Cambridge.
- Siram, Swamy L.N. (2012), *ISO27001 for Ground Segment Security*, VEGA Space GmbH, Darmstadt.
- Sophos (2013), *Sophos Security Threat Report 2013*, Sophos, Boston.
- SquirrelMail (2016), *What is SquirrelMail?*, SquirrelMail, dari <http://www.squirrelmail.org/about/>, diakses 19/03/2017.
- Symantec (2015), *Internet Security Threat Report Vol.20*, Symantec, Mountain View.
- Teori Komputer (2015), *Perbedaan DDL (Data Definition Language) dan DML (Data Manipulation Language)*, Teori Komputer, dari <http://www.teorikomputer.com/2015/10/perbedaan-ddl-data-definition-language.html>, diakses 09/04/2017.
- Techopedia (2017), *Virtual Private Server (VPS)*, Techopedia, dari <https://www.techopedia.com/definition/4800/virtual-private-server-vps>, diakses 19/03/2017.

- Tempo (2015), *Cyber Crime Costs Indonesia More than Rp33 M*, Tempo, dari <http://en.tempo.co/read/news/2015/08/26/240695173/cyber-crime-costs-indonesia-more-than-rp33-m>, diakses 03/11/15.
- Temukan Pengertian (2013a), *Pengertian Database*, Temukan Pengertian, dari <http://www.temukanpengertian.com/2013/07/pengertian-database.html>, diakses 20/10/2016.
- Temukan Pengertian (2013b), *Pengertian URL*, Temukan Pengertian, dari <http://www.temukanpengertian.com/2013/06/pengertian-url.html>, diakses 20/10/2016.
- Totaltren (2015), *Mengenal Lisensi Software*, Totaltren, dari <http://www.totaltren.com/2015/01/mengenal-lisensi-software.html>, diakses 19/03/2017.
- Turner, Richard (2011), "A New Focus for IT Security?", *Computer Fraud & Security*, Elsevier, Philadelphia.
- Ulinnuha, Luthfiya (2013), *Evaluasi Pengelolaan Keamanan Jaringan di ITS dengan Menggunakan Standar Indeks Keamanan Informasi (KAMI) Kemenkominfo RI*, Bachelor Final Report, Institut Teknologi Sepuluh Nopember, Surabaya.
- United Nations - Asian and Pacific Training Centre for Information and Communication Technology (2009), *Akademi Esensi Teknologi Informasi dan Komunikasi untuk Pimpinan Pemerintahan - Modul 6: Keamanan Jaringan dan Keamanan Informasi dan Privasi*, UN-APCICT, Songdo-dong.
- Universities and Colleges Information Systems Association (2015), *UCISA Information Security Management Toolkit*, Edisi ke-1, Vol. 1, UCISA, Banbury Road.
- Utama, Agung (2016), *Ancaman Keamanan NTP dan Penanggulangannya*, Sekolah Teknik Elektro dan Informatika - Institut Teknologi Bandung, dari <https://keamanan-informasi.stei.itb.ac.id/2016/09/04/2016/>, diakses 27/03/2017.
- Vu, Khoun M. (2011), "ICT as a Source of Economic Growth in The Information Age: Empirical Evidence from The 1996-2005 Period", *Telecommunications Policy*, Vol. 35, hal. 357-372.
- Wibowo, Arrianto M. (2006), *Business Continuity Plan & Disaster Recovery Plan*, Universitas Indonesia, Jakarta.

*Halaman ini sengaja dikosongkan*

## BIOGRAFI



**FURQON MAULADANI** adalah keturunan orang orang Sumenep yang memiliki minat dalam bidang TIK terutama dalam pengembangan perangkat lunak maupun keamanan informasi. Meskipun mempunyai darah orang madura, namun penulis tidak mampu mengerti bahasa madura apalagi menggunakannya dalam berkomunikasi. Pendidikan formal yang pernah ditempuh penulis

adalah SD Negeri Sodong di Tangerang, SLTP Negeri 1 Tigaraksa di Tangerang dan SMKN 37 Pasar Minggu jurusan tata boga di Jakarta. Mungkin saja anda bertanya mengapa penulis memilih jurusan memasak. Alasannya adalah karena belajar memasak dapat dimanfaatkan secara langsung karena makanan kebutuhan primer manusia. Selain itu menurut penulis ilmu teori di SMA tidak semuanya bisa diterapkan pada kehidupan sehari-hari (padahal alasan yang benar penulis tidak ingin banyak menghadapi ujian saat ujian nasional, karena SMK hanya menguji bahasa Indonesia, bahasa Inggris dan matematika saja). Setelah lulus, penulis melanjutkan kuliah S1 di STMIK Swadharma Jakarta jurusan Sistem Informasi. Disana penulis menempa banyak ilmu dasar tentang perancangan dan pemrograman perangkat lunak, pembuatan dan pengelolaan *database*, bisnis dan manajemen, pengenalan TIK, dan lainnya. Setelah lulus dengan nilai yang bisa dibilang memuaskan (bagi penulis), penulis melihat peluang untuk langsung melanjutkan kuliah S2 di ITS. Kuliah di ITS memang memberi banyak *shock therapy* bagi penulis. Hal ini mungkin diakibatkan perbedaan dosen, kultur, kondisi kampus ataupun uang SPP per-semester. Meskipun demikian penulis tetap berjuang, walau seberat apapun tugas (yang terkadang banyak), ujian (yang terkadang menggemaskan) maupun dosen penguji yang semuanya merintangi penulis untuk segera menikah (maaf kesalahan ketik “lulus”, red). Untuk menghubungi penulis, dapat melalui:

| <b>Kontak</b>       |                                                                                                                             |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Gmail               | <a href="mailto:furqonmauladani@gmail.com">furqonmauladani@gmail.com</a> (utama)                                            |
| Yahoo Mail          | <a href="mailto:furqon_37@yahoo.co.id">furqon_37@yahoo.co.id</a>                                                            |
| <b>Media sosial</b> |                                                                                                                             |
| Facebook            | <a href="https://www.facebook.com/furqon.mauladani">https://www.facebook.com/furqon.mauladani</a>                           |
| Twitter             | <a href="https://twitter.com/furqonmauladani">https://twitter.com/furqonmauladani</a>                                       |
| Google+             | <a href="https://plus.google.com/+FurqonMauladani">https://plus.google.com/+FurqonMauladani</a>                             |
| LinkedIn            | <a href="https://id.linkedin.com/in/furqon-mauladani-479603b3">https://id.linkedin.com/in/furqon-mauladani-479603b3</a>     |
| <b>Kontribusi</b>   |                                                                                                                             |
| Academia.edu        | <a href="http://independent.academia.edu/FurqonMauladani">http://independent.academia.edu/FurqonMauladani</a>               |
| SlideShare          | <a href="https://www.slideshare.net/furqonmauladani">https://www.slideshare.net/furqonmauladani</a>                         |
| Scribd              | <a href="https://www.scribd.com/user/266254987/Furqon-Mauladani">https://www.scribd.com/user/266254987/Furqon-Mauladani</a> |
| ResearchGate        | <a href="https://www.researchgate.net/profile/Furqon_Mauladani">https://www.researchgate.net/profile/Furqon_Mauladani</a>   |
| Blog                | <a href="https://tukanglinux.blogspot.com">https://tukanglinux.blogspot.com</a>                                             |

## Daftar Wawancara

Lampiran ini berisikan daftar pertanyaan yang ditanyakan kepada para pemangku kepentingan ketika aktifitas wawancara. Tabel A.1 berisikan pertanyaan yang digunakan untuk pengaturan kriteria resiko, dampak dan kemungkinan. Pertanyaan akan ditanyakan hanya kepada pemimpin/ketua organisasi saja.

Tabel A.1 Daftar Wawancara untuk Pengaturan Kriteria Resiko, Dampak dan Kemungkinan

| No | Pertanyaan                                                                                                                  |
|----|-----------------------------------------------------------------------------------------------------------------------------|
| 1  | Pilihlah skala yang akan digunakan untuk skala nilai dampak dan skala nilai kemungkinan?<br><br>[3x3 / 5x5 / 10x10 / .....] |
| 2  | Berapakah batasan nilai level resiko untuk resiko yang tidak diterima dan resiko yang diterima?                             |
| 3  | Bagaimana pembagian kriteria dampak pada skala nilai dampak sesuai dengan besarnya skala yang sudah ditetapkan?             |
| 4  | Bagaimana pembagian kriteria kemungkinan pada skala nilai kemungkinan sesuai dengan besarnya skala yang sudah ditetapkan?   |

Sumber: Penelitian

Tabel A.2 berisikan pertanyaan yang digunakan untuk aktifitas penilaian resiko. Khusus untuk pertanyaan nomor 7 dan 8, pertanyaan akan ditanyakan hanya kepada pemilik resiko saja. Pemilik resiko cukup memilih salah satu sesuai dengan table skala nilai dampak dan kemungkinan yang sudah disusun.



Tabel A.2 Daftar Wawancara untuk Penilaian Resiko

| No | Pertanyaan                                                                                                                                                 |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Apa saja aset kritis yang dimiliki oleh grup/departemen/unit fungsional anda?                                                                              |
| 2  | Siapa pemilik aset dan pemilik resiko dari masing-masing aset tersebut?                                                                                    |
| 3  | Berada dimanakah lokasi aset tersebut berada?                                                                                                              |
| 4  | Apa saja ancaman/gangguan/hambatan terhadap aset tersebut yang anda ketahui atau yang anda curigai terjadi?                                                |
| 5  | Apa saja perangkat/prosedur/kebijakan/tindakan yang melindungi aset tersebut dari ancaman yang teridentifikasi?                                            |
| 6  | Apa saja penyebab/celah/kerentanan yang dapat menimbulkan terjadinya ancaman terhadap aset yang ada?                                                       |
| 7  | Menurut anda seberapa besar nilai dampak yang diterima jika ancaman tersebut terjadi berdasarkan skala nilai dampak?<br><br><i>[low / medium / high] *</i> |
| 8  | Menurut anda seberapa besar nilai kemungkinan dari ancaman tersebut berdasarkan skala nilai kemungkinan?<br><br><i>[unlikely / possible / likely] *</i>    |

Sumber: Penelitian \*) Dipilih sesuai dengan skala nilai pada tabel yang tersedia

## Contoh Kebijakan Keamanan TIK

1. Setiap ID pengguna dan *password* tidak untuk diberikan kepada orang lain. Setiap orang bertanggung jawab terhadap setiap transaksi yang dilakukan dengan menggunakan ID pengguna-nya.
2. Setiap *password* harus dibuat minimal 6 karakter dan tidak mudah ditebak.
3. Penggunaan fasilitas *internet* hanya pada kebutuhan perusahaan.
4. Dilarang untuk menggunakan fasilitas *internet* mengunduh *file* yang tidak berhubungan dengan pekerjaan.
5. Semua karyawan dilarang untuk memasang *game* dan juga tidak diperkenankan untuk main *game* baik pada jam kerja maupun jam istirahat.
6. Tidak diperbolehkan memasang perangkat lunak tambahan ke dalam komputer yang akan menyebabkan kinerja komputer menjadi lambat. Apabila diperlukan pemasangan perangkat lunak tambahan untuk kepentingan organisasi, maka harus mendapat izin dari Sub Bidang Sistem Aplikasi.
7. Apabila ditemukan adanya pemasangan diluar perangkat lunak yang ditetapkan, maka akan dikenakan sangsi.
8. Setiap informasi, data, peralatan komputer harus dipastikan aman dan tidak untuk diinformasikan/dipublikasikan kepada pihak yang tidak berhak. Sehingga menjadi tanggung jawab seluruh karyawan untuk menjaga kerahasiaan data organisasi.
9. Setiap data dan laporan dari sistem tidak boleh diberikan kepada pihak manapun kecuali telah mendapatkan persetujuan secara tertulis dari pimpinan organisasi.
10. Apabila *flashdisk* yang disediakan untuk digunakan transfer data dari cabang ke kantor pusat hanya boleh dipakai untuk menyimpan data program saja, dan *flashdisk* tersebut tidak boleh dipakai dikomputer lain dan juga tidak boleh digunakan untuk menyimpan *file-file* diluar pekerjaan kantor.

11. *Harddisk* eksternal yang disediakan tidak boleh dibawa pulang karena harus disimpan di kantor pada tempat yang aman.
12. *Harddisk* eksternal tidak boleh digunakan di komputer lain dan juga tidak boleh digunakan untuk menyimpan *file-file* diluar pekerjaan kantor seperti *games*.
13. Seluruh pembelian peralatan komputer hanya dapat dilakukan dengan sepengetahuan dan atas persetujuan dari pimpinan organisasi.
14. Penyalahgunaan, pelanggaran, dan ketidaknormalan harus segera dilaporkan kepada pimpinan organisasi.
15. Semua karyawan yang menyalahgunakan peralatan komputer dan seluruh aset organisasi serta yang tidak mematuhi akan dikenakan sanksi indisipliner yang dapat berakibat pada pemutusan hubungan kerja.
16. Jika terjadi kerusakan aset tetap yang dikarenakan unsur kesengajaan dari pemakai setelah dilakukan pemeriksaan, maka hal tersebut menjadi tanggung jawab pemakai sepenuhnya. Jika kerusakan aset tetap yang dikarenakan adanya unsur kelalaian pemakai setelah dilakukan pemeriksaan maka hal tersebut menjadi tanggung jawab pemakai sebesar 80% dari nilai aset tetap, dan tanggung jawab atasan yang bersangkutan sebesar 20% dari nilai aset tetap.

Sumber: Salim, 2012

## Hasil Wawancara

Narasumber : Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D

Jabatan : Kasubdit Infrastruktur & Keamanan Teknologi Informasi

Organisasi : DPTSI-ITS

| No Annex           | Pertanyaan & Jawaban                                                                                                                                                                                                     |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.5.1.1            | Apakah kebijakan untuk keamanan informasi dibuat dan dikomunikasikan ke karyawan dan pemangku kepentingan yang terkait?                                                                                                  |
|                    | Belum ada dan sedang dibuatkan <i>draft</i> -nya.                                                                                                                                                                        |
| A.5.1.1<br>A.6.1.5 | Apakah kebijakan untuk keamanan informasi yang dibuat merefleksikan hasil dari penilaian resiko?                                                                                                                         |
|                    | Tidak, karena tidak dilakukan proses penilaian atau manajemen resiko.                                                                                                                                                    |
| A.5.1.1            | Apakah terdapat prosedur untuk mengelola dokumen kebijakan, termasuk format, distribusi, penarikan dan penyimpanannya?                                                                                                   |
|                    | Masih belum ada.                                                                                                                                                                                                         |
| A.5.1.2            | Apakah kebijakan untuk keamanan informasi ditinjau dalam jangka waktu yang direncanakan atau jika terjadi perubahan dalam organisasi?                                                                                    |
|                    | Peninjauan kebijakan secara berkala masih belum dilakukan.                                                                                                                                                               |
| A.6.1.1            | Apakah organisasi memiliki fungsi atau bagian yang bertugas dan bertanggung jawab dalam mengelola dan menjaga keamanan informasi?                                                                                        |
|                    | Sudah ada bagian khusus yang menangani yaitu Subdit Infrastruktur.                                                                                                                                                       |
| A.6.1.1            | Apakah semua tanggung jawab tentang keamanan informasi didefinisikan dan dialokasikan?                                                                                                                                   |
|                    | Tanggung jawab tentang keamanan informasi tidak terlalu dispesifikasikan untuk perorangan atau didalam <i>job desc</i> , yang ada seperti karyawan memasang jaringan dan koneksinya, atau aktifitas operasional lainnya. |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.6.1.2                         | Apakah beberapa tugas dan area tanggung jawab yang berlawanan dipisahkan untuk mengurangi peluang perubahan dan penyalahgunaan tanpa izin atau tidak disengaja pada aset?                                                                                                                                                                                                          |
|                                 | Terdapat pembagian tugas dan tanggung jawab seperti bagian kelistrikan, jaringan, dan sistem, namun tidak ada tugas khusus dan tidak dilakukan pengkotakan bagian secara tertulis dan paten. Selain itu karena kekurangan karyawan, terkadang setiap tugas dilakukan oleh satu orang. Contohnya analisis sistem, <i>programmer</i> , dan penguji sistem dilakukan oleh satu orang. |
| A.6.1.3                         | Apakah hubungan dengan organisasi/pemerintahan dikelola dengan tepat?                                                                                                                                                                                                                                                                                                              |
|                                 | Ada koordinasi dengan pihak lain, seperti pihak <i>ISP</i> untuk pelaporan insiden.                                                                                                                                                                                                                                                                                                |
| A.6.1.4                         | Apakah hubungan dengan forum keamanan dikelola dengan tepat?                                                                                                                                                                                                                                                                                                                       |
|                                 | Kalau itu dilakukan oleh masing-masing karyawan, organisasi tidak mengatur ataupun menyarankan <i>forum</i> apa saja yang harus diikuti.                                                                                                                                                                                                                                           |
| A.6.1.5                         | Apakah keamanan informasi dirujuk kedalam manajemen proyek tanpa menghiraukan tipe dari proyek?                                                                                                                                                                                                                                                                                    |
|                                 | Untuk pemasangan <i>server</i> lebih ke konfigurasi. Karena kita punya <i>subnet-subnet</i> , nah ini mau diletakkan dimana dan tingkat keamanannya seperti apa. Dalam hal ini berhubungan dengan aplikasi dan <i>port</i> berapa yang boleh lewat melalui <i>firewall</i> .                                                                                                       |
| A.6.1.5<br>A.10.1.1<br>A.11.1.1 | Apakah organisasi melakukan penilaian resiko/manajemen resiko sebagai bagian dari manajemen proyek apapun?                                                                                                                                                                                                                                                                         |
|                                 | Belum ada penilaian atau manajemen resiko secara tertulis dan resmi.                                                                                                                                                                                                                                                                                                               |
| A.6.1.5<br>A.6.1.1              | Apakah sudah ada penanggung jawab aktifitas manajemen risiko dan pelaporan manajemen resiko?                                                                                                                                                                                                                                                                                       |
|                                 | Masih belum ada penanggung jawab resiko yang ditugaskan khusus.                                                                                                                                                                                                                                                                                                                    |
| A.6.1.5                         | Apakah organisasi menggunakan kerangka kerja tertentu untuk manajemen resiko?                                                                                                                                                                                                                                                                                                      |
|                                 | Belum ada, masih perencanaan untuk menggunakan ISO/IEC 27001.                                                                                                                                                                                                                                                                                                                      |

|         |                                                                                                                                                                                  |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.6.1.5 | Apakah setiap ancaman dan kerentanan yang terkait dengan aset informasi sudah teridentifikasi?                                                                                   |
|         | Sudah pernah dilakukan identifikasi, namun tidak ada dokumen tertulisnya.                                                                                                        |
| A.6.1.5 | Apakah sudah dilakukan analisa resiko terkait resiko yang ada pada aset informasi?                                                                                               |
|         | Biasanya saat rapat analisa resiko dibahas, namun untuk dokumentasinya memang masih belum ada.                                                                                   |
| A.6.1.5 | Apakah setiap penanganan resiko sudah disusun berdasarkan resiko yang teridentifikasi?                                                                                           |
|         | Saat memikirkan resiko yang akan terjadi, otomatis juga langsung dipikirkan langkah penanganannya.                                                                               |
| A.6.1.5 | Apakah setiap penanganan resiko yang disusun ditetapkan prioritas pelaksanaannya?                                                                                                |
|         | Untuk dokumentasi masih belum ada, namun tingkat prioritasnya berdasarkan <i>urgency</i> -nya. Biasanya yang harus dipulihkan cepat itu terkait data pengguna dan infrastruktur. |
| A.6.1.5 | Apakah status penanganan resiko yang sedang diterapkan diawasi secara berkala?                                                                                                   |
|         | Biasanya dibahas melalui grup <i>chat</i> , tidak dilakukan secara resmi.                                                                                                        |
| A.6.1.5 | Apakah setiap penanganan resiko yang sudah diterapkan dilakukan evaluasi ulang untuk mengukur keefektifannya?                                                                    |
|         | Tidak dilakukan evaluasi ulang terhadap penanganan yang dilakukan, karena biasanya yang dilakukan sudah dianggap baik dan membantu menyelesaikan masalah.                        |
| A.7.2.1 | Apakah terdapat pengarahan sebelum diberikan akses ke sistem informasi sesuai dengan peran dan tanggung jawab dalam keamanan informasi?                                          |
|         | Tidak selalu dilakukan karena mereka sudah tahu apa yang harus dilakukan dalam keamanan informasi.                                                                               |

|         |                                                                                                                                                                                                                                                                                                                                               |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.7.2.2 | Apakah semua karyawan dan kontraktor menerima program kesadaran keamanan sebelum penempatan kerja?                                                                                                                                                                                                                                            |
|         | Sosialisasi secara resmi ada, namun untuk sosialisasi sebelum penempatan kerja tidak langsung dilakukan.                                                                                                                                                                                                                                      |
| A.7.2.2 | Apakah semua karyawan dan kontraktor menerima pembaharuan berkala pada kebijakan dan prosedur yang terkait pekerjaannya?                                                                                                                                                                                                                      |
|         | Untuk pemberitahuan ada kebijakan atau prosedur baru biasanya bisa dilakukan melalui rapat.                                                                                                                                                                                                                                                   |
| A.7.2.2 | Apakah terdapat pelatihan kerja yang diadakan untuk Subdit Infrastruktur?                                                                                                                                                                                                                                                                     |
|         | Ditahun 2016 ini ada pelatihan tentang <i>honeypot</i> yang diadakan oleh KEMENKOMINFO bagi beberapa Subdit Infrastruktur.                                                                                                                                                                                                                    |
| A.8.1.1 | Apakah aset yang berhubungan dengan informasi dan fasilitas pendukungnya diidentifikasi dan daftar inventarisnya didokumentasikan dan dikelola?                                                                                                                                                                                               |
|         | Kalau aset yang berhubungan dengan informasi kami ada, seperti <i>IP address</i> apa dipakai <i>server</i> apa dan <i>server</i> ini isinya apa saja itu ada. Kami simpannya di Google Drive. Tapi tidak mendokumentasikan misalnya dokumen sekian-sekian ini tentang <i>server</i> .                                                         |
| A.8.1.2 | Apakah setiap aset yang dikelola pada inventaris terdapat pemilik atau pengelolanya?                                                                                                                                                                                                                                                          |
|         | Kalau yang disini yang megang sih di fungsi atau tugas mereka, tapi bukan di asetnya. Ya misalnya manajemen untuk sistem seperti <i>server</i> dan instalasi sistem operasi itu ada. Terus kalau akses jaringan seperti <i>access point</i> dan pengkabelan. Listrik juga ada sendiri. Secara tugas ada, yang berkaitan dengan tema tertentu. |
| A.8.1.4 | Apakah ilmu-ilmu karyawan yang dimiliki selama bekerja didokumentasikan ( <i>knowledge management</i> )?                                                                                                                                                                                                                                      |
|         | DPTSI-ITS tidak mendokumentasikan ilmu yang dimiliki karyawan selama bekerja.                                                                                                                                                                                                                                                                 |

|         |                                                                                                                                                                                                                          |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.8.2.1 | Apakah informasi diklasifikasikan berdasarkan nilai, kekritisannya, atau kerahasiaan?                                                                                                                                    |
|         | Tidak ada aturan atau undang-undang yang digunakan untuk klasifikasi aset.                                                                                                                                               |
| A.8.3.1 | Apakah prosedur untuk <i>removable media</i> dibuat dan diterapkan berdasarkan klasifikasi informasi?                                                                                                                    |
|         | Tidak ada.                                                                                                                                                                                                               |
| A.9.2.2 | Apakah dokumentasi tentang hak akses <i>administrator</i> yang dimiliki karyawan pada aset tertentu? Jadi bisa tahu bahwa pak X punya akses <i>administrator</i> ke <i>firewall</i> , <i>router</i> dan <i>lainnya</i> . |
|         | Untuk dokumentasi tidak ada, tapi sudah tahu orang ini bagiannya apa.                                                                                                                                                    |
| A.9.2.3 | Apakah alokasi dan penggunaan hak akses <i>administrator</i> untuk perangkat <i>server</i> dan jaringan dikontrol dan dibatasi melalui proses yang formal?                                                               |
|         | Kalau yang berkepentingan dikasih <i>login</i> , kalau tidak berkepentingan tidak dikasih. Kalau dokumentasi prosedurnya tidak ada.                                                                                      |
| A.9.2.3 | Apakah terdapat tingkatan hak akses <i>administrator</i> ?                                                                                                                                                               |
|         | Tidak ada pembatasan dan tingkatan hak akses untuk <i>administrator</i> .                                                                                                                                                |
| A.9.2.3 | Apakah terdapat hak akses yang memiliki jangka waktu <i>expired</i> ?                                                                                                                                                    |
|         | Tidak diatur seperti itu.                                                                                                                                                                                                |
| A.9.2.3 | Apakah terdapat pemisahan hak akses pada sistem untuk penggunaan <i>administrator</i> dengan aktifitas biasa?                                                                                                            |
|         | Tidak dipisahkan. Kalau dia punya <i>login</i> ya berarti <i>login</i> tersebut bisa digunakan sesuai dengan pekerjaannya.                                                                                               |
| A.9.2.3 | Apakah ada penggunaan <i>password</i> umum <i>administrator</i> ( <i>sharing</i> )? Dan apakah ada dokumentasi prosedur pengelolaan <i>password</i> tersebut?                                                            |
|         | Ada, dan kita kadang pakai di beberapa perangkat jaringan atau perangkat lunak tertentu. Kan biasanya ada perangkat yang tidak bisa pemisahan akun. Kalau dokumentasi prosedurnya tidak ada.                             |



|                      |                                                                                                                                                                                                                        |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.9.2.5              | Apakah pemilik aset meninjau hak akses pengguna dalam jangka waktu tertentu? Dan apakah ada dokumentasi prosedurnya?                                                                                                   |
|                      | Peninjauan ada tapi tidak terlalu sering, mungkin setahun sekali. Kita tahu karena ya orangnya itu-itulah saja. Kalau prosedurnya tidak ada.                                                                           |
| A.9.2.6              | Apakah hak akses fisik karyawan seperti kunci pintu atau data kunci <i>fingerprint</i> ditinjau secara berkala? Dan apakah ada dokumentasi prosedurnya?                                                                |
|                      | Kalau itu tidak kita lakukan.                                                                                                                                                                                          |
| A.9.2.6              | Apakah hak akses karyawan pada sistem dihapuskan ketika pemberhentian kerja atau kontrak? Dan apakah ada dokumentasi prosedurnya?                                                                                      |
|                      | Ya pasti dihapus. Kalau dokumentasi prosedur tidak ada.                                                                                                                                                                |
| A.9.2.6              | Apakah hak akses fisik karyawan dicabut/dihapus (kunci pintu atau data kunci <i>fingerprint</i> ) ketika pemberhentian kerja atau kontrak? Dan apakah ada dokumentasi prosedurnya?                                     |
|                      | Kalau itu kita juga pasti lakukan. Kalau dokumentasi prosedurnya tidak ada.                                                                                                                                            |
| A.9.4.3              | Apakah terdapat sistem manajemen <i>password</i> yang gencar dan memastikan kualitas <i>password</i> pada <i>server</i> dan perangkat jaringan (harus panjang delapan karakter, huruf besar huruf kecil, dan lainnya)? |
|                      | Ya, untuk perangkat jaringan (seperti <i>switch</i> dan <i>router</i> ) dan <i>server</i> sudah menggunakan <i>password</i> yang aman. Kalau untuk aplikasi masing-masing orang/pengguna.                              |
| A.10.1.1<br>A.17.2.1 | Apa saja yang dienkripsi oleh organisasi? <i>VPN</i> dan <i>HTTPS</i> kan sudah termasuk enkripsi, apa ada selain itu misalnya <i>hardisk</i> ini harus dienkripsi?                                                    |
|                      | <i>VPN</i> kan enkripsi dan <i>SSL</i> enkripsi, ya sudah itu saja. Cuma kalau <i>hardisk</i> harus dikonfigurasi secara <i>RAID</i> , redundan itu. Tapi tidak terenkripsi.                                           |
|                      | Apakah perlindungan yang diterapkan didalam ruangan pusat data?                                                                                                                                                        |

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.11.1.1<br>A.11.1.2<br>A.11.1.4<br>A.11.2.2 | <i>CCTV</i> , kunci <i>fingerprint</i> , pengamanan listrik, <i>diesel generator</i> , <i>UPS</i> , alarm kebakaran dan APAR. Terus pakai gas bukan air dan tidak berbentuk, jadi kalau ada asap langsung nyemprot untuk memadamkan api.                                                                                                                                                                            |
| A.11.1.1                                     | Apa ada alarm yang berbunyi jika ada percobaan pencurian?                                                                                                                                                                                                                                                                                                                                                           |
|                                              | Tidak ada.                                                                                                                                                                                                                                                                                                                                                                                                          |
| A.11.1.2                                     | Siapa saja yang diperbolehkan/diizinkan masuk kedalam pusat data?                                                                                                                                                                                                                                                                                                                                                   |
|                                              | Yang berkepentingan saja. Kalau kesinikan pasti ditanya apa kepentingannya, mau menaruh <i>server</i> atau konfigurasi. Untuk hak akses masuk ke pusat data khusus dimiliki Subdit Infrastruktur dan Direktorat DPTSI-ITS. Jadi nanti akan dibukakan oleh karyawan sini kalau ada yang berkepentingan mau masuk.                                                                                                    |
| A.11.1.2                                     | Apakah terdapat pengelolaan dan pengawasan pada rekaman elektronik kunci <i>fingerprint</i> dan <i>CCTV</i> ?                                                                                                                                                                                                                                                                                                       |
|                                              | Kalau pengelolaan dan peninjauan tidak secara khusus dilakukan, paling kalau ada insiden saja baru ditinjau.                                                                                                                                                                                                                                                                                                        |
| A.11.1.2                                     | Apakah terdapat peninjauan dan pembaharuan/penghapusan/pencabutan hak akses fisik dari pintu <i>fingerprint</i> atau kunci <i>analog</i> yang dimiliki karyawan?                                                                                                                                                                                                                                                    |
|                                              | Untuk peninjauan tidak ada, karena orangnya sedikit. Kalau pencabutan hak akses fisik dilakukan ketika karyawan tersebut keluar atau pindah.                                                                                                                                                                                                                                                                        |
| A.11.1.4                                     | Apakah ada karyawan yang bertugas dimalam hari untuk mengawasi dan menangani masalah yang ada pada jaringan dan <i>server</i> ?                                                                                                                                                                                                                                                                                     |
|                                              | Kita memang membutuhkan tenaga malam. Kalau yang jaga malam sih ada, tapi memang bukan tugasnya jaga malam. Dia karyawan sini juga dan bukan tugasnya secara <i>jobdesc</i> di malam hari, tapi karena dia mau tidur disini dan itu dijadikan fasilitas. Ya mungkin kalau ada <i>troubleshooting</i> sedikit-sedikit ya bisa, tapi kalau masalahnya tidak bisa diselesaikan sendiri ya minta bantuan karyawan pagi. |
| A.11.2.4                                     | Apakah ada kebijakan asuransi yang mengharuskan perawatan perangkat tertentu?                                                                                                                                                                                                                                                                                                                                       |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | Sepertinya kebijakan seperti itu tidak ada.                                                                                                                                                                                                                                                                                                                                                                                            |
| A.11.2.5             | Apakah ada aset yang boleh dibawa keluar kantor seperti laptop dinas?                                                                                                                                                                                                                                                                                                                                                                  |
|                      | Ada laptop dinas, bisa dibawa pulang atau bisa ditaruh disini.                                                                                                                                                                                                                                                                                                                                                                         |
| A.11.2.6<br>A.6.2.2  | Apakah keamanan diterapkan pada aset yang dibawa keluar kantor, seperti harus dipasang perangkat lunak apa dan harus dikonfigurasi bagaimana?                                                                                                                                                                                                                                                                                          |
|                      | Tidak sampai kesitu.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| A.12.1.2             | Apakah perubahan pada organisasi, proses bisnis dan sistem informasi yang mempengaruhi keamanan informasi dikontrol?                                                                                                                                                                                                                                                                                                                   |
|                      | Ada pengelolaan perubahan sistem dan konfigurasi.                                                                                                                                                                                                                                                                                                                                                                                      |
| A.12.1.2<br>A.12.4.1 | Apakah setiap perubahan konfigurasi perangkat seperti si X mengganti konfigurasi terdapat <i>log</i> yang dapat memberikan informasi siapa yang merubah?                                                                                                                                                                                                                                                                               |
|                      | Kalau yang mengganti kita tidak tahu. Tapi kita berkomunikasi saja, karena yang megang cuma tiga orang saja dan bukan orang luar. Kalau tidak ini ya itu, kalau tidak itu ya ini. Jadi walaupun perlu tapi belum terlalu perlu menurut saya.                                                                                                                                                                                           |
| A.12.1.3             | Subdit Infrastruktur kan mengawasi kemampuan <i>server</i> sampai dimana dapat melayani pelanggan. Apakah ada dokumentasi perencanaan manajemen kapasitas sistem yang memudahkan contohnya dalam penambahan kapasitas <i>server</i> kedepan?                                                                                                                                                                                           |
|                      | Secara terencana masih belum ada. <i>Server</i> itu kan sebenarnya ada penanggung jawabnya. Kita punya standar spesifikasi untuk penyediaan <i>server</i> , seperti <i>processor</i> , <i>memory</i> dan sebagainya. Misalnya ditengah operasional kurang, bisa saja diminta ke Subdit Infrastruktur. Ya tapi kita tidak mengawasi penggunaannya seberapa dan sebagainya, ya paling melihat saja tapi tidak melihat sampai kedalamnya. |
| A.12.3.1             | Apakah salinan informasi, perangkat lunak dan <i>clone</i> dari <i>hardisk</i> diambil dan diuji secara teratur berdasarkan kebijakan <i>backup</i> ?                                                                                                                                                                                                                                                                                  |
|                      | Dilakukan <i>backup</i> secara berkala dan ada prosedur yang mengaturnya.                                                                                                                                                                                                                                                                                                                                                              |

|          |                                                                                                                                                                                                                                                                         |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.12.4.4 | Apakah ada dokumentasi persyaratan yang dibuat untuk pengaturan, sinkronisasi dan keakuratan jam (berdasarkan peraturan/hukum, perjanjian kontrak, standar atau kebutuhan internal)?                                                                                    |
|          | Kalau dokumentasi itu tidak kami buat karena tidak ada yang mengharuskannya. Untuk pengaturannya sudah dilakukan pakai <i>NTP</i> .                                                                                                                                     |
| A.12.5.1 | Apakah ada sistem manajemen konfigurasi untuk komputer, <i>server</i> dan perangkat jaringan?                                                                                                                                                                           |
|          | Kalau sistemnya tidak ada, yang ada <i>template</i> untuk <i>server</i> yang berisikan apa saja yang dipasang dan diaktifkan. Misalnya dalam Apache HTTP Server apa saja yang diaktifkan fiturnya. Itupun kami tidak bisa berikan kepada siapapun <i>template</i> -nya, |
| A.12.6.1 | Apakah dalam pemasangan <i>patch</i> ada prosedur dan rekamannya misalnya mana yang belum dan sudah atau bahkan tidak bisa di <i>patch</i> , karena ada beberapa <i>server</i> yang tidak bisa berjalan normal kalau di <i>patch</i> .                                  |
|          | Untuk <i>patch</i> sebenarnya sudah dilakukan dan baik-baik saja selama ini. Kalau sudah dilihat di versinya sudah terbaharui ya sudah. Namun tidak ada prosedur khusus yang diterapkan.                                                                                |
| A.13.1.1 | Apakah terdapat keamanan yang berlapis pada jaringan?                                                                                                                                                                                                                   |
| A.10.1.1 | Kalau akses dari luar, kita pakai <i>VPN</i> . Tapi itu terbatas untuk <i>administrator</i> dan Subdit Pengembangan saja, bukan untuk pengguna. Jadi kalau mengakses kedalam harus pakai <i>VPN</i> .                                                                   |
| A.13.2.2 | Apakah perjanjian menyinggung pengiriman yang aman pada informasi bisnis diantara organisasi dengan pihak ketiga?                                                                                                                                                       |
|          | Ada koordinasi dengan pihak lain yang terkait, namun masih belum ada dokumen yang resmi menyangkut hal tersebut.                                                                                                                                                        |
| A.13.2.4 | Apakah di Subdit Infrastruktur ada persyaratan untuk perjanjian kerahasiaan dan tidak-menyingkap informasi seperti dokumen Kesepakatan Bersama Menjaga Kerahasiaan Aset Sistem Informasi Institusi Dilingkungan Kampus ITS bagi Subdit Pengembangan?                    |

|          |                                                                                                                                                                                                              |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Kalau disini tidak ada, karena mayoritas karyawan tetap semua. Soalnya karyawan disana datang dan pergi karena <i>recruitment</i> -nya kontrak waktu pendek. Mungkin perlu tapi waktu saya disini tidak ada. |
| A.15.1.1 | Apakah ada vendor yang memiliki hak akses pada sistem?                                                                                                                                                       |
|          | Tidak ada. Kalaupun ada ketika pemasangan jaringan, tapi pasti dihapus.                                                                                                                                      |
| A.15.2.1 | Apakah organisasi mengawasi layanan yang diberikan vendor (seperti <i>ISP</i> ) secara berkala?                                                                                                              |
|          | Disinikan ada penyimpanan <i>file log</i> untuk perangkat <i>IAM</i> , jadi bisa dilihat dan ditinjau seberapa banyak jumlah koneksi <i>drop</i> -nya.                                                       |
| A.15.2.1 | Apakah organisasi meninjau layanan yang diberikan oleh vendor melalui rapat dengan vendor?                                                                                                                   |
|          | Kalau rapat sendiri kita sering lakukan dengan vendor. PT. Telkom sendirikan suka mengirimkan orang yang khusus untuk berhubungan dan penanganan masalah di ITS.                                             |
| A.15.2.1 | Apakah organisasi mengadakan audit vendor <i>ISP</i> untuk layanan yang diberikan?                                                                                                                           |
|          | Untuk audit sendiri dilakukan seperti apakah layanan masih sesuai kontrak atau tidak. Hal ini sih tidak dilakukan sering, mungkin setahun sekali.                                                            |
| A.16.1.7 | Apakah terdapat peran dan tanggung jawab khusus untuk analisa forensik? Dan apakah terdapat karyawan yang berkualifikasi/bersertifikasi?                                                                     |
|          | Kalau peran dan tanggung jawab disini tidak didefinisikan secara khusus. Untuk sertifikasi kayaknya belum diadakan untuk forensik.                                                                           |
| A.17.1.1 | Apakah organisasi sudah merencanakan <i>business continuity plan</i> atau <i>disaster recovery plan</i> berikut persyaratannya untuk situasi krisis atau bencana?                                            |
|          | Disini belum ada dokumen <i>DRP</i> .                                                                                                                                                                        |
| A.17.1.3 | Apakah organisasi menguji secara berkala kontrol tentang <i>business continuity</i> ataupun <i>disaster recovery</i> yang dibangun dan diterapkan benar dan efektif ketika krisis atau bencana?              |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Tidak pernah ada pengujian.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| A.17.2.1 | Apakah ada jumlah minimum cadangan komponen dan perangkat jaringan seperti <i>switch</i> , <i>firewall</i> , <i>hardisk</i> dan lainnya yang harus dimiliki?                                                                                                                                                                                                                                                                                                                                                            |
|          | Kalau itu kita tidak punya cadangan, kecuali yang mampu kita beli. <i>Hardisk</i> ada, <i>switch</i> ada tapi bukan yang <i>core</i> seperti <i>access point</i> , <i>access switch</i> dan <i>distribution switch</i> . Kalau yang mahal-mahal seperti <i>firewall</i> dan <i>core switch</i> kita tidak ada.                                                                                                                                                                                                          |
| A.17.2.1 | Jadi bagaimana kalau rusak dan tidak ada cadangannya? Kan perangkat lainnya bisa ikut mati.                                                                                                                                                                                                                                                                                                                                                                                                                             |
|          | Ya biarin sambil menunggu pengadaan. Memang begitu karena kita tidak punya cadangan. Kalau itu kan masalah pendanaan, kita tidak punya pendanaan untuk itu dan administrasinya juga. Ya mungkin secara standar tertentu kita harus menyediakan <i>backup</i> , tapi kenyataannya tidak ada. Kita lebih mengelola di lingkungannya seperti dipasang <i>AC</i> dan sebagainya supaya tidak terjadi hal seperti itu. Kalau faktor eksternal seperti suhu atau listriknya baik, saya kira tahan lama dan tidak mudah rusak. |
| A.18.2.2 | Apakah pimpinan meninjau secara berkala kepatuhan karyawan terhadap kebijakan, prosedur, standar dan persyaratan keamanan lainnya saat menjalankan proses bisnis didalam area tanggung jawab mereka?                                                                                                                                                                                                                                                                                                                    |
|          | Tidak dilakukan peninjauan secara berkala dan efektif terhadap kepatuhan kebijakan atau prosedur keamanan informasi.                                                                                                                                                                                                                                                                                                                                                                                                    |

Narasumber : Achmad Bustari, ST.

Jabatan : Pengembang Jaringan dan Pangkalan Data (Bagian Kelistrikan)

Subdit : Subdirektorat Infrastruktur & Keamanan Teknologi Informasi

| No Annex | Pertanyaan & Jawaban                                                                                                    |
|----------|-------------------------------------------------------------------------------------------------------------------------|
| A.11.1.2 | Apakah area pusat data dilindungi oleh kontrol keluar-masuk untuk memastikan hanya karyawan yang diizinkan boleh masuk? |
|          | Pusat data dilindungi <i>CCTV</i> dan <i>fingerprint</i> untuk masuk.                                                   |
| A.11.1.2 | Siapa saja yang diperbolehkan/diizinkan masuk kedalam pusat data?                                                       |

|          |                                                                                                                                                                                                                                                                            |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Yang memiliki akses masuk itu tim saja. Untuk selain tim, seperti vendor saja tidak memiliki akses masuk. Seperti Telkom kan punya karyawan yang bertugas di DPTSI-ITS kalau ada masalah, dia tidak punya akses masuk. Jadi kalau dia mau masuk harus didampingi oleh tim. |
| A.11.1.4 | Apakah perlindungan fisik terhadap bencana alam, kecelakaan dan tindak kejahatan didesain dan diterapkan?                                                                                                                                                                  |
|          | Untuk perlindungan dari kebakaran dipasang pendeteksi asap, perangkat pemadam otomatis dari gas dan APAR.                                                                                                                                                                  |
| A.11.1.4 | Apakah ada karyawan yang bertugas dimalam hari untuk mengawasi dan menangani masalah yang ada pada jaringan dan <i>server</i> ?                                                                                                                                            |
|          | Karyawan yang berjaga malam ada. Tapi dia tidak bisa menangani kalau ada apa-apa, biasanya karyawan pagi yang bisa menanganinya. Seperti dulu ada <i>server</i> yang mati, saya datang malam-malam buat memperbaikinya.                                                    |
| A.11.1.4 | Apakah ada pelatihan simulasi kebakaran untuk karyawan?                                                                                                                                                                                                                    |
|          | Untuk pelatihan simulasi kebakaran ada, tapi tidak semua karyawan diikutkan. Biasanya kalau diadakan pelatihan yang bisa ikut hanya 2 orang. Memang seharusnya semua karyawan diikutkan.                                                                                   |
| A.11.1.4 | Apakah ada pengujian perangkat kebakaran? Diuji bisa tidak perangkat nantinya kalau terjadi kebakaran.                                                                                                                                                                     |
|          | Kalau pengujian dulu ada tapi semacam simulasi. Jadi kalau ada kebakaran nanti perangkatnya bagaimana, misalnya nanti perangkatnya bunyi dan nanti bagaimana.                                                                                                              |
| A.11.1.4 | Apakah simulasi tersebut sampai mencoba apakah perangkat bisa beroperasi atau tidak?                                                                                                                                                                                       |
|          | Tidak, sampai kesana. Soalnya gas <i>hydrant</i> -nya aja bisa sampai ratusan juta. Jadi kalau diuji apakah bisa berjalan atau tidak bakal mahal. Kalau misalkan perangkat tidak menyala saat kebakaran, hanya bisa dipasrahkan kepada tuhan saja.                         |
| A.11.1.5 | Apakah prosedur untuk bekerja pada area pusat data didesain dan diterapkan (contohnya dilarang makan-minum, merokok dan lainnya)?                                                                                                                                          |

|          |                                                                                                                                                                                                                                                                                                                                            |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Peraturan untuk melarang makan dan minum didalam ruangan pusat data ada. Peraturan tersebut untuk menjaga juga dari tikus. Karena tikus kan ada kalau ada makanan, kalau misalkan tidak ada makanan biasanya tidak ada tikus.                                                                                                              |
| A.11.2.2 | Apakah peralatan dilindungi dari kegagalan daya dan gangguan lainnya yang disebabkan gangguan pada utilitas pendukung?<br><br>Disini dipasang <i>UPS</i> dan <i>generator</i> yang bersifat <i>online</i> . Jadi kalau terjadi mati lampu <i>UPS</i> akan menangani langsung, dan setelah itu <i>generator</i> akan mulai memasok listrik. |
| A.11.2.2 | Apa spesifikasi dari <i>UPS</i> dan <i>generator</i> yang digunakan?<br><br>Untuk <i>generator</i> merek Katapilar dan <i>UPS</i> merek Vector. Kapasitas internal bahan bakar generator 500 liter dan memakan 4 liter setiap satu jam. Itu bisa ditambah lagi kapasitasnya.                                                               |
| A.11.2.2 | Apakah listrik yang dipasok <i>UPS</i> dan <i>generator</i> mencakup seluruh kantor DPTSI-ITS?<br><br>Sesuai kebijakan yang dipasok hanya pusat data saja. Jadi kalau mati lampu, ya ruangan lain akan gelap. Untuk <i>research center</i> sendiri insya allah tahun depan disediakan <i>UPS</i> dan <i>generator</i> .                    |
| A.11.2.2 | Kalau begitu bagaimana dengan perangkat komputer yang digunakan karyawan?<br><br>Kalau untuk masalah itu dipasang <i>UPS</i> yang cukup bagi karyawan untuk menyimpan hasil pekerjaan saja.                                                                                                                                                |
| A.11.2.2 | Apakah ada sumber penerangan dan komunikasi cadangan jika terjadi keadaan darurat?<br><br>Ada senter ukuran besar apabila terjadi mati lampu. Kalau komunikasi cadangan paling <i>walkie-talkie</i> .                                                                                                                                      |
| A.11.2.2 | Apakah pernah terjadi mati lampu yang waktunya lama dan tidak bisa ditangani <i>UPS</i> dan <i>generator</i> ?                                                                                                                                                                                                                             |



|          |                                                                                                                                                                                                                                                                                                                   |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Waktu itu pernah terjadi bahan bakar belum ditambah, kok jam segini belum menyala. Maka dari itu diskusi dengan pusat, bagaimana ini penanganannya. Akhirnya semua <i>server</i> pendukung dimatikan dan hanya <i>server</i> utama saja yang hidup.                                                               |
| A.11.2.1 | Apakah ada perlindungan perangkat dari ancaman petir?                                                                                                                                                                                                                                                             |
|          | Kalau disini standar menggunakan <i>grounding</i> . Jika ada lonjakan listrik berlebih karena petir langsung diarahkan ke tanah.                                                                                                                                                                                  |
| A.11.2.1 | Bagaimana dengan perangkat pendingin ruangan di pusat data?                                                                                                                                                                                                                                                       |
|          | Disini sudah menggunakan <i>AC</i> yang sudah presisi, dimana selain pengaturan suhu ada juga pengaturan kelembaban.                                                                                                                                                                                              |
| A.11.2.1 | Apakah <i>UPS</i> dan <i>generator</i> ditaruh dan dilindungi untuk mengurangi resiko dari ancaman lingkungan dan akses tanpa izin?                                                                                                                                                                               |
|          | <i>Generator</i> dan <i>UPS</i> ditaruh di ruangan yang terkunci dan yang tidak dicurigai terjadinya kebocoran.                                                                                                                                                                                                   |
| A.11.2.3 | Apakah kabel listrik dan jaringan dilindungi dari gangguan dan kerusakan?                                                                                                                                                                                                                                         |
|          | Kabel dilindungi oleh pipa pelindung kabel untuk perlindungannya, jadi kalau di pacul memantul. Tapi kadang kalau dipaksa bisa hancur juga, apalagi kalau pakai mesin. Mungkin dikiranya akar pas ditarik “breet” patah. Setiap sebulan sekali dicek secara fisik apakah ada kabel yang rusak                     |
| A.11.2.3 | Apa tidak ada pemetaan atau kontrol apa yang menandakan lokasi kabel?                                                                                                                                                                                                                                             |
|          | Sebenarnya ada tandanya disetiap berapa meter seperti portal kotak bertuliskan “FO” yang warnanya kuning. Kalau pekerja proyeknya membaca itu insya allah aman, tapi kalau tidak membaca atau portal tersebut lepas kita tidak tahu. Jadi pada dasarnya secara teknis sudah diamankan, tergantung pelaksanaannya. |
| A.11.2.3 | Apakah kabel listrik dan jaringan sudah dipisahkan dalam pemasangannya?                                                                                                                                                                                                                                           |
|          | Kalau didalam gedung sebelumnya di UPT. Perpustakaan lantai 6 tidak dipisah. Sedangkan didalam gedung baru sudah dipisah untuk mencegah gangguan. Kabel listrik dipasang didalam lantai dan kabel jaringan dipasang diatas.                                                                                       |

|          |                                                                                                                                                                                                                                                                                                 |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.11.2.3 | Apakah penempatan <i>power panel</i> dan <i>circuit breaker</i> sudah aman dari akses tanpa izin?                                                                                                                                                                                               |
|          | <i>Power panel</i> dan <i>circuit breaker</i> ditempatkan didalam pusat data, jadi sudah aman.                                                                                                                                                                                                  |
| A.11.2.4 | Apakah <i>UPS</i> dan <i>generator</i> dipelihara secara benar untuk memastikan integritas dan ketersediaanya?                                                                                                                                                                                  |
|          | Untuk <i>generator</i> dilakukan pemanasan mesin selama satu minggu sekali, sekaligus pengecekan air aki dan kondisi radiatornya. Baru saja dilakukan penggantian oli mesin satu tahun sekali. Kalau untuk <i>UPS</i> dilakukan pengecekan informasi pada panel-panel selama dua minggu sekali. |
| A.11.2.4 | Apakah pemeliharaan atau perawatan <i>UPS</i> dan <i>generator</i> sesuai dengan standar tertentu atau spesifikasi vendor?                                                                                                                                                                      |
|          | Biasanya pada setiap perangkat yang dibeli disediakan prosedur cara perawatannya.                                                                                                                                                                                                               |
| A.11.2.4 | Apakah terdapat pencatatan perawatan? Jadi bisa tahu mana yang belum dilakukan perawatan dan mana yang belum.                                                                                                                                                                                   |
|          | Untuk bagian jaringan belum dilakukan. Tapi kalau untuk bagian saya sudah mulai menempelkan label yang ada tanggalnya, jadi kalau sudah saya rawat tinggal saya centang.                                                                                                                        |

Narasumber : Cahya Purnama Dani, A.Md.

Jabatan : Penyusun Laporan dan Pengelola Barang Milik Negara.

Subdit : Subdirektorat Infrastruktur & Keamanan Teknologi Informasi

| No Annex | Pertanyaan & Jawaban                                                                                                                            |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| A.8.1.1  | Apakah aset yang berhubungan dengan informasi dan fasilitas pendukungnya diidentifikasi dan daftar inventarisnya didokumentasikan dan dikelola? |

|                     |                                                                                                                                                                                                                                                       |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | Ada dokumentasinya, daftar inventaris aset milik DPTSI-ITS. Jika ada aset baru maka akan ditambahkan kedalam daftar inventaris. Kita sekarang di ITS pakai E-Aset, dulu SIMAK BMN. Selain itu saya ada <i>file</i> Ms.Excel-nya buat inventaris aset. |
| A.8.1.4             | Apakah ada dokumentasi prosedur pengembalian aset yang dipinjam karyawan yang berhenti bekerja?                                                                                                                                                       |
|                     | Untuk dokumentasi prosedurnya tidak ada, namun kalau ada yang keluar pasti kita cek apakah ada barang yang mereka pinjam.                                                                                                                             |
| A.8.2.2             | Saya pernah melihat ada perangkat komputer yang ditemplei <i>label</i> seperti “sangat rahasia”. Apakah terdapat klasifikasi kerahasiaan pada perangkat?                                                                                              |
|                     | Kalau itu karyawan sendiri yang iseng menempelkan dari tempelan waktu SNMPTN. Bahkan ada yang ditemplei di tong sampah.                                                                                                                               |
| A.8.3.2<br>A.11.2.7 | Apakah media penyimpanan (media kertas dan elektronik) dibuang secara aman ketika tidak diperlukan menggunakan prosedur formal?                                                                                                                       |
|                     | Kalau untuk dokumen sudah ada prosedur Pemusnahan Dokumen. Sedangkan kalau untuk perangkat yang sudah rusak atau tidak bisa digunakan yang mengurus itu pak Rahmat di BAUK-ITS. Jadi saya memberikan perangkat tersebut dan berita acaranya.          |
| A.8.3.2<br>A.11.2.7 | Bagaimana dengan <i>CD/DVD</i> yang dibuang?                                                                                                                                                                                                          |
|                     | Kalau itu Subdit masing-masing yang mengatur.                                                                                                                                                                                                         |
| A.11.2.4            | Apakah <i>server</i> dan perangkat jaringan dipelihara secara berkala, misalnya pembersihan debu?                                                                                                                                                     |
|                     | Kalau disini dilakukan tapi tidak dicatat harus kapan bersih-bersih dan lihat kondisi saja. Jadi tidak ada jadwal bersih-bersih.                                                                                                                      |
| A.11.2.4            | Bagaimana kalau terjadi kerusakan pada perangkat jaringan seperti <i>switch</i> atau <i>firewall</i> ?                                                                                                                                                |
|                     | Biasanya digunakan perangkat cadangan, kalau tidak ada cadangannya menggunakan perangkat pengganti tapi kecepatannya turun. Contohnya <i>distribution switch</i> yang rusak bisa menggunakan beberapa <i>access switch</i> .                          |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.11.2.5 | Apakah perangkat keras/lunak, peralatan dan informasi tidak boleh dibawa keluar organisasi tanpa izin terlebih dahulu?                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|          | Untuk barang yang dipinjam keluar harus mengajukan surat permohonan berupa Berita Acara Perminjaman Barang Peminjaman tidak sering dilakukan dan biasanya dilakukan oleh unit atau jurusan yang ada di ITS. Contohnya dulu ada peminjaman <i>access point</i> untuk keperluan meningkatkan sinyal <i>Wi-Fi</i> pada acara tertentu. Lama peminjamannya juga sebentar, biasanya satu hari.                                                                                                                                                                       |
| A.8.1.4  | Apakah laptop dinas yang ada disini dimiliki karyawan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|          | Tidak, karena itu BMN. Jadi dikembalikan lagi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| A.11.2.5 | Apakah ada perjanjian untuk peminjaman laptop dinas?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|          | Perjanjian tidak ada, yang ada itu Berita Acara Pemakaian Barang Inventaris kalau dia membawa barang tersebut. Kalau misalkan peminjamannya sehari dua hari biasanya tidak pakai berta acara, tapi kalau lama harus pakai. Nanti kan kalau ada pemeriksaan lebih mudah.                                                                                                                                                                                                                                                                                         |
| A.11.2.6 | Apa yang dilakukan jika laptop dinas hilang?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|          | Kalau misalkan hilang karena kepentingan dinas kan harus melaporkan kehilangan barang ke polisi. Nanti surat keterangan tadi dipakai untuk bukti mengurus di pusat.                                                                                                                                                                                                                                                                                                                                                                                             |
| A.17.2.1 | Apa saja cadangan komponen untuk perangkat yang dimiliki?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|          | <i>Hardisk</i> untuk <i>server</i> . Kalau untuk komponen lain seperti <i>processor</i> , <i>memory</i> atau <i>motherboard</i> biayanya mahal. Contohnya <i>processor</i> sendiri saja semakin lama harganya semakin murah. Jadi kalau menyimpan cadangan tidak irit biaya dan dengan harga segitu sudah bisa membeli yang lebih cepat. Untuk <i>memory</i> sendiri, <i>server</i> masih bisa jalan kan kalau cuma dipasang satu meski kecepatannya turun. Kalau <i>hardisk</i> memang sesuai kebutuhan harus ada, jadi kalau ada yang rusak tinggal dipasang. |
| A.17.2.1 | Apa saja cadangan perangkat jaringan seperti <i>switch</i> atau <i>firewall</i> yang dimiliki?                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|          |                                                                                                                                                                                                                                                                                                                                               |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Perangkat jaringan kan bukan komponen, biasanya ada cadangannya. Untuk <i>access point</i> kita ada banyak cadangan, bahkan kita dapat perangkat dari pengadaan kebanyakan merek Cina semua karena masuk spesifikasinya. Tapi lumayan bagus juga sih. Kalau <i>distribution switch</i> ada tapi tadi kepakai semua untuk pemasangan jaringan. |
| A.17.2.1 | Apakah ada jumlah minimum cadangan komponen dan perangkat jaringan seperti <i>switch</i> , <i>firewall</i> , <i>hardisk</i> dan lainnya yang harus dimiliki?                                                                                                                                                                                  |
|          | Tidak ada, tapi kita usahakan harus ada cadangannya.                                                                                                                                                                                                                                                                                          |
| A.17.2.1 | Apakah pernah terjadi kerusakan namun cadangannya tidak ada?                                                                                                                                                                                                                                                                                  |
|          | Pernah, itukan cadangan jumlahnya cuma berapa. Misalkan listrik mati mendadak dan ada alat yang peka, alat tadi jadi bermasalah.                                                                                                                                                                                                              |
| A.17.2.1 | Berapa lama waktu perangkat atau komponen yang dibeli melalui pengadaan sampai?                                                                                                                                                                                                                                                               |
|          | Biasanya satu minggu baru sampai.                                                                                                                                                                                                                                                                                                             |

Narasumber : Jananta Permata Putra, S.ST

Jabatan : Pengembang Jaringan dan Pangkalan Data (Bagian Jaringan)

Subdit : Subdirektorat Infrastruktur & Keamanan Teknologi Informasi

| No Annex           | Pertanyaan & Jawaban                                                                                                                                                                                                                                     |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.9.2.2            | Apakah dokumentasi tentang hak akses <i>administrator</i> yang dimiliki karyawan pada aset tertentu? Jadi bisa tahu bahwa pak X punya akses <i>administrator</i> ke <i>firewall</i> , <i>router</i> dan lainnya.                                         |
|                    | Pencatatan terpisahnya tidak ada, misalnya ada <i>server</i> yang dipegang tiga orang maka yang bisa mengakses ketiga orang itu. Kalau satu orang kan bahaya. Untuk yang megang perangkat jaringan seperti CISCO ASA Firewall juga lebih dari dua orang. |
| A.9.2.3<br>A.6.1.2 | Apakah Subdit Infrastruktur memiliki hak akses pada <i>server</i> yang diberikan ke Subdit Pengembangan?                                                                                                                                                 |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Kalau <i>server</i> -nya untuk layanan ITS, kita Subdit Infrastruktur tahu semua karena kita yang memberikan. Soalnya kalau ada apa-apa itu kita yang menangani untuk masalah sistemnya, kayak <i>server</i> atau sistem operasi itu kita. Kalau Subdit Pengembangan hanya aplikasinya saja, jadi <i>password</i> aplikasi kita tidak punya.                                                                                                              |
| A.9.2.4  | <p>Bagaimana kalau ada yang lupa <i>password</i> untuk masuk kedalam sistem operasi pada <i>server</i>?</p> <p>Akun kan untuk mereka <i>login</i> ke <i>server</i>, jadi kalau mereka lupa kita yang melakukan <i>reset</i>. Terus kita beritahu <i>password</i> barunya.</p>                                                                                                                                                                             |
| A.9.2.4  | <p>Apakah <i>password default</i> pabrik sistem atau perangkat lunak diganti saat pemasangan?</p> <p>Pasti kita ganti. Kita juga kan manajemen konfigurasi beberapa perangkat.</p>                                                                                                                                                                                                                                                                        |
| A.9.4.3  | <p>Apakah terdapat sistem manajemen <i>password</i> yang gencar dan memastikan kualitas <i>password</i> pada <i>server</i> (harus panjang delapan karakter, huruf besar huruf kecil, dan lainnya)?</p> <p>Iya, kalau <i>server</i> buat yang butuh keamanan tinggi, kita buat <i>password</i> ke sistem operasi yang <i>random</i> seperti itu. Tapi kalau pengguna yang melekat ke akun aplikasinya tergantung orangnya masing-masing mau diisi apa.</p> |
| A.9.4.3  | <p>Apakah <i>password</i> yang diberikan ada tanggal kadaluarsanya dan harus diganti?</p> <p>Kita sih tidak memaksa seperti itu, tergantung orangnya masing-masing. Jadi ya sudah <i>password</i>-nya ini, mau diganti atau tidak terserah.</p>                                                                                                                                                                                                           |
| A.9.4.4  | <p>Apakah penggunaan aplikasi utilitas yang mampu merubah sistem dan kontrol aplikasi (terminal, CMD, <i>control panel</i> dan lainnya) dibatasi dan dikontrol secara ketat?</p> <p>Untuk pembatasan seperti itu kita tidak lakukan. Karena kalau sudah diberikan akses ya semua yang didalamnya bisa kita pakai.</p>                                                                                                                                     |
| A.11.2.4 | Kalau perangkat masih ada garansinya kan bisa menghubungi vendor kalau terjadi kerusakan. Bagaimana dengan perangkat yang sudah melewati batas garansi?                                                                                                                                                                                                                                                                                                   |

|                      |                                                                                                                                                                                    |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | Kalau garansinya habis dan rusak, ya terpaksa beli yang baru.                                                                                                                      |
| A.11.2.4             | Apakah terdapat perawatan perangkat ( <i>switch</i> , <i>router</i> dan lainnya) secara berkala dan pencatatannya, seperti pembersihan debu dan pengecekan perangkat secara fisik? |
|                      | Tidak, itu tidak rutin. Untuk <i>switch</i> semacam membersihkan itu tergantung kita ada waktu longgar atau tidak. Jadi tidak ada jadwal rutin yang tetap.                         |
| A.11.2.8             | Apakah pengguna menjamin bahwa peralatan yang tidak diawasi telah terlindungi, contohnya <i>logout</i> otomatis atau pembatasan waktu <i>session</i> ?                             |
|                      | Sudah diterapkan kesemuanya, dan khusus untuk jaringan biasanya akan diputus kalau sudah lama tidak dipakai.                                                                       |
| A.12.1.2             | Apakah terdapat rekaman setiap perubahan konfigurasi jaringan dan <i>server</i> , seperti penambahan <i>rule</i> baru pada <i>firewall</i> ?                                       |
|                      | Tidak ada catatannya. Itu sih semua yang megang bisa lihat sebenarnya. Misalkan mem- <i>block port</i> ini, jadi saya bisa lihat bahwa <i>port</i> ini telah di <i>block</i> .     |
| A.12.1.2<br>A.12.4.1 | Apakah setiap perubahan konfigurasi perangkat seperti CISCO ASA Firewall terdapat <i>log</i> yang dapat memberikan informasi siapa yang merubah?                                   |
|                      | Tidak ada dan tidak tahu siapa yang merubah.                                                                                                                                       |
| A.12.1.2             | Apakah setiap perubahan konfigurasi pada jaringan misalkan <i>firewall</i> diperlukan izin kepada Kasubdit Infrastruktur terlebih dahulu?                                          |
|                      | Tidak juga sih.                                                                                                                                                                    |
| A.12.1.2             | Apakah ada waktu khusus untuk perubahan konfigurasi perangkat, misalkan malam?                                                                                                     |
|                      | Tidak, bisa setiap saat selama dibutuhkan.                                                                                                                                         |
| A.12.1.3             | Apakah kemampuan atau kapasitas dari <i>server</i> dan jaringan dalam menangani pengguna diawasi dan diatur kemampuannya untuk memenuhi kebutuhan kedepan?                         |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Tidak ada, kecuali kalau memang <i>server</i> -nya berat ya kita cek apa yang membuat berat. Misalkan kalau yang membuat berat gara-gara pengguna, kita tambahkan sumber dayanya.                                                                                                                                                                                                                                                                                                      |
| A.12.2.1 | Apakah kontrol pendeteksi, perlindungan dan perbaikan untuk menangani <i>malware</i> diterapkan pada perangkat <i>server</i> ?                                                                                                                                                                                                                                                                                                                                                         |
|          | Ada, pakai ClamAV.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| A.12.3.1 | Apakah salinan informasi, perangkat lunak dan <i>clone</i> dari <i>hardisk</i> diambil dan diuji secara teratur berdasarkan kebijakan <i>backup</i> ?                                                                                                                                                                                                                                                                                                                                  |
|          | Ada <i>server backup</i> , misalnya <i>server</i> seperti <i>DNS</i> dan <i>email</i> disimpan disatu <i>server</i> yang sama untuk melakukan <i>backup</i> . Kalau <i>backup</i> untuk konfigurasi <i>switch</i> dan <i>router</i> -nya itu ada <i>server backup</i> -nya tersendiri, dipisahkan untuk <i>DNS</i> dan <i>email</i> . Kalau <i>backup</i> konfigurasi tergantung adanya perubahan, kalau ada perubahan di <i>backup</i> , kalau tidak ada perubahan ya tetap yang itu. |
| A.12.3.1 | Apakah ada pengujian hasil <i>backup</i> secara berkala untuk memastikan keandalannya (tidak <i>corrupt</i> atau dapat dibaca)?                                                                                                                                                                                                                                                                                                                                                        |
|          | Kalau pengujian sih tidak ada ya. Tapi selama kita <i>restore</i> pasti bisa, contohnya kan ada <i>switch</i> yang rusak dan diganti baru. Setelah <i>restore</i> itu pasti bisa.                                                                                                                                                                                                                                                                                                      |
| A.12.4.1 | Apakah perekaman <i>log</i> aktifitas pengguna, <i>error</i> , dan kejadian keamanan informasi lainnya dibuat, disimpan dan ditinjau secara berkala?                                                                                                                                                                                                                                                                                                                                   |
|          | Kita sih ada <i>server</i> sendiri untuk penyimpanan <i>log</i> apapun yang disimpan sampai batas waktu tertentu. Selain itu ada <i>dashboard sensor</i> yang berisi analisa dari <i>log</i> yang dikumpulkan, yaitu AllienVault.                                                                                                                                                                                                                                                      |
| A.12.5.1 | Apakah DPTSI-ITS menyimpan perangkat lunak sebelumnya sekaligus catatan lengkap yang berisikan informasi perangkat lunak, prosedur, dan rincian konfigurasi?                                                                                                                                                                                                                                                                                                                           |
|          | Kalau menyimpan versi lama sih iya. Tapi kalau sampai konfigurasi, dokumentasi informasi sampai prosedurnya itu tidak sampai kesana.                                                                                                                                                                                                                                                                                                                                                   |
| A.12.6.1 | Apakah <i>server</i> dan perangkat jaringan dimutakhirkan dengan versi <i>patch</i> terbaru secara berkala?                                                                                                                                                                                                                                                                                                                                                                            |



|                      |                                                                                                                                                                                                                                                                                                                                           |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | Dilakukan tapi kalau secara berkala sih tidak. Kalau misalkan ada waktu meng- <i>update</i> ya kita meng- <i>update</i> . Kalau misalkan ada <i>update</i> baru tidak langsung dipasang, tapi dilihat juga apakah fungsinya dapat berjalan di versi terbaru. Kalau ada fungsi yang terganggu maka tetap menggunakan versi yang lama.      |
| A.12.6.1             | Apakah terdapat penjadwalan dan pencatatan untuk pemutakhiran versi <i>patch</i> terbaru?                                                                                                                                                                                                                                                 |
|                      | Tidak ada.                                                                                                                                                                                                                                                                                                                                |
| A.13.1.1             | Apakah ada pembagian <i>bandwith</i> dan pembatasan <i>internet</i> ?                                                                                                                                                                                                                                                                     |
|                      | Saat ini kan <i>bandwith</i> -nya masih mencukupi, terus untuk pengguna sendiri kita tidak batasi <i>bandwith</i> -nya, ya kita <i>loss</i> -kan saja. Jadi ya misalkan unit sini sama unit sana perlakuannya sama. Kalau untuk Youtube, media sosial dan lainnya itu kita kurangi <i>bandwith</i> -nya agar tidak habis semuanya kesana. |
| A.13.2.4             | Apakah waktu mas kerja disini ada perjanjian menjaga kerahasiaan seperti dokumen Kesepakatan Bersama Menjaga Kerahasiaan Aset Sistem Informasi Institusi Dilingkungan Kampus ITS bagi Subdit Pengembangan? Dan apakah mas itu karyawan PNS?                                                                                               |
|                      | Kayaknya tidak deh. Saya non-PNS.                                                                                                                                                                                                                                                                                                         |
| A.15.1.1             | Apakah ada vendor yang memiliki hak akses pada sistem?                                                                                                                                                                                                                                                                                    |
|                      | Tidak ada. Misalkan vendor tersebut yang mengembangkan jaringan/ sistem dan untuk sementara dia membuat akun untuk mengembangkan. Biasanya kalau sudah selesai dihapus.                                                                                                                                                                   |
| A.16.1.5             | Apakah setiap insiden keamanan informasi ditanggapi sesuai dengan prosedur yang terdokumentasi (misalnya <i>troubleshooting</i> untuk <i>server</i> )?                                                                                                                                                                                    |
|                      | Tidak ada secara terdokumentasi.                                                                                                                                                                                                                                                                                                          |
| A.18.2.3<br>A.12.6.1 | Apakah sistem informasi ditinjau secara berkala agar patuh terhadap kebijakan dan standar keamanan informasi organisasi, contoh dengan penetrasi tes dan pemindaian kerentanan?                                                                                                                                                           |

|  |                                                                                                                                                            |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Kalau dilakukan sih iya untuk pengecekan kerentanan itu, tapi tidak dilakukan rutin. Tergantung ada waktu luang atau tidak, dan jika terjadi insiden saja. |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------|

Narasumber : Faishal Halim Saputra, S.ST

Jabatan : Pengembang Jaringan dan Pangkalan Data (Bagian Jaringan)

Subdit : Subdirektorat Infrastruktur & Keamanan Teknologi Informasi

| No Annex | Pertanyaan & Jawaban                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.12.4.1 | Apa saja <i>log</i> yang disimpan <i>SIEM</i> AlienVault?                                                                                                                                                                                                                                                                                                                                                                                                        |
|          | <i>Log</i> -nya dari <i>server</i> saja, dimana setiap <i>server</i> dipasang <i>agent</i> yang berkewajiban mengirimkan <i>file log</i> tadi. Misalnya dari luar mencoba <i>bruteforce</i> ke kita, nah nanti ada informasi <i>IP address</i> -nya yang bisa kita buat <i>rule</i> -nya di <i>firewall</i> buat diblok. Untuk perangkat jaringan semacam <i>router</i> dan <i>firewall</i> tidak termasuk cakupan karena tidak bisa dipasang <i>agent</i> tadi. |
| A.12.4.1 | Sampai berapa lama penyimpanan <i>file log</i> yang disimpan <i>SIEM</i> AlienVault?                                                                                                                                                                                                                                                                                                                                                                             |
|          | Ya sampai <i>hardisk</i> -nya penuh. Tidak ada keharusan menyimpan selama 6 bulan dan lainnya.                                                                                                                                                                                                                                                                                                                                                                   |
| A.12.5.1 | Apakah ada sistem manajemen konfigurasi untuk komputer, <i>server</i> dan perangkat jaringan?                                                                                                                                                                                                                                                                                                                                                                    |
|          | Tidak ada, kalau mau konfigurasi biasanya udah didalam kepala. Misalnya mau buat <i>proxy</i> , ya udah kita buat dari awal.                                                                                                                                                                                                                                                                                                                                     |
| A.13.1.1 | CISCO ASA Firewall kan punya fitur <i>VPN</i> , <i>anti-virus</i> , <i>anti-spam</i> , <i>IPS</i> dan <i>IDS</i> , dan setiap fitur berlisensi. Apa saja lisensi fitur yang dibeli?                                                                                                                                                                                                                                                                              |
|          | <i>Firewall</i> saja.                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| A.13.1.1 | Apa fungsi Tsubame dan Honeypot Dionaea, lalu bagaimana pengelolaannya?                                                                                                                                                                                                                                                                                                                                                                                          |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Itu kan dari kerja sama dengan KEMENKOMINFO dan <i>server</i> -nya dari mereka ditaruh disini. Jadi intinya mereka dikasih <i>IP address</i> publik supaya bisa <i>filter</i> keamanan di PTN-PTN. Sistemnya seperti apa kita tidak tahu karena kita juga tidak dikasih akses untuk masuk ke <i>server</i> itu. Untuk Honeypot Dionaea juga dikelola mereka.                                                                          |
| A.13.1.1 | Apakah Tsubame memerlukan <i>log</i> dari <i>server</i> yang ada? Dan apakah DPTSI-ITS pernah mengirimkan <i>file log</i> ke <i>CSRIT</i> untuk dianalisa lebih lanjut?                                                                                                                                                                                                                                                               |
|          | Tidak ada penyimpanan <i>log</i> oleh Tsubame. Jadi kan Tsubame itu mengirim email yang isinya <i>IP address</i> ini kena serang, tidak ada pertukaran informasi atau <i>file log</i> ke mereka.                                                                                                                                                                                                                                      |
| A.13.1.1 | Apa saja yang dilakukan ketika terjadi serangan <i>hacker</i> ?                                                                                                                                                                                                                                                                                                                                                                       |
|          | Biasanya dia mengoprek di <i>www</i> -nya, entah merubah atau menghapus konten, atau merubah <i>file php</i> -nya. Penanganannya biasanya di <i>restore</i> . Kalau portal ITS kita tingkatkan keamanannya, tapi disinikan ada <i>website</i> yang <i>co-location</i> dari jurusan dan mereka yang mengelola. Jadi kalau mereka kena <i>hack</i> ya, mereka sendiri yang melakukan dengan informasi celah keamanan yang kita berikan. |

Narasumber : Satriyo Wicaksono, S.Kom.

Jabatan : Pengembang Jaringan dan Pangkalan Data (Bagian Jaringan)

Subdit : Subdirektorat Infrastruktur & Keamanan Teknologi Informasi

| No Annex | Pertanyaan & Jawaban                                                                                                                                                                        |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.9.4.4  | Apakah penggunaan aplikasi utilitas yang mampu merubah sistem dan kontrol aplikasi dibatasi dan dikontrol secara ketat?                                                                     |
|          | Tidak ada pembatasan khusus untuk aplikasi semacam CMD, terminal dan lainnya. Kalau orangnya bisa mengakses <i>server</i> , maka dia bisa pakai terminal, konfigurasi dan aplikasi lainnya. |
| A.10.1.1 | Apakah setiap halaman <i>login</i> perangkat jaringan seperti <i>router</i> dan <i>firewall</i> dilindungi oleh <i>SSL/TLS</i> ?                                                            |

|          |                                                                                                                                                                                                                                                                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Ya, pakai DigiCert.                                                                                                                                                                                                                                                                                                                                   |
| A.10.1.1 | Apakah <i>login</i> yang dilakukan <i>administrator</i> ke <i>server</i> ditolak jika tidak menggunakan <i>VPN</i> ?                                                                                                                                                                                                                                  |
|          | <i>IP address</i> -nya tidak bisa masuk, ketutup di <i>firewall</i> .                                                                                                                                                                                                                                                                                 |
| A.10.1.2 | Apakah untuk koneksi <i>VPN</i> menggunakan kunci enkripsi atau <i>password</i> ?                                                                                                                                                                                                                                                                     |
|          | Ada yang pakai kunci enkripsi dan ada juga yang pakai kunci, tergantung kebutuhan mas.                                                                                                                                                                                                                                                                |
| A.10.1.2 | Apakah kebijakan mengenai penggunaan, perlindungan dan umur kunci kriptografi dibuat dan diterapkan pada keseluruhan daur hidupnya?                                                                                                                                                                                                                   |
|          | Tidak ada, karena kita anggap sudah pada tahu. Jadi panduan bagaimana cara seperti penyimpanannya dan mendistribusikannya itu tidak ada.                                                                                                                                                                                                              |
| A.10.1.2 | Apakah kunci enkripsi dan <i>password</i> tersebut diganti secara berkala?                                                                                                                                                                                                                                                                            |
|          | Kalau <i>password</i> tergantung penggunaanya. Kalau kunci enkripsi berkalanya tidak sering-sering amat, mungkin satu tahun sekali. Atau sekiranya kita merasa perlu misalnya ada yang menaruh <i>file</i> kunci di <i>flashdisk</i> terus hilang. Kalau untuk <i>file</i> kunci DigiCert juga kan bisa diganti ke DigiCert-nya jika dirasa terbajak. |
| A.11.2.4 | Apakah peralatan dipelihara/dirawat secara benar untuk memastikan integritas dan ketersediaanya?                                                                                                                                                                                                                                                      |
|          | Pemeliharaan biasanya dilakukan masing-masing oleh karyawan yang bertugas dan tidak secara berkala sih dilakukan.                                                                                                                                                                                                                                     |
| A.11.2.4 | Apakah perawatan dilakukan untuk perangkat komputer?                                                                                                                                                                                                                                                                                                  |
|          | Biasanya perawatan dilakukan pada jaringan, tidak dilakukan perawatan komputer secara khusus.                                                                                                                                                                                                                                                         |
| A.11.2.4 | Bagaimana kalau terjadi kerusakan terhadap perangkat?                                                                                                                                                                                                                                                                                                 |
| A.11.1.2 | Kalau perangkat masih ada garansinya, maka menghubungi vendor untuk diperbaiki. Sebelumnya kita mengecek dulu apa yang rusak, misalkan pada <i>server</i> setelah dicek ada indikasi “wah <i>motherboard</i> -nya nih”. Jadi kita menghendaki jawaban tersebut keluar dari vendor. Pas vendor datang untuk                                            |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <p>mengecek, kita tungguin. Pada saat mengecek vendor bisa langsung bilang “oh rusaknya ini hih” dan ada juga yang “pak ini harus kita harus bawa untuk mengecek lebih dalam”. Kalau perangkat tersebut sudah beres ditempat kita ya sudah. Sedangkan kalau perangkat dibawa, <i>hardisk</i>-nya kita lepas. Jadi yang dibawa memang yang diindikasi rusak, misalnya kalau <i>memory</i>-nya yang rusak, ya <i>memory</i>-nya saja yang dibawa. Kalau <i>motherboard</i>, ya <i>motherboard</i>-nya yang dibawa. Yang pasti <i>hardisk</i> kita amankan.</p> |
| A.11.2.4 | <p>Apa saja perangkat yang bisa diperbaiki sendiri oleh karyawan tanpa bantuan vendor?</p> <p>Perangkat seperti <i>server</i>, <i>router</i>, <i>switch</i>, <i>access point</i>, <i>firewall</i>, <i>printer/scanner/fax</i>, <i>generator</i>, <i>UPS</i> atau <i>AC</i> tidak bisa diperbaiki sendiri oleh karyawan. Mungkin kita hanya mampu memperbaiki sendiri perangkat komputer yang digunakan.</p>                                                                                                                                                  |
| A.11.2.4 | <p>Apakah terdapat rekaman riwayat perbaikan pada perangkat yang berisikan semua kesalahan sebenarnya atau yang diperkirakan, dan semua tindakan pencegahan atau perbaikannya?</p> <p>Tidak ada rekaman perbaikan perangkat secara rinci disini.</p>                                                                                                                                                                                                                                                                                                         |
| A.11.2.4 | <p>Apakah dilakukan pengecekan kode <i>BIOS</i> dengan yang ada di <i>website</i> perangkat untuk melindungi perangkat dari perubahan tanpa izin?</p> <p>Waktu kita beli kita pastikan dari <i>delivery order</i>-nya. Kita cek spesifikasi umumnya saja sesuai yang kita minta, misalnya <i>memory</i> sekian dan <i>processor</i> sekian, ya itu aja yang kita cek. Kalau sampai ke <i>BIOS</i>-nya, ya sampai <i>BIOS</i>-nya kita cek.</p>                                                                                                               |
| A.12.1.1 | <p>Apakah prosedur operasional didokumentasikan dan tersedia untuk Subdit Infrastruktur yang membutuhkan?</p> <p>Ada dokumen prosedurnya didalam ISO 9000. Dokumennya ada di Subdit Pelayanan. Karena itu semua sudah diluar kepala maka kami tidak pegang. Mungkin kalau ada karyawan baru karyawan itu bisa membaca dokumen ISO tersebut.</p>                                                                                                                                                                                                              |
| A.12.1.1 | <p>Apakah ada panduan konfigurasi atau pengaturan yang aman untuk <i>server</i> dan perangkat jaringan yang diterapkan secara konsisten?</p>                                                                                                                                                                                                                                                                                                                                                                                                                 |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <p>Kalau itu tergantung permintaan mas. Misalnya Subdit Pengembangan mintanya <i>VPS</i>, ya sudah kita berikan <i>VPS</i>. Kalau mereka mintanya “tolong dong dikasih layanan ini-ini, yang satu ini dimatikan”, ya kita lakukan. Kalau orangnya sudah mengerti, biasanya urusan konfigurasi sistemnya mereka kerjakan sendiri. Ada juga yang hanya mengerti pemrograman dan minta pokoknya aplikasi saya bisa jalan, nah itu kita bantu pemasangannya. Tapi kalau urusan kita di Subdit Infrastruktur, kan kita juga mengelola <i>server</i> dan aplikasi juga, seperti Webmail ITS, <i>proxy</i> dan lainnya itu kita buka tutup sendiri untuk pengaturan <i>firewall</i>-nya.</p> |
| A.12.1.2 | Apakah setiap perubahan konfigurasi pada jaringan diperlukan izin kepada Kasubdit Infrastruktur terlebih dahulu?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|          | Biasanya kalau itu kan didiskusikan dulu sebelum kita bekerja, misalnya kita disuruh pakai satu <i>core switch</i> saat memasang jaringan, kalau kita malah pakai dua <i>core switch</i> kan bermasalah.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| A.12.1.2 | Apakah setiap perubahan konfigurasi pada jaringan yang dilakukan didokumentasikan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|          | Kalau memang perubahannya biasa kita lakukan dan diluar kepala, tidak kita dokumentasikan. Kalau memang tidak pernah kita lakukan pasti didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| A.12.1.2 | Apakah ada waktu khusus untuk perubahan konfigurasi perangkat, misalkan malam atau saat jumlah pengguna sedikit?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|          | Kalau itu berdasarkan kebutuhan, misalnya dari jurusan A mau menambahkan segmen <i>IP address</i> itu baru dilakukan perubahan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| A.12.1.3 | Apakah kemampuan atau kapasitas dari <i>server</i> dan jaringan dalam menangani pengguna diawasi dan diatur kemampuannya untuk memenuhi kebutuhan kedepan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|          | Pakai aplikasi <i>open source</i> Cacti. Misalnya penggunaan <i>bandwidth</i> pada <i>backbone</i> dengan MMT-ITS besarnya 10 MB, nah kita bisa lihat per 5 menit itu apakah penggunaannya melebihi dari itu. Cacti kerjanya pakai protokol <i>SNMP</i> dia. Untuk melihat kapasitas <i>hardisk server</i> juga bisa pakai Cacti.                                                                                                                                                                                                                                                                                                                                                     |
| A.12.1.3 | Apakah ada penghapusan data-data atau <i>temporary</i> yang tidak penting di <i>server</i> untuk mengurangi penggunaan kapasitas <i>hardisk</i> ?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Tidak juga sih, kan di <i>server</i> ada logrotate di Linux Debian. Logrotate itu <i>default</i> -nya setiap <i>log</i> yang usianya lebih dari 3 hari dihapus sama dia. Cuman kalau logrotate-nya tidak diaktifkan harus kita hapus setiap hari.                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| A.12.1.3 | <p>Bapak kan melakukan pengawasan penggunaan <i>bandwith</i> sekaligus mengatur berapa besarnya <i>bandwith</i>, terus kan ada formulir Permintaan Pelebaran <i>Bandwith</i> yang meminta untuk diatur besarnya <i>bandwith</i>. Apa sih persyaratan dan perbedaanya?</p> <p>Kalau saya sih gampang cuma mengikuti apa kata Kasubdit Infrastruktur saja, kan tugas saya pelaksana dan tidak ada wewenang. Biasanya itu kejadian kalau unit atau jurusan tertentu lagi ada kegiatan yang perlu akses khusus. Misalnya direktorat mengadakan acara dan mengundang pejabat X yang perlu koneksi lebih cepat, ya kita lakukan.</p>                                                         |
| A.12.1.3 | <p>Jadi tugas bapak hanya mengawasi dan membuat laporan penggunaan <i>bandwith</i> ke pak Royyana (Kasubdit Infrastruktur)?</p> <p>Ya, tapi kalau kondisi stabil begini tidak ada yang perlu saya laporkan.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| A.12.1.4 | <p>Apa perbedaan <i>server development</i>, <i>server live</i> dan <i>server co-location</i>?</p> <p>Kalau <i>server development</i> itu <i>server</i> yang kita sediakan untuk Subdit Pengembangan mengembangkan aplikasinya, jadi dia tidak perlu menyediakan sendiri. Kalau <i>server live</i> itu untuk <i>server</i> yang kita sediakan untuk aplikasi yang beroperasi atau sudah selesai dikembangkan. Sedangkan <i>server co-location</i> itu kita menyediakan tempat sama jaringan, dimana <i>server</i> mereka bawa sendiri. Misalkan si A mau menaruh <i>server</i> di kita, nah itu kita sediakan tempat, kabel dan persiapannya.</p>                                       |
| A.12.1.4 | <p>Apa untuk pindah dari <i>server development</i> ke <i>server live</i> itu perlu izin tambahan atau langsung dirubah fungsinya yang tadinya <i>server development</i> ke <i>server live</i>?</p> <p>Kalau itu dari Subdit Pengembangan sendiri, jadi pada pengembangan aplikasi kan tidak bisa jalan sendiri dan harus dengan sepersetujuan Kasubdit Pengembangannya. Nah dengan Kasubdit Pengembangannya, mereka menaruh aplikasinya di <i>server live</i>. Kalau urusan sama kita itu buka tutup <i>firewall</i>-nya mas. Jadi untuk <i>server development</i> hanya kita buka untuk Subdit Pengembangan saja, sedangkan untuk <i>server live</i> kita buka untuk semua orang.</p> |

|                     |                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.12.1.4<br>A.9.4.3 | Apakah <i>server development</i> atau <i>server live</i> memiliki sistem manajemen <i>password</i> yang gencar dan memastikan kualitas <i>password</i> (seperti harus mengganti <i>password</i> yang diberikan)?                                                                                                                                                    |
|                     | Tidak ada, kan kita biasanya tidak ada pengaturan seperti itu. Jadi <i>password</i> udah kita kasih, ya sudah itu urusan mereka mau <i>password</i> -nya diganti silahkan atau mau diganti secara berkala juga silahkan. Karena setelah kita buat, kita tidak ikut kedalam sistemnya itu. Kalau tidak bisa di <i>ping</i> atau tidak bisa apa, baru kita yang urus. |
| A.12.1.4            | Apakah pengujian perangkat lunak atau sistem operasi selain SIM yang dirubah dilakukan ditempat berbeda untuk <i>server live</i> ?                                                                                                                                                                                                                                  |
|                     | Kalau itu sih iya. Kan kalau misal kita rubahnya di <i>server live</i> tau-tau ada <i>error</i> , proses bisnis bisa berhenti.                                                                                                                                                                                                                                      |
| A.12.2.1            | Apakah kontrol pendeteksi, perlindungan dan perbaikan untuk menangani <i>malware</i> diterapkan pada perangkat komputer?                                                                                                                                                                                                                                            |
|                     | Ada Windows Defender, <i>default</i> dari Windows.                                                                                                                                                                                                                                                                                                                  |
| A.12.2.1            | Kalau tidak salah dulu pakai Kaspersky ya untuk <i>anti-virus</i> ? Dan apa tidak menggunakan <i>anti-virus</i> lain juga?                                                                                                                                                                                                                                          |
|                     | Karena masalah lisensi mas, penggunaan Kaspersky kan berbayar. Kalau pakai Windows Defender sudah cukup dan tidak berbayar. Kalau pakai <i>anti-virus</i> lain nanti Windows Defender-nya non-aktif.                                                                                                                                                                |
| A.12.2.1            | Apakah ada peninjauan apakah terdapat <i>file</i> atau penambahan tanpa izin secara formal pada <i>server</i> atau komputer/laptop dinas?                                                                                                                                                                                                                           |
|                     | Tidak ada peninjauan seperti itu disini.                                                                                                                                                                                                                                                                                                                            |
| A.12.2.1            | Bagaimana kalau ada kasus <i>malware</i> yang merusak sistem? Apakah dilakukan karantina terhadap sistem?                                                                                                                                                                                                                                                           |
|                     | Pasti ada kita <i>block</i> supaya tidak menyebar ke sistem lain ke jaringan, terus kita periksa sistem dan konfigurasinya. Seteah itu <i>scan</i> pakai <i>anti-malware</i>                                                                                                                                                                                        |
|                     | yang ter- <i>update</i> atau produk lain. Kalau memang <i>virus</i> -nya tidak bisa diatasi terpaksa di <i>install</i> ulang asal datanya bisa dipulihkan/ada <i>backup</i> -nya.                                                                                                                                                                                   |



|          |                                                                                                                                                                                                                                                                      |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.12.3.1 | Apakah salinan informasi, perangkat lunak dan <i>clone</i> dari <i>hardisk</i> diambil dan diuji secara teratur berdasarkan kebijakan <i>backup</i> ?                                                                                                                |
|          | Untuk <i>backup</i> sendiri dilakukan setiap hari pada jam 1 malam, sedangkan untuk konfigurasi perangkat jaringan dilakukan hanya ketika terjadi perubahan saja. Ini yang dilakukan oleh Subdit Infrastruktur, kalau untuk Subdit Pengembangan lain lagi urusannya. |
| A.12.3.1 | Apakah hasil <i>backup</i> disimpan secara ganda (mencegah jika satu <i>backup</i> mengalami <i>corrupt</i> )?                                                                                                                                                       |
|          | <i>Backup</i> yang dilakukan itu sinkronisasi, jadi tidak ada yang berganda. Untuk <i>backup</i> ada <i>server</i> -nya sendiri.                                                                                                                                     |
| A.12.3.1 | Apakah hasil <i>backup</i> tadi disimpan didalam gedung lain?                                                                                                                                                                                                        |
|          | Tidak, satu ruangan didalam pusat data. Niatnya sih inginnya begitu.                                                                                                                                                                                                 |
| A.12.4.1 | Apakah perekaman <i>log</i> aktifitas pengguna, <i>error</i> , dan kejadian keamanan informasi lainnya dibuat, disimpan dan ditinjau secara berkala?                                                                                                                 |
|          | Disini tidak disimpan mas dan walaupun ada tidak lama penyimpanannya. Misalkan saya mau melihat <i>log</i> untuk 7 hari kedepan itu tidak bisa.                                                                                                                      |
| A.12.4.4 | Apakah semua jam pada semua sistem pemrosesan informasi disinkronisasikan kedalam satu referensi yang sama?                                                                                                                                                          |
|          | Ada, pakai protokol <i>NTP</i> . Kalau yang baru-baru seperti <i>server development</i> masih belum, kalau yang <i>server live</i> pasti.                                                                                                                            |
| A.12.5.1 | Apakah prosedur diterapkan untuk mengontrol pemasangan perangkat lunak pada sistem operasi?                                                                                                                                                                          |
|          | Kalau prosedur tidak ada secara tertulis.                                                                                                                                                                                                                            |
| A.12.5.1 | Apakah Subdit Infrastruktur bertanggung jawab terhadap pemasangan sistem operasi dan perangkat lunak komputer?                                                                                                                                                       |
|          | Kami tidak melakukan itu, karena tugas kami hanya mengurus jaringan. Untuk pemasangan biasanya dilakukan oleh yang bisa memasang, jadi tanggung jawab pemasangan ada di masing-masing Subdit. Kalau misalkan                                                         |

|          |                                                                                                                                                                                                                         |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | ada yang minta bantuan maka akan kami bantu, dan biasanya masalahnya di pengaturan <i>IP address</i> atau jaringan lainnya.                                                                                             |
| A.12.6.1 | Apakah informasi tentang kerentanan teknis pada sistem informasi didapatkan pada waktu tertentu dan dilakukan tindak lanjutnya (seperti <i>patch</i> ) untuk mengacu pada resiko yang terkait?                          |
|          | Tidak semuanya sih dan walaupun ada cuma yang bermasalah saja. Selain itu juga disini tidak selalu mengawasi setiap <i>patch</i> baru yang keluar dan diharuskan untuk dipasang semua dengan yang baru.                 |
| A.12.6.1 | Apakah pemasangan <i>patch</i> perlu dilakukan pengujian?                                                                                                                                                               |
|          | Ya, soalnya kita tidak berani ambil resiko mas. Misalkan sekarang versi 2, lalu muncul versi 3. Kita tidak berani langsung <i>update</i> di <i>server live</i> .                                                        |
| A.12.6.1 | Jadi pemasangan <i>patch</i> dilakukan manual untuk <i>server</i> ya pak?                                                                                                                                               |
|          | Ya, kalau otomatis tambah ngeri mas. Takutnya kalau lebih cocok yang versi 2 bagaimana?                                                                                                                                 |
| A.12.6.1 | Apakah ada aktifitas membandingkan resiko yang ada ketika memasang <i>patch</i> dengan kerentanan yang ada?                                                                                                             |
|          | Kita tidak sampai kesitu. Walaupun resiko ya apa perangkat lunak tersebut bermasalah atau tidak setelah dipasang.                                                                                                       |
| A.12.6.2 | Apakah peraturan untuk mengatur pemasangan perangkat lunak oleh pengguna dibuat dan diterapkan?                                                                                                                         |
|          | Tidak ada pembatasan pemasangan perangkat lunak pada komputer. Dulu pernah dibatasi, kalau tidak salah diatur di <i>group policy</i> -nya Windows. Tapi karena karyawan banyak yang mengeluh, maka tidak lagi dibatasi. |
| A.12.6.2 | Jadi siapapun bisa memasang perangkat lunak terutama yang bajakan ya pak?                                                                                                                                               |
|          | Ya, dulu pernah ada komputer yang <i>error</i> . Masalahnya karena komputernya dipasang <i>game</i> bajakan itu.                                                                                                        |
| A.13.1.1 | Apakah terdapat keamanan yang berlapis pada jaringan?                                                                                                                                                                   |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | Sudah ada menggunakan <i>firewall</i> . Secara <i>default</i> -nya <i>firewall</i> -nya ada satu yaitu CISCO ASA Firewall. Ada juga <i>firewall</i> lain yaitu ShoreWall yang menggunakan <i>IP Table</i> . Tapi ShoreWall itu digunakan untuk keamanan bertingkat pada SIM saja, bukan untuk cadangan kalau <i>firewall</i> -nya mati.                                                                                                                                                                                                                               |
| A.13.1.1             | <p>Apa saja <i>port</i> yang biasa di <i>block</i> dengan <i>firewall</i>?</p> <p>Kalau disini yang biasa dibuka. Jadi disini itu <i>default</i>-nya <i>denided</i>, terus yang <i>allow</i> apa saja. Yang di <i>allow</i> seperti <i>port</i> 80 dan <i>port</i> 443 untuk <i>website</i>, POP3 untuk <i>email</i>, dan lainnya. Jadi <i>port</i>-<i>port</i> aneh dan tidak digunakan seperti <i>FTP</i>, <i>P2P</i> dan lainnya itu kita <i>block</i>. Pokoknya <i>port</i> untuk kebutuhan aplikasi.</p>                                                         |
| A.13.1.1<br>A.12.1.3 | <p>Apakah penggunaan <i>internet</i> diatur, seperti pemblokiran situs tertentu?</p> <p>Ada, diatur pakai <i>Internet Access Management</i> dari Sangfor itu. <i>IAM</i> itu fungsinya untuk mengurus koneksi <i>internet</i> saja, seperti <i>download</i>, pengaturan <i>bandwith</i>, dan pemblokiran. Dulu kita pakai Fortigate <i>UTM</i>.</p>                                                                                                                                                                                                                   |
| A.16.1.1             | <p>Saya lihat di prosedur Keluhan Pelanggan ada penanganan secara langsung dan <i>remote</i>. Kalau untuk <i>remote</i> masalah apa saja yang bisa ditangani?</p> <p>Tergantung permasalahannya apa. Selama <i>server</i> atau perangkat itu bisa kita <i>remote</i>, ya kita <i>remote</i>. Misalkan saya lagi di rumah, terus ada <i>server</i> A yang layanan Apache <i>HTTP Server</i>-nya <i>down</i>, ya kita <i>remote server</i>-nya. Kita nyalakan layanannya. Tapi kalau layanannya tidak bisa kita <i>remote</i>, mau tidak mau harus datang langsung.</p> |
| A.16.1.5             | <p>Apakah setiap insiden keamanan informasi ditanggapi sesuai dengan prosedur yang terdokumentasi (misalnya <i>troubleshooting</i> untuk <i>server</i>)?</p> <p>Untuk penanganan insiden atau <i>troubleshooting</i>-nya yang sederhana, tidak perlu mengurus banyak waktu dan tenaga, ya kita kerjakan langsung. Cuman kalau perlu waktu lama, ya itu kira tulis.</p>                                                                                                                                                                                                |
| A.16.1.5             | <p>Apakah benar tidak ada prosedur yang spesifik untuk <i>troubleshooting</i> tertentu? Misalkan untuk masalah ini ada prosedur <i>troubleshooting</i>-nya.</p> <p>Tidak bisa mas. Misalnya koneksi <i>internet</i> di jurusan A mati, bayangan anda apa penyebab matinya? Setelah kita datang ternyata disana baru renovasi ruang/geser-geser ruang dan kabel <i>LAN</i>-nya belum terpasang ke komputer.</p>                                                                                                                                                        |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <p>Kayak begitu ya susah-susah gampang, kecuali kalau orang yang komplain itu orang yang mengerti. Kadang ibu-ibu komplain atau dosen yang sudah sepuh ke kita. Tahunya kan mereka <i>internet</i>-nya tidak jalan. Contoh lainnya ada kepala UPT yang tidak bisa buka Webmail ITS, bayangan anda apa penyebabnya? Mungkin <i>server</i>-nya bermasalah, tapi saya coba bisa. Setelah kita datangi ternyata dia lupa mematikan tombol <i>capslock</i> pada saat memasukkan <i>password</i>. Ini saya kasih contoh dimana kita kesulitan untuk menulis prosedur bakunya. Kalau Subdit Pelayanan kan enak misalkan prosedur keluhan, langkahnya pasti seperti terima keluhan, laporkan ke petugas yang akan menangani, menginformasikan ke pelapor kalau masalah sudah selesai dan pencatatan. Kalau Subdit Infrastruktur langkahnya tidak pasti.</p> |
| A.16.1.5 | <p>Apakah dilakukan diskusi sebelum penanganan insiden keamanan informasi?</p> <p>Tergantung masalahnya apa dulu. Kalau masalahnya mudah, ya langsung kita kerjakan saja. Misalnya “bagaimana laptop ini dengan <i>access point</i> yang sama bisa menyambung ke lantai 6?”, itukan mudah masalahnya. Kecuali kalau rumit, baru kita diskusikan. Untuk yang sebelum penanganan misalnya “ada masalah seperti begini, kira-kira apa ya solusinya?”, nah itu kita lakukan sebelum penanganan dan hasilnya kita laporkan Kasubdit Infrastruktur.</p>                                                                                                                                                                                                                                                                                                   |
| A.16.1.6 | <p>Apakah ilmu yang didapat dari analisa dan penanganan insiden keamanan informasi didiskusikan dan digunakan untuk mengurangi kemungkinan dan dampak pada insiden kedepan?</p> <p>Ada sih diskusi setelah mengerjakan penanganan. Tapi ini juga balik lagi tergantung dari masalahnya apa dulu. Kalau masalahnya sudah sering kita lakukan maka tidak ada diskusi, sedangkan kalau jarang itu biasanya ada diskusi.</p>                                                                                                                                                                                                                                                                                                                                                                                                                            |
| A.18.2.3 | <p>Apakah sistem informasi ditinjau secara berkala agar patuh terhadap kebijakan dan standar keamanan informasi organisasi, contoh dengan penetrasi tes dan pemindaian kerentanan?</p> <p>Tidak dilakukan, tapi dulu pernah pengujian sistem dengan <i>stress test</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| A.17.2.1 | <p>Apakah terdapat penggantian <i>hardisk server</i> yang sudah melewati garansi dengan yang baru?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|  |                                                                                                                                                                                                                               |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Waktu itu pak Febriliyan (Direktur DPTSI-ITS) sempat mengusulkan kalau <i>hardisk</i> yang sudah habis garansinya harus diganti ke pusat, tapi tidak bisa. Jadi solusinya menggunakan <i>RAID</i> pada setiap <i>server</i> . |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Narasumber : Satriyo Wicaksono, S.Kom. & Faishal Halim Saputra, S.ST

Jabatan : Pengembang Jaringan dan Pangkalan Data (Bagian Jaringan)

Subdit : Subdirektorat Infrastruktur & Keamanan Teknologi Informasi

| <i>Server</i>                         | <i>VPS/<br/>dedicated</i>                                                                                  | <i>DMZ/private</i>                                  | <b>Redundan</b>     | <b>Backup<br/>data<br/>berkala</b> |
|---------------------------------------|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|---------------------|------------------------------------|
| Webmail ITS                           | <i>D</i>                                                                                                   | <i>DMZ</i>                                          | Tidak               | Ya                                 |
| <i>DNS</i> (BIND)                     | <i>V</i>                                                                                                   | <i>DMZ</i>                                          | <i>Master/slave</i> | Ya                                 |
| <i>Proxy</i> ITS (Squid)              | <i>V &amp; D</i>                                                                                           | <i>DMZ</i>                                          | Ya                  | Tidak                              |
| Tsubame                               | Dikelola oleh KEMENKOMINFO                                                                                 |                                                     |                     |                                    |
| Honeypot                              | Dikelola oleh KEMENKOMINFO                                                                                 |                                                     |                     |                                    |
| Cacti                                 | Satu <i>server</i> dengan <i>website</i> ITS ( <a href="https://www.its.ac.id">https://www.its.ac.id</a> ) |                                                     |                     |                                    |
| Nagios                                | <i>V</i>                                                                                                   | <i>Private</i>                                      | Tidak               | Tidak                              |
| ITS Web Monitoring System             | <i>V</i>                                                                                                   | <i>DMZ</i>                                          | Tidak               | Tidak                              |
| Sinkronisasi <i>database server</i>   | <i>D</i>                                                                                                   | <i>Private + IP address</i><br>Subdit Infrastruktur | Tidak               | Tidak                              |
| Sinkronisasi <i>database jaringan</i> | <i>D</i>                                                                                                   | <i>Private + IP address</i><br>Subdit Infrastruktur | Tidak               | Tidak                              |
| <i>SIEM</i> AlienVault                | <i>V</i>                                                                                                   | <i>DMZ</i>                                          | Tidak               | Ya                                 |
| Open VPN                              | <i>V</i>                                                                                                   | <i>DMZ</i>                                          | Tidak               | Tidak                              |
| Git ITS                               | <i>V</i>                                                                                                   | <i>DMZ</i>                                          | Tidak               | Ya                                 |

\*) *VPS* = *Virtual Private Server*, *Dedicated* = *server* fisik.

Narasumber : Anny Yuniarti, S.Kom., M.Comp.Sc.

Jabatan : Kasubdit Pengembangan Sistem Informasi

Organisasi : DPTSI-ITS

| No Annex            | Pertanyaan & Jawaban                                                                                                                                                                                                                                                               |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.6.1.5             | Apakah keamanan informasi dirujuk kedalam manajemen proyek pengembangan?                                                                                                                                                                                                           |
|                     | Mungkin tidak spesifik, ayo kita bahas tentang isu keamanan informasi. Tapi umumnya itu sudah menjadi praktik keseharian, seperti pembuatan sistem informasi harus ada pemisahan operasional dan pengembangan, ada <i>backup</i> yang rutin, ada manajemen hak akses, dan lainnya. |
| A.6.1.5<br>A.14.1.1 | Apakah organisasi melakukan penilaian resiko/manajemen resiko sebagai bagian dari manajemen proyek pengembangan?                                                                                                                                                                   |
|                     | Tidak dilakukan.                                                                                                                                                                                                                                                                   |
| A.7.2.1             | Apakah terdapat pengarahan sebelum diberikan akses ke sistem informasi sesuai dengan peran dan tanggung jawab dalam keamanan informasi?                                                                                                                                            |
|                     | Mungkin secara khusus tidak dilakukan. Apalagi sebelum diberikan akseskan harus menandatangani perjanjian menjaga kerahasiaan.                                                                                                                                                     |
| A.8.1.1             | Apakah aset yang berhubungan dengan sistem informasi diidentifikasi dan daftar inventarisnya didokumentasikan dan dikelola?                                                                                                                                                        |
|                     | Ada sih tapi misah-misah dan belum dipusatkan satu data. Karena dulu ada Pusat Pengembangan dan Pusat Layanan Data yang semuanya melakukan pengembangan, sehingga yang satu mencatat dan yang satunya juga. Sekarangkan pengembangan sudah jadi satu yaitu Subdit Pengembangan.    |
| A.8.1.1             | Kalau tidak salah mencatatnya di SI Inventaris SIM ya?                                                                                                                                                                                                                             |
|                     | Kayaknya itu sudah tidak digunakan dan tidak aktif lagi. Sementara masih berupa <i>file</i> yang di <i>share online</i> saja. Kalau yang SIM itu dulu ada, tapi karena tidak digunakan datanya tidak aktif.                                                                        |
| A.8.1.1<br>A.8.1.2  | Apa ada daftar inventaris aset berupa dokumen dan <i>file</i> yang ada di Subdit Pengembangan?                                                                                                                                                                                     |

|          |                                                                                                                                                                                                                                                                                                                                                                         |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Ada, tapi tidak tersusun rapih satu Subdit atau tempat. Misalnya alur proses bisnis A ada di satu <i>file</i> Ms. Visio dan di <i>share</i> diantara timnya. Nanti beda tim lagi punya yang berbeda. Jadi mencar-mencar, kalau butuh kita tahu ada di mas ini, mbak itu. Harusnya sih dibuat untuk identifikasi aset apa saja yang ada.                                 |
| A.9.4.5  | Siapa saja yang bisa mengakses <i>source code</i> ?                                                                                                                                                                                                                                                                                                                     |
|          | <i>Programmer</i> dan Kasubdit Pengembangan saja yang bisa mengakses.                                                                                                                                                                                                                                                                                                   |
| A.9.4.5  | Apakah akses ke <i>source code</i> perangkat lunak dibatasi?                                                                                                                                                                                                                                                                                                            |
|          | Kalau yang <i>native</i> (sistem informasi lama) sudah ada seperti itu, jadi yang mengakses hanya <i>IP address</i> komputer tertentu yang sudah didaftar. Jadi kita mengasih <i>IP address</i> ke Subdit Infrastruktur, nanti mereka yang mengatur di <i>firewall</i> . Kalau yang baru pakai pendekatan Git. Jadi kita punya GitLab khusus untuk pengembangan di ITS. |
| A.10.1.1 | Apa saja yang dienkripsi oleh organisasi? Dan apakah terdapat acuan standar dalam penggunaan enkripsi?                                                                                                                                                                                                                                                                  |
|          | Yang dienkripsi <i>HTTPS</i> dan <i>password</i> pengguna untuk <i>login</i> saja. Untuk acuan standarnya tidak ada.                                                                                                                                                                                                                                                    |
| A.12.7.1 | Apakah persyaratan dan aktifitas audit termasuk memastikan sistem operasional (audit sistem informasi) untuk mengurangi gangguan pada proses bisnis?                                                                                                                                                                                                                    |
|          | Saya itukan baru tahun kemarin masuk, itu belum pernah sampai sekarang. Kalau sebelumnya saya tidak tahu.                                                                                                                                                                                                                                                               |
| A.14.1.1 | Apa saja metode yang digunakan untuk mengidentifikasi persyaratan keamanan?                                                                                                                                                                                                                                                                                             |
|          | Mematuhi kebijakan atau hukum yang berlaku, peninjauan insiden yang pernah terjadi, kerentanan yang ditemukan atau dicurigai, dan wawancara dengan pengguna atau pelanggan.                                                                                                                                                                                             |
| A.14.1.1 | Apakah persyaratan keamanan diidentifikasi bersamaan dengan <i>user requirement</i> ?                                                                                                                                                                                                                                                                                   |
|          | Kalau itu pastinya sama-sam dari awal proyek sudah diidentifikasi.                                                                                                                                                                                                                                                                                                      |

|                      |                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.14.2.5             | Apakah standar keamanan teknis untuk pemrograman yang aman dibangun, didokumentasikan, dirawat dan diterapkan pada setiap penerapan sistem informasi?                                                                                                                                                                                                                     |
|                      | Belum ada standar khusus. Yang ada contoh yang ada “begini kalau mau membuat” dari yang sudah pernah dikembangkan.                                                                                                                                                                                                                                                        |
| A.14.2.5             | Apakah Subdit Pengembangan menggunakan kerangka kerja tertentu?                                                                                                                                                                                                                                                                                                           |
|                      | Kalau pengembangan yang baru-baru ini itu kita pakai <i>framework PHP</i> Laravel. Kalau <i>database</i> kita dulu ada banyak, ada yang pakai Postgrate, MySQL dan Ms.SQL Server. Tapi mulai tahun kemarin kita standarkan semua pakai SQL Server. Jadi sistem informasi yang masih menggunakan MySQL dijadikan ke Ms.SQL Server, karena pengelolaannya jadi lebih mudah. |
| A.17.1.1<br>A.17.1.2 | Apakah organisasi sudah merencanakan <i>business continuity plan</i> atau <i>disaster recovery plan</i> berikut persyaratannya untuk situasi krisis atau bencana?                                                                                                                                                                                                         |
|                      | Untuk prosedur <i>DRP</i> sendiri DPTSI-ITS masih belum punya, namun untuk rencana pemulihan sudah diterapkan dan DPTSI-ITS memiliki <i>disaster recovery center</i> di beberapa tempat yang terpisah.                                                                                                                                                                    |
| A.17.1.3             | Apakah organisasi menguji secara berkala kontrol tentang <i>business continuity</i> ataupun <i>disaster recovery</i> yang dibangun dan diterapkan benar dan efektif ketika krisis atau bencana?                                                                                                                                                                           |
|                      | Belum pernah dilakukan pengujian apapun.                                                                                                                                                                                                                                                                                                                                  |

Narasumber : Sri Lestari, S.ST.

Jabatan : Pengembangan Jaringan dan Pangkalan Data (Bagian Pengembang)

Subdit : Subdirektorat Pengembangan Sistem Informasi

| No Annex | Pertanyaan & Jawaban                                                                                                                                                      |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.6.1.2  | Apakah beberapa tugas dan area tanggung jawab yang berlawanan dipisahkan untuk mengurangi peluang perubahan dan penyalahgunaan tanpa izin atau tidak disengaja pada aset? |



|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | Sudah ada pembagian tugas di Subdit Pengembangan, seperti analis sistem dan <i>desainer</i> itu dirangkap satu orang, sedangkan <i>programmer</i> , penguji sistem dan dokumentator itu masing-masing satu orang. Tapi bisa jadi analis dan <i>programmer</i> dirangkap jadi satu orang tergantung dari besar kecilnya kegiatan pengembangan sistem itu. Biasanya kalau dokumentator itu mahasiswa, jadi kalau sistem kita sudah selesai, mereka mengecek dan mendokumentasikannya.                                                                                                                                                                                                                                                                                     |
| A.6.1.2             | Apakah <i>programmer</i> dan penguji sistem juga dirangkap?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                     | Tidak dirangkap. Terkadang penguji sistem dan dokumentator yang dirangkap. Kalau sistemnya kecil sih dua orang sudah cukup, seperti analis sistem merangkap <i>programmer</i> dan penguji sistem merangkap dokumentator.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| A.9.4.5<br>A.14.2.2 | Apakah setiap perubahan pada <i>source code</i> yang dilakukan <i>programmer</i> diperlukan izin kepada Kasubdit Pengembangan sebelum dilakukan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                     | Biasanya sih kalau itu otomatis karena kebutuhan dan lebih cepat lebih baik, kecuali kalau itu memang berhubungan dengan kebijakan. Kita hanya menyampaikan “oh ini ada perubahan seperti begini”, asalkan tidak keluar dari koridor proses bisnis di sistemnya. Misalnya ada perubahan fitur pada sistem malah membuat pelebaran dari kegiatan pengembangan, karena ada yang penambahan fitur pada sistem “ya sudah begini saja selesai, butuh sedikit halaman saja sudah selesai”, dan ada yang berkaitan dengan fitur lainnya nah ini kan nanti mengerjakannya tambah banyak dan perlu didiskusikan. Untuk yang berkaitan dengan perubahan kebijakan dan proses bisnis harus kita didiskusikan, sedangkan yang tidak merubah proses bisnis ya tidak perlu dilakukan. |
| A.7.2.2             | Apakah terdapat pelatihan kerja yang diadakan untuk Subdit Pengembangan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|                     | Pernah kita adakan di tahun 2016, ada pelatihan Laravel untuk bahasa pemrograman <i>PHP</i> bagi beberapa Subdit Pengembangan atau karyawan lainnya yang memang mau konsentrasi kesitu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| A.8.1.1             | Apakah aset yang berhubungan dengan sistem informasi diidentifikasi dan daftar inventarisnya didokumentasikan dan dikelola?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <p>Kalau itu kita punya SI Inventaris SIM, jadi khusus SIM saja dan hanya bisa diakses oleh Subdit Pengembangan saja. Isinya itu memuat <i>log</i> pengembangan, misalnya ada sistem yang sudah berjalan dan ada pengembangan fitur. Nah itu disitu tinggal ditambah informasi, mau mengembangkan fitur atau modul. Yang besar itu namanya SIM, satuannya modul dan satuan yang paling kecil itu fitur. Contohnya ada pengembangan modul di SIM Kepegawaian, jadi nanti yang mengembangkan modul itu berkewajiban menyampaikan pengembangan modul tersebut, misalnya isinya apa saja dan lebih cenderung ke fiturnya apa saja. Selain itu ada informasi untuk merawat, seperti apa saja <i>server development</i> dan/atau <i>live</i> yang digunakan, nomor <i>IP address</i>-nya, platform yang digunakan, dan lainnya. Informasi lainnya dikembangkan oleh siapa, tahun berapa dan dananya (jika ada). Kecuali kalau <i>password</i> ada khusus sendiri yang menyimpan.</p> |
| A.9.2.3  | <p>Apakah <i>programmer</i> dan penguji sistem memiliki hak akses kedalam sistem yang mereka kembangkan dan uji?</p> <p>Biasanya punya, karena setelah pengembangan selesai, dia berlaku sebagai pengelola atau <i>administrator</i>. Jadi secara otomatis dia punya hak akses. Biasanya kalau di Subdit Pengembangan kan selain mengembangkan sistem juga mengelola. Sedangkan kalau untuk sistem yang dibuat untuk diluar lingkungan ITS, biasanya disana yang mengelola setelah kita serahkan sistemnya, dan tidak ada kelanjutan bekerjasama lagi.</p>                                                                                                                                                                                                                                                                                                                                                                                                                     |
| A.9.4.5  | <p>Apakah bisa diketahui siapa yang membuat atau memperbaharui baris <i>source code</i> jika <i>programmer</i>-nya ada banyak?</p> <p>Kalau itu kita pakai semacam perangkat <i>git</i>. Dulu kita pernah pakai Github, terus sekarang pakai <i>git</i> lokalnya ITS itu. Jadi itu bisa dilihat kontributornya atau yang membuat itu siapa.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| A.10.1.1 | <p>Apakah Subdit Pengembangan melakukan pemasangan <i>SSL/TLS</i>?</p> <p>Oh itu biasanya Subdit Infrastruktur yang memasang. Kita hanya terima kosongan atau <i>server</i> yang sudah siap dipasang sama sistem yang kita kembangkan.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| A.12.7.1 | <p>Apakah persyaratan dan aktifitas audit termasuk memastikan sistem operasional (audit sistem informasi) untuk mengurangi gangguan pada proses bisnis?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Kita belum pernah diadakan audit untuk sistem informasi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| A.12.1.4 | Apakah ada kontrol keamanan untuk pemindahan dari <i>server development</i> ke <i>server live</i> ?                                                                                                                                                                                                                                                                                                                                                                                                                                |
|          | Untuk itu misalkan ada yang dia hanya bisa mengakses ke <i>server development</i> saja, sedangkan untuk menaikkan ke <i>server live</i> -nya kita setelah dipastikan sudah berjalan dan sebagainya. Itu biasanya dilakukan untuk <i>programmer</i> dari luar atau mahasiswa magang.                                                                                                                                                                                                                                                |
| A.12.1.4 | Apakah pemindahan dari <i>server development</i> ke <i>server live</i> itu perlu izin tambahan ke Subdit Infrastruktur?                                                                                                                                                                                                                                                                                                                                                                                                            |
|          | Biasanya saat pertama kali membangun sistem, kita sudah meminta <i>server development</i> dan <i>live</i> . Tapi untuk yang <i>server development</i> sih bisa digunakan oleh beberapa sistem asalkan memiliki <i>platform</i> yang sama. Kalau yang <i>server live</i> , teman-teman di Subdit Infrastruktur sudah menata dan tidak mencampur sistem pada <i>server live</i> dengan sistem lain.                                                                                                                                  |
| A.12.4.1 | Apakah perekaman <i>log</i> aktifitas <i>administrator</i> sistem seperti merubah data dan lainnya dibuat, disimpan dan ditinjau secara berkala?                                                                                                                                                                                                                                                                                                                                                                                   |
|          | Itu tidak ada dan memang itu kekurangan dari kami, tapi kami jamin kerahasiaan data yang kami pegang. Kan kami punya kode etik sendiri untuk menjaga kerahasiaannya, ya seperti dokter yang punya kode etik sendiri. Jadi misalnya ada karyawan yang memegang SIM Keuangan, dia tidak mungkin menyebarkan bahwa karyawan X gajinya berapa. Memang sih lebih aman kalau ada perekaman dan dokumentasinya, tapi karena kami padat karya (banyak pekerjaan dan kurang karyawan) jadi hal-hal yang seperti itu tidak sempat dilakukan. |
| A.12.7.1 | Apakah persyaratan dan aktifitas audit termasuk memastikan sistem operasional (audit sistem informasi) untuk mengurangi gangguan pada proses bisnis?                                                                                                                                                                                                                                                                                                                                                                               |
|          | Belum pernah diadakan audit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| A.13.2.4 | Apakah di Subdit Pengembangan ada persyaratan untuk perjanjian kerahasiaan dan tidak-menyingkap informasi untuk melindungi informasi diidentifikasi dan didokumentasikan?                                                                                                                                                                                                                                                                                                                                                          |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Ada, Kesepakatan Bersama Menjaga Kerahasiaan Aset Sistem Informasi Institusi Dilingkungan Kampus ITS khusus untuk Subdit Pengembangan. Kita simpan data ini dengan lampiran <i>photocopy</i> KTP. Teman-teman yang masuk ke Subdit Pengembangan itukan bisa dari mahasiswa atau dari pusat, Direktorat SDM dan Organisasi. Kalau dari pusat kan sudah diatur secara otomatis menjaga kerahasiaan bagaimana. Tapi untuk menjaga itu semua, ya semuanya tanda tangan. Baik karyawan PNS, karyawan non-PNS maupun mahasiswa magang.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| A.13.2.4 | Apakah dokumen tersebut ditinjau secara berkala untuk melihat kelayakannya saat ini?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|          | Kalau peninjauannya sih tidak dilakukan secara berkala. Karena kalaupun dokumen berubah karena perlu menambahkan poin yang harus dilakukan dalam keamanan informasi, perubahannya tidak terlalu spesifik.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| A.14.1.1 | Apakah keamanan informasi yang berhubungan dengan persyaratan dimasukkan untuk sistem informasi baru atau pembaharuan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|          | Biasanya kalau pengguna lebih membutuhkan dari sisi fungsi. Kalau dari segi keamanan mereka menyerahkan ke kita. Mungkin ada waktu itu mereka mintanya pakai <i>CAPTCHA</i> di formulir <i>login</i> -nya. Kalau dari kami sih keamanan lebih di manajemen hak aksesnya saja.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| A.14.1.1 | Apakah terdapat panduan untuk sistem yang dibangun?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|          | Ada 2 dokumen seperti <i>User Guide</i> dan <i>Developer Guide</i> . Untuk <i>User Guide</i> menjelaskan penggunaan sistemnya seperti apa untuk pengguna. Sedangkan untuk <i>Developer Guide</i> menjelaskan kedalam sistem yang dibangun dan kegiatan yang dilakukan <i>programmer</i> , seperti pada halaman ini mana me-link ke halaman mana. Jadi lebih banyak ke fungsionalitas dari sistem itu, termasuk <i>source code</i> -nya dan <i>database</i> -nya. Contohnya <i>database</i> -nya struktur seperti apa, nanti <i>database</i> tersebut dipergunakan dimana. Artinya setiap halaman <i>source code</i> itukan harus memuat dia harus me-link ke halaman yang mana, atau <i>database</i> yang mana. Jadi kalau ada <i>programmer</i> berikutnya yang bertugas memegang sistem, dia cukup melihat dari <i>Developer Guide</i> tersebut. Setiap baris fungsi dari <i>source code</i> juga dijelaskan, seperti <i>query</i> dalam halaman itu untuk mengambil daftar laporan ini. |
| A.14.1.1 | Apa metode yang digunakan untuk menggambar desain suatu sistem?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Ada macam-macam kayak <i>UML</i> , <i>use case</i> , atau lainnya. Tergantung dari masing-masing dokumentasinya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| A.14.2.3 | <p>Apakah aplikasi bisnis yang kritis ditinjau dan diuji ketika <i>platform</i> operasional dirubah (sistem operasi, <i>database</i>, <i>middleware</i>) untuk memastikan tidak ada dampak yang merugikan pada operasional dan keamanan organisasi?</p> <p>Peninjauan apakah sistem informasi masih berjalan setelah dilakukan perubahan pada <i>platform</i>-nya itu pasti dilakukan, entah itu hasil dari pembaharuan <i>patch</i> dan lainnya. Misalnya saja memasang sistem operasi terbaru pada <i>server</i>, ya kita lakukan <i>backup</i> terlebih dahulu, lalu setelah dipasang dilakukan pengujian apakah sistem informasinya berjalan normal atau tidak.</p> |
| A.14.2.4 | <p>Apakah modifikasi pada paket perangkat lunak diurungkan, dibatasi untuk perubahan yang diperlukan dan semua perubahan harus dikontrol secara ketat?</p> <p>Kalau itu tidak diatur. Untuk modifikasi pada paket perangkat lunak memang perlu dilakukan, misalnya pada kerangka kerja Laravel kan banyak sekali fungsi-fungsi yang dimiliki. Tidak mungkin semuanya dimasukkan semua karena akan memberatkan dari sistem tersebut.</p>                                                                                                                                                                                                                                 |
| A.14.2.4 | <p>Apakah setiap paket perangkat lunak yang dimodifikasi diuji secara formal dan didokumentasikan?</p> <p>Oh maksudnya dokumentasi apa saja yang diisi kedalam <i>server</i> dan perubahannya, seperti Apache <i>HTTP Server</i>, My SQL dan lainnya? Kalau itu kita tidak sampai dokumentasi kesana. Sedangkan kalau untuk pengujian kita tidak lakukan secara formal, masing-masing karyawan sih menguji apa modifikasinya sesuai kebutuhan atau tidak.</p>                                                                                                                                                                                                           |
| A.14.2.7 | <p>Apakah ada pengembangan sistem informasi yang dilakukan oleh vendor atau pihak ketiga?</p> <p>Sekarang DPTSI-ITS sudah mengembangkan sistem informasi secara mandiri. Kalaupun ada bantuan pun itu berasal dari pihak lain yang merupakan kepanjangan tangan kami, artinya karyawan diluar Subdit Pengembangan dan masih didalam lingkup ITS.</p>                                                                                                                                                                                                                                                                                                                    |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.14.2.8 | Apakah pengujian fungsi keamanan dilakukan selama pengembangan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|          | Pengujian sih lebih ke pengujian <i>input</i> data dan hasil yang diharapkan pada kondisi tertentu. Pengujian biasanya dilakukan oleh tim penguji dan pengguna sistem nantinya.                                                                                                                                                                                                                                                                                                                                                        |
| A.14.2.9 | Apakah program pengujian dan kriteria yang berhubungan dengan penerimaan sistem dibangun untuk sistem informasi baru atau versi pembaharuan?                                                                                                                                                                                                                                                                                                                                                                                           |
|          | Kalau untuk pengujian kita tidak menggunakan alat ukur, metode pengujian atau standar tertentu. Jadi pengujian yang kita lakukan berdasarkan komplain dari pengguna. Kalau sudah sedikit komplain, berarti sudah bisa di operasionalkan di <i>server live</i> . Pengujian dilakukan di <i>server development</i> dan dilakukan oleh penguji yang bekerjasama dengan pemilik sistem nantinya. Misalnya SIM Keuangan, berarti pemilik sistemnya adalah BAUK-ITS. Kalau menurut mereka sudah ok, maka kita pasang ke <i>server live</i> . |
| A.14.2.9 | Apakah ada perekaman apa saja kesalahan dan perbaikan sistem yang dikembangkan saat pengujian?                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|          | Ya, biasanya kalau pakai <i>git</i> itu lebih tercatat. Jadi si penguji mengasih komentar, kemudian <i>programmer</i> mengeksekusi. Lebih enak kalau pakai perangkat <i>git</i> itu. Ada juga sih yang masih dicatat di kertas yang isinya “ini loh salahnya yang ini dan ini”.                                                                                                                                                                                                                                                        |
| A.14.3.1 | Apakah pengujian menggunakan data yang asli dilindungi dan dikontrol? Atau apakah pengujian menggunakan data <i>dummy</i> ?                                                                                                                                                                                                                                                                                                                                                                                                            |
|          | Biasanya kita pakai data <i>dummy</i> untuk keperluan pengujian.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Narasumber : Akhmad Budi Kurniawan

Jabatan : Pengembangan Jaringan dan Pangkalan Data (Bagian Pengembang)

Subdit : Subdirektorat Pengembangan Sistem Informasi

| No Annex | Pertanyaan & Jawaban                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.6.1.2  | Apakah tanggung jawab terhadap <i>programmer</i> sistem informasi dan <i>administrator database</i> -nya dipisahkan untuk mengurangi peluang perubahan dan penyalahgunaan tanpa izin atau tidak disengaja pada aset?                                                                                                                                                                                                            |
|          | Kalau itu kami merangkap <i>database</i> -nya juga, jadi tidak ada yang <i>programmer</i> sendiri dan <i>administrator database</i> -nya sendiri.                                                                                                                                                                                                                                                                               |
| A.6.1.2  | Jadi apakah <i>programmer</i> juga bisa mengubah data pada <i>database</i> ?                                                                                                                                                                                                                                                                                                                                                    |
|          | Oh bisa, karena <i>programmer</i> -nya kita-kita ini. Kalau misalnya ada kesalahan kita yang dipegang. Seperti saya SIM Akademik, ya sudah SIM Akademik saja. Misalnya yang di BAUK-ITS, ya nanti tanyanya ke <i>programmer</i> SIM Keuangan. Pasti orang tersebut yang mengakses, karena tidak banyak yang megang. Karena yang megang itu ada <i>administrator</i> dari BAUK-ITS dan <i>programmer</i> dari kita yang membuat. |
| A.9.2.3  | Apa perbedaan hak akses antara <i>administrator</i> dari unit dengan <i>administrator</i> dari Subdit Pengembangan?                                                                                                                                                                                                                                                                                                             |
|          | Berbeda, karena mereka hanya terbatas perintah <i>Data Manipulation Language (DML)</i> saja, sedangkan kami bisa sampai <i>Data Definition Language (DDL)</i> .                                                                                                                                                                                                                                                                 |
| A.9.2.3  | Apakah alokasi dan penggunaan hak akses <i>administrator</i> dikontrol dan dibatasi melalui proses yang formal?                                                                                                                                                                                                                                                                                                                 |
|          | Kita punya yang namanya manajemen hak akses di Integra ITS. Misalkan saya mau lihat siapa dan punya hak akses ke mana saja, ada disana. Bisa juga saya mau lihat <i>administrator</i> SIM Akademik siapa saja bisa kelihatan.                                                                                                                                                                                                   |
| A.9.4.5  | Kalau untuk manajemen <i>source code</i> disini menggunakan <i>git</i> ya pak?                                                                                                                                                                                                                                                                                                                                                  |
|          | Ya, pakai <i>git</i> . Tapi tidak semuanya, kan <i>git</i> itu baru, jadi yang lama-lama masih belum masuk. Kalau yang baru-baru yang dikembangkan sama teman-                                                                                                                                                                                                                                                                  |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                      | teman sudah masuk <i>git</i> semua. Tapi <i>git</i> -nya lokal sini. Jadi kita bikin sendiri tidak dinaikkan ke <i>git</i> . Kita punya sendiri di <a href="https://git.its.ac.id">https://git.its.ac.id</a> .                                                                                                                                                                                                                                                                                                                                      |
| A.12.4.1             | Apakah perekaman <i>log</i> aktifitas <i>administrator</i> sistem seperti merubah data dan lainnya dibuat, disimpan dan ditinjau secara berkala?                                                                                                                                                                                                                                                                                                                                                                                                    |
|                      | Tidak ada.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| A.14.2.2             | Apakah penerapan sistem baru dilakukan diwaktu yang tidak mengganggu proses bisnis?                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                      | Ya, biasanya kalau perubahan diwaktu yang tidak banyak menggunakan SIM. Misalkan SIM Akademik ya perubahannya bukan pada waktu mahasiswa isi FRS.                                                                                                                                                                                                                                                                                                                                                                                                   |
| A.14.2.5             | Apakah ada standar dalam menulis <i>source code</i> seperti tata cara penulisan dan struktur yang disetujui untuk setiap bahasa pemrograman yang digunakan?                                                                                                                                                                                                                                                                                                                                                                                         |
|                      | Tidak ada. Tapi yang kita sepakati hanya menggunakan bahasa <i>PHP</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| A.14.2.8             | Apakah pengujian fungsi keamanan dilakukan selama pengembangan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|                      | Pengujian termasuk sistemnya sih, misalnya kalau sistemnya SIM Akademik yang diuji keamanan hak aksesnya. Kalau yang menguji itu pengguna utamanya yaitu BAAK-ITS.                                                                                                                                                                                                                                                                                                                                                                                  |
| A.14.2.9<br>A.18.2.3 | Apakah pengujian sistem secara teknis seperti tes penetrasi atau pemindaian kerentanan dilakukan?                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|                      | Itu yang diuji biasanya Integra ITS, karena semua <i>login</i> ada disitu. Yang nguji sebelum pak Febriliyan (Direktur DPTSI-ITS) ada, jadi kita minta tolong mahasiswa untuk menguji, nanti <i>feedback</i> -nya apa saja. Kalau kita sendirikan, kita merasa aman saja. Jadi minta tolong pihak luar “coba di tes penetrasi” sama mahasiswa jaringan saja yang usil-usil itu. Kalau <i>stress test</i> yang pernah dilakukan di SIM Akademik terutama modul FRS. Itu pakai Apache JMeter di 20 komputer lab, kita <i>hit</i> sama-sama, itu saja. |
| A.14.2.9<br>A.18.2.3 | Jadi dalam pengembangan sistem baru tidak ada keharusan pengujian seperti tes penetrasi atau pemindaian kerentanan dilakukan?                                                                                                                                                                                                                                                                                                                                                                                                                       |



|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Ya, itu yang kita kurang memang. Jadi pengujiannya ditingkat aplikasi saja, apakah sudah jalan atau belum. Kalau untuk yang keamanan dan <i>stress test</i> jarang itu. Kecuali kalau sudah kejadian, misalnya tiba-tiba diakses lambat baru dilakukan. Itu saja kita yang kurang.                                                                                                                                                                                                                                                               |
| A.14.2.9 | Apakah ada peninjauan <i>source code</i> untuk memeriksa apakah ada kode berbahaya atau kerentanannya?<br><br>Itu tergantung adanya waktu atau tidak setelahnya. Kalau kita biasanya mengerjakan proyek itu dilanjutkan dengan proyek berikutnya. Jarang kita ada waktu untuk meninjau yang ini. Kecuali misalnya itu tadi, bukan kerentanan sih. Biasanya yang bikin lambat, misalnya ada <i>query</i> yang buat lambat atau ada fungsi yang seharusnya tidak seperti itu. Itu saja yang kita tinjau, tapi biasanya itu menunggu saat kejadian. |
| A.17.1.1 | Apa saja sistem informasi yang di- <i>backup</i> didalam <i>server</i> yang ditaruh di Telkom Gubeng?<br><br>Yang ada di Gubeng itu kalau tidak salah <i>website</i> ITS dan Webmail ITS. Jadi kalau ada yang mati atau gangguan, nanti akan dialihkan kesana.                                                                                                                                                                                                                                                                                   |

Narasumber : Hanim Maria Astuti, S.Kom., M.Sc.

Jabatan : Kasubdit Pelayanan Teknologi dan Sistem Informasi

Organisasi : DPTSI-ITS

| No Annex | Pertanyaan & Jawaban                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.5.1.1  | Apakah kebijakan untuk keamanan informasi dibuat dan dikomunikasikan ke karyawan dan pemangku kepentingan yang terkait?<br><br>Kalau soal kebijakan tentang keamanan informasi baru dibuat tahun kemarin tapi belum selesai. Kami kemarin ada mekanisme pengambil penelitian kebijakan, harapannya kan merilis kebijakan keamanan informasi. Nah itu sama pak Febriliyan (Direktur DPTSI-ITS) tahun ini harus dilanjutkan dan harus jadi. Kalau kemarin kan masih menggali, tapi kebijakannya disahkannya harusnya saat ini. Masalahnya repot mas kalau tidak ada kebijakan dan prosedur itu. |
| A.5.1.1  | Apakah tidak ada kebijakan keamanan informasi tertulis di organisasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|         |                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | Tidak ada, makanya ini ada satu program kerja yang membuat untuk tata kelolanya untuk tiga Subdit dan satu yang umum. Harusnya <i>quarter</i> I kami sudah memulai, tapi kami belum memulai karena pindahan sih.                                                                                                                                                                                    |
| A.6.1.2 | Apakah beberapa tugas dan area tanggung jawab yang berlawanan dipisahkan untuk mengurangi peluang perubahan dan penyalahgunaan tanpa izin atau tidak disengaja pada aset?                                                                                                                                                                                                                           |
|         | Sudah ada pembagian tugas dan area tanggung jawab.                                                                                                                                                                                                                                                                                                                                                  |
| A.6.1.5 | Apakah organisasi melakukan penilaian resiko/manajemen resiko sebagai bagian dari manajemen proyek apapun?                                                                                                                                                                                                                                                                                          |
|         | Kalau disini itu sifatnya kebanyakan kalau sudah terjadi, baru ditangani. Tapi kalau mitigasi yang sifatnya pencegahan itu, ya paling dari aspek teknis itu kabelnya diganti seperti begitu, tapi kalau tertulis apa resikonya terus pencegahnya apa, prosedurnya apa, kontrolnya apa, itu kami belum ada. Kami kan juga butuh resiko tertinggi disini itu apa, misalkan resiko dari sisi keamanan. |
| A.7.2.1 | Apakah terdapat pengarahan sebelum diberikan akses ke sistem informasi sesuai dengan peran dan tanggung jawab dalam keamanan informasi?                                                                                                                                                                                                                                                             |
|         | Mungkin yang kami lakukan sebatas jangan bagi-bagi <i>password</i> ke karyawan lain, sebenarnya mereka juga kan yang diberikan akses umumnya sudah tahu apa yang harus mereka lakukan.                                                                                                                                                                                                              |
| A.8.1.1 | Apakah aset yang berhubungan dengan informasi dan fasilitas pendukungnya diidentifikasi dan daftar inventarisnya didokumentasikan dan dikelola?                                                                                                                                                                                                                                                     |
|         | Tidak ada, semua aset seperti dokumen atau perangkat lunak masih belum tercatat.                                                                                                                                                                                                                                                                                                                    |
| A.8.1.1 | Jadi yang tercatat barang BMN itu ya?                                                                                                                                                                                                                                                                                                                                                               |
|         | Iya, tapi kan milik orang BAUK-ITS, kalau tidak salah E-Aset itu. Tapi kalau aset informasi internal apa, seperti dokumen atau perangkat lunak belum tercatat dan masih sedang direncanakan.                                                                                                                                                                                                        |
| A.8.1.2 | Jadi tidak tahu siapa yang memegang dokumen atau aset informasi tertentu?                                                                                                                                                                                                                                                                                                                           |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                 | <p>Itu mbak Widiyaningsih. Saya sih mintanya ke mbak Widiyaningsih, karena dia memegang akun Office 365 yang di DPTSI-ITS. Kayak <i>file</i> Power Point DPTSI-ITS kemudian dokumen-dokumen lain itu juga mbak Widiyaningsih. Cuma sebenarnya ada banyak dokumen yang lain yang dulu itu dipegang mbak Mudji yang sekarang sudah pindah. Mestinya kan ditarik dan disimpan, nah itu masih belum. Disimpan pun tapi tidak dicatat.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| A.8.1.2                         | <p>Siapa yang bertanggung jawab mengelola komputer yang digunakan karyawan?</p> <p>Kalau ada kerusakan fisik ke mas Cahya (Penyusun Laporan dan Pengelola BMN) karena masuk bagian Subdit Infrastruktur. Soalnya yang mendaftar aset komputernya siapa saja dan laptopnya ada berapa itu mas Cahya. Tapi kalau pemasangan Windows-nya dan sebagainya ke mas Rizky karena masuk bagian Subdit Pelayanan. Soalnya yang membawa perangkat lunak berlisensi seperti Windows itu disini, Subdit Pelayanan.</p>                                                                                                                                                                                                                                                                                                                                                                                                        |
| A.8.1.2<br>A.12.1.1<br>A.18.1.2 | <p>Bagaimana tata cara pemasangan perangkat lunak pada komputer?</p> <p>Kami melepas semua pemasangan perangkat lunak. Kayak duluan ketika mereka membutuhkan kode lisensi, kami melakukan <i>remote</i> ketika mereka mengkontak. Pak Arif Junaedi bicara “Hah? komputer saya mau di-<i>remote</i>? Males aku tidak mau, tidak aman”. Soalnya untuk aktivasi kan ada metode MAK yang kita lakukan injeksi kode lisensinya sama model KMS yang satu institusi bisa mengaktifasi dengan satu serial number. Dulu pakai yang MAK, tapi sekarang pakai yang KMS. Jadi kami tidak perlu direpoti bolak-balik, apalagi kalau dibayangkan ada 1000 orang yang minta aktivasi terus kami harus melakukan <i>remote</i>. Jadi mereka memasang sendiri dan sudah ada panduannya, seperti kalau Windows 8 harus apa konfigurasinya. Semuanya sudah ada di <a href="http://unduh.its.ac.id">http://unduh.its.ac.id</a>.</p> |
| A.8.1.3                         | <p>Apakah peraturan dalam menggunakan aset yang berhubungan dengan informasi dan fasilitas pendukungnya didokumentasi dan diterapkan?</p> <p>Tidak ada, akarnya itu tadi kebijakannya belum ada soalnya. Memang sih lebih aman patuh ke ISO 27001, tapi jalannya itu panjang. Tapi kami terbentur jumlah SDM-nya sangat kurang, jadi kami kebanyakan kurang untuk dokumentasi, dan sibuk dengan operasional dan menangani insiden. Pencegahannya kurang, jadikan mestinya kita bisa menebak apa terjadi dan apa yang bisa ditutup/mitigasinya. Orangnya kurang dan kadang memegang beberapa tugas.</p>                                                                                                                                                                                                                                                                                                           |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.8.2.1 | Apakah informasi diklasifikasikan berdasarkan nilai, kekritisannya, atau kerahasiaan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|         | Tidak ada, pandangan tentang mana informasi yang pribadi atau publik itu sendiri masih berbeda antara pak Febriliyan (Direktur DPTSI-ITS), kami Subdit Pelayanan, dan Subdit Pengembangan. Karena ya itu tadi prosedur dan kebijakan masih belum ada, sehingga klasifikasi data dan informasi belum jelas. Kayak misalkan dulukan kita buka Integra ITS, kita bisa lihat                                                                                                                                                                                                            |
|         | nilainya teman kita. Kalau sekarang sudah ditutup, karena menurut bu Anny (Kasubdit Pengembangan) itu adalah hal yang pribadi bagi setiap orang. Tapi kata pak Febriliyan tidak begitu, itu sifatnya internal untuk satu institusi jadi tidak masalah, tapi kalau untuk publik tidak boleh. Semuanya itu ada di kepala masing-masing, jadi itu masih belum tertulis.                                                                                                                                                                                                                |
| A.8.2.3 | Apakah prosedur untuk menangani aset, seperti untuk aset ini harus dienkripsi kalau disimpan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|         | Oh tidak ada disini, pokonya kalau soal kebijakan keamanan kebanyakan tidak ada.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| A.8.3.2 | DPTSI-ITS kan ada prosedur Pemusnahan Dokumen, itu fungsinya untuk apa?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|         | Itu yang mana? Kalau tidak salah untuk SNMPTN ya?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| A.8.3.2 | Apakah dokumen kertas yang bukan terkait SNMPTN dimusnahkan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|         | Tidak, karena itu tadi kami belum memiliki klasifikasi informasi. Jadi sifatnya yang sangat pribadi itu tidak dilakukan. Kami kan pakai sistem <i>online</i> , jadi berbaginya ke orang tertentu untuk mengurangi penggunaan kertas. Tapi kalau adapun, ya itu tadi kami belum ada klasifikasi informasi. “Mas-mas tolong dimusnahkan”, tidak juga kalau begitu. Kayak <i>password</i> semuanya di sistem, secara kertas itu tidak ada. Kita kan juga melayani informasi sensitif seperti lembar jawaban SNMPTN yang digudangkan dan dimusnahkan kayaknya setelah 3 sampai 5 tahun. |
| A.9.2.3 | Apakah alokasi dan penggunaan hak akses <i>administrator</i> dikontrol dan dibatasi melalui proses yang formal?                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|         | Untuk pemberian hak akses <i>administrator</i> , misalkan ada karyawan baru masuk ke DPTSI-ITS. Dia diberi tugas untuk menangani Integra ITS bagian                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <p><i>reset password</i>, ya kita berikan akses ke situ. Didalam sistemnya ada <i>log</i>-nya siapa yang punya akses kemana, misalnya SIM Keuangan, kita tahu siapa yang megang/administratornya. Didalam sistemnya itu sudah terdokumentasikan secara lengkap termasuk pengguna yang bukan <i>administrator</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| A.12.1.1 | <p>Apakah penerapan ISO 9000 sudah menjadi bagian dari aktifitas organisasi?</p> <p>Itu sudah tidak pernah dipakai, ISO 9000 itu kan manajemen kualitas organisasi. Selama saya disini ISO 9000 itu belum dikelola sama sekali. Masih belum terlihat dimana penerapan ISO itu, kan mestinya <i>PDCA</i> ya? Jadi kami itu aspek tata kelolanya yang kurang sekali.</p>                                                                                                                                                                                                                                                                                                                                                                                         |
| A.12.4.3 | <p>Apakah setiap aktifitas <i>administrator</i> sistem direkam (membuat, me-<i>reset</i> dan menghapus akun <i>email</i>) dan setiap <i>log</i> dilindungi dan ditinjau secara berkala?</p> <p>Iya tidak ada, pokoknya <i>log</i> itu kami kurang sekali. Cuma berdasarkan permintaan saja. Seringkali saya mengasih tahu agar harus melalui <i>email</i>, dengan harapan ketahuan siapa yang melakukan <i>reset</i>. Tapi kadang juga tidak begitu, misalkan pernah pak Wakil Rektor III minta untuk me-<i>reset password</i>, ya sudah saya <i>reset</i> sendiri, jadi tidak ada <i>log</i>. Kalau mas Jainul (Subdit Pelayanan) sih setiap <i>reset</i> atau apa punya dokumentasinya, cuma <i>log</i> yang otomatis dari sistemnya itu kami belum ada.</p> |
| A.13.2.4 | <p>Apakah di Subdit Pelayanan ada persyaratan untuk perjanjian kerahasiaan dan tidak-menyingskap informasi seperti dokumen Kesepakatan Bersama Menjaga Kerahasiaan Aset Sistem Informasi Institusi Dilingkungan Kampus ITS bagi Subdit Pengembangan?</p> <p>Kalau di Subdit Pelayanan tidak ada deh. Mungkin karena berhubungan dengan banyak sistem dan harus dijamin keamanannya, Subdit Pengembangan membuat perjanjian seperti itu bagi mereka.</p>                                                                                                                                                                                                                                                                                                        |
| A.16.1.4 | <p>Apakah ada penilaian atau pengklasifikasian laporan insiden, jadi bisa tahu mana harus ditangani terlebih dahulu meski kedua-duanya dilaporkan dengan waktu yang sama?</p> <p>Biasanya kami kan menangani berdasarkan yang duluan masuk, semuanya sih seharusnya melalui <i>email</i> kalau sekarang. Setelah ini kami kan sedang</p>                                                                                                                                                                                                                                                                                                                                                                                                                       |

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                           | <p>mengembangkan sistem umpan balik, yaitu E-Tiket. Maunya nanti semuanya harus lewat E-Tiket. Tapi kalau sekarang ada yang lewat telepon, <i>email</i>, mana begitu. Kalau lewat <i>email</i> kita tetap menangani siapa yang meminta duluan, tapi kalau ada yang lebih prioritas misalkan pak X yang dari sisi jabatan butuh penting maka itu yang didahulukan. Tapi kalau kategorisasi atau prioritasi insiden itu masih belum tertulis secara formal.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <p>A.17.1.1<br/>A.17.1.2</p>              | <p>Apakah organisasi sudah merencanakan <i>business continuity plan</i> atau <i>disaster recovery plan</i> berikut persyaratannya untuk situasi krisis atau bencana?</p> <p>Belum ada dokumen <i>BCP</i> dan <i>DRP</i> secara formal, namun tetap dilakukan oleh masing-masing bagian di DPTSI-ITS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <p>A.17.1.1</p>                           | <p>Apa saja sistem informasi yang di-<i>backup</i> didalam <i>server</i> yang ditaruh di Telkom Gubeng?</p> <p>Tidak, kami tidak punya. <i>DRC</i> yang <i>co-location</i> di Telkom Gubeng belum keisi dan memang kedepannya mau ditaruh kesitu. Kayaknya cuma <i>website</i> ITS saja yang ada.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <p>A.18.1.1<br/>A.14.1.1<br/>A.12.4.3</p> | <p>Apakah semua undang-undang/peraturan dan persyaratan kontrak diidentifikasi, didokumentasikan dan diperbaharui untuk organisasi dan setiap sistem informasi?</p> <p>Undang-undang atau peraturan pastinya dipenuhi dan diidentifikasi di DPTSI-ITS. Misalnya tentang peraturan ya, cuman seperti oh kita melakukan pengadaan, jadi jangan sampai ketubruk sama peraturan pemerintah yang apa. Kan ada peraturan pemerintah tentang pengadaan yang kurang dari 2,5 milyar harus dari perusahaan kecil, jadi jangan mencari perusahaan yang besar. Nah itu manajemen kualitasnya balik lagi ke ULP-ITS. Cuma kalau mengembangkan sistem seperti SIM Akademik kan berdasarkan peraturan akademik dan peraturan lainnya, tapi yang tahu itu pelanggan kami. Kami kan mengikuti pelanggan dan kami yang mempelajari, jadi pelanggan yang menterjemahkan dan kami memahami apa yang diminta pelanggan karena kami sudah berpikir itu sudah patuh terhadap peraturan. Kalau SIM pasti harus patuh peraturan, apalagi SIM Keuangan yang banyak sekali aturannya seperti pajak, remunerasi, dan lainnya. Jadi kalau patuh terhadap peraturan kebanyakan ada di sistem informasi terpadu, tapi kalau di Subdit Infrastruktur dan Subdit Pelayanan</p> |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <p>masih belum. Cuma kalau kami ada tapi tidak tertulis, misalnya ketika ada permintaan Integra ITS, kan semua orang bisa mengirimkan <i>email</i> untuk permohonan <i>reset password</i>. Tapi kan tetap harus ada autentikasi apakah benar siapa yang memohon, nah itu kami lakukan. Tapi kalau dari sisi tertulis kami masih belum ada karena kami hanya melakukan, jadi dokumen, <i>log</i> dan bukti itu tidak ada.</p>                                                                                                                                                                                                                                                                                          |
| A.18.1.2 | <p>Apakah prosedur diterapkan untuk memastikan kepatuhan terhadap undang-undang/peraturan yang berhubungan dengan hak kekayaan intelektual dan penggunaan lisensi perangkat lunak asli?</p> <p>Itu juga masuk kedalam kebijakan TIK, bukan keamanan informasi. Tidak ada sih. Kami itu bekerjanya berdasarkan <i>common sense</i>, kalau dari sisi perangkat lunak itu memang mimpinya departemen TIK disebuah organisasi kan? Semua harus menggunakan perangkat lunak asli dan dimanfaatkan dengan baik. Tapi peraturan untuk itu masih belum ada. Kalau tidak salah kan ada otomatis “oh perangkat lunak anda belum berlisensi”, itu masih belum disini. Jadi banyak sekali yang pakai perangkat lunak bajakan.</p> |
| A.18.1.2 | <p>Atau mungkin diatur agar tidak bisa memasang perangkat lunak secara bebas ya bu? Karena saya lihat disini ada pengguna komputer yang hak aksesnya <i>administrator</i>.</p> <p>Karena itu tadi kami masih kebanyakan menangani di operasional atau menangani masalah. Selama tidak ada permasalahan signifikan kan akhirnya jadi kurang prioritas. Seperti yang mas bilang tadi kenapa tidak ada pemblokiran perangkat lunak bajakan? Itukan sifatnya inovasi dan bukan bersifat operasional. Karena kami masih berkutat di operasional dan hal-hal yang bersifat peningkatan masih kurang. Kan hal-hal yang seperti itu bisa dibidang peningkatan.</p>                                                            |

Narasumber : Widiyaningsih, S.Kom.

Jabatan : Pranata Komputer Pelaksana Lanjutan (mengurusi dokumen ISO 9000)

Subdit : Subdirektorat Pelayanan Teknologi dan Sistem Informasi

| No Annex | Pertanyaan & Jawaban                                                                                                                                                                                                                                                                                                                     |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.6.1.3  | Apakah ada prosedur yang menspesifikasikan kapan dan siapa yang akan dihubungi (vendor, unit lain, pemerintahan) jika terjadi masalah?                                                                                                                                                                                                   |
|          | Tidak ada secara tertulis. Selama ini disini sudah tahu karena dari dulu itu tidak pernah berubah. Misalkan saya di Subdit Pelayanan, berarti saya terus disini. Jadi kalau mau menghubungi siapa sudah tahu.                                                                                                                            |
| A.7.2.1  | Apakah terdapat panduan tingkah laku yang berisikan ekspektasi keamanan informasi bagi karyawan didalam organisasi, seperti menyangkut kerahasiaan, perlindungan data, etika, penggunaan yang tepat peralatan dan fasilitas dan lainnya?                                                                                                 |
|          | Panduan seperti itu tidak ada disini.                                                                                                                                                                                                                                                                                                    |
| A.7.2.2  | Apakah terdapat pengujian untuk melihat penyerapan ilmu setelah dilakukan pelatihan kerja?                                                                                                                                                                                                                                               |
|          | Waktu itu pernah diadakan, jadi disuruh jawab pertanyaan sebelum dan sesudah pelatihan. Nah disitu nanti dilihat seberapa besar perbandingannya setelah dilakukan pelatihan.                                                                                                                                                             |
| A.8.1.1  | Apakah aset yang berhubungan dengan informasi dan fasilitas pendukungnya diidentifikasi dan daftar inventarisnya didokumentasikan dan dikelola?                                                                                                                                                                                          |
|          | Kalau itu biasanya ada dimasing-masing bagian dan didokumentasikan sesuai kebutuhan. Kalau misalkan perangkat keras dan barang-barang seperti meja atau lemari disini kita mengikuti sistem BMN dan ada petugasnya sendiri. Nah sedangkan kalau perangkat lunak kita ada SI Inventaris SIM nah itu punya data apa saja dan aset-asetnya. |
| A.8.2.1  | Apakah informasi diklasifikasikan berdasarkan nilai, kekritisannya, atau kerahasiaan, misalkan publik, internal, rahasia?                                                                                                                                                                                                                |



|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | Biasanya data-data yang ada di DPTSI-ITS kebanyakan <i>softcopy</i> , bukan <i>hardcopy</i> . Jadi kalau <i>softcopy</i> memang yang publik dan pribadi itu, biasanya kalau orang ini yang memegang ini berarti orang lain tidak boleh tahu selain dia dan kepalanya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| A.8.2.3 | <p>Apakah prosedur untuk menangani aset contohnya dokumen yang tadi pribadi harus diberi <i>password</i> untuk penyimpanan dan kalau dikirim harus diberi pengaman tambahan, sedangkan untuk yang publik tidak perlu saat penyimpanan didokumentasikan?</p> <p>Secara terdokumentasi tidak ada, kalau itu langsung jalan saja. Sudah biasa begitu, kita kerjakan. Kecuali kalau pemusnahan dokumen ada prosedurnya. Seperti disinikan memproses ujian masuk perguruan tinggi ataupun CPNS, itu ada data-data pelanggan kita yang dimusnahkan, itu ada prosedurnya. Terus untuk dokumen yang terkait dengan keuangan dan kantor menganut dari UPT Kearsipan ITS. Kalau tidak salah masing-masing punya daya simpan, seperti keuangan disimpan selama 5 tahun setelah itu boleh dimusnahkan. Itu ada petunjuknya, jadi kita mengikuti itu. Cara menyimpan surat dan dokumen kita mengikuti UPT Kearsipan ITS, kalau data itu tidak ada tertulis. Data setahu saya kita batasi yang mengakses sesuai dengan hak aksesnya masing-masing.</p> |
| A.8.3.2 | <p>Apakah media penyimpanan (media kertas atau elektronik) dibuang secara aman ketika tidak diperlukan menggunakan prosedur formal?</p> <p>Petunjuknya tadi dari UPT Kearsipan ITS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| A.9.2.3 | <p>Apakah DPTSI-ITS mengidentifikasi dan mendokumentasikan hak akses yang dimiliki karyawan kedalam sistem?</p> <p>Ya, disini pakai manajemen hak akses di Integra ITS yang bisa memberikan hak akses langsung ke karyawan. Misalkan karyawan A mau dikasih akses ke sistem B misalnya, langsung dia dapat hak akses tersebut. Jadi gak hanya pencatatan saja.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| A.9.2.3 | <p>Apa cakupan sistem pemberian akses oleh manajemen akses di Integra ITS? Apakah Webmail ITS, Git ITS dan sistem yang dimiliki Subdit Infrastruktur termasuk?</p> <p>Tidak mencakup kesana. Sistem tersebut tidak diatur di manajemen akses di Integra ITS.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.9.2.3  | Apakah terdapat hak akses yang memiliki jangka waktu <i>expired</i> ?                                                                                                                                                                                                                                                                                                                                                                                        |
|          | Disini tidak ada yang seperti itu.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| A.9.2.3  | Apakah terdapat pemisahan akun dengan hak akses <i>administrator</i> dengan akun untuk penggunaan biasa? Misalnya akun Integra ITS buat aktifitas <i>administrator</i> dibedakan dengan akun Integra ITS buat penggunaan biasa.                                                                                                                                                                                                                              |
|          | Kalau itu tidak ada pemisahan. Jadi akun itu ya bisa kita pakai buat kerjain yang lain.                                                                                                                                                                                                                                                                                                                                                                      |
| A.9.2.4  | Apakah alokasi informasi <i>password</i> (me-reset <i>password</i> ) pengguna <i>email</i> dikontrol melalui proses formal?                                                                                                                                                                                                                                                                                                                                  |
|          | Prosedur untuk me-reset <i>password email</i> ada. Kalau prosedur untuk lupa <i>password</i> mahasiswa melalui <i>website</i> -nya, sedangkan karyawan dan dosen melalui surat permohonan yang disetujui TU jurusan. Dulu lewat telepon bisa dengan menyebut identitas diri. Cuma dari sisi keamanan kurang. Kalau kita tahu orangnya sih tidak masalah, kalau tidak tahu orangnya itukan bahaya. Verifikasinya bagaimana? Ya verifikasinya dari TU jurusan. |
| A.11.2.5 | Apakah perangkat keras/lunak, peralatan dan informasi tidak boleh dibawa keluar organisasi tanpa izin terlebih dahulu?                                                                                                                                                                                                                                                                                                                                       |
|          | Boleh untuk urusan pekerjaan. Kayak tim jaringan mengecek jaringan di Asrama, itu boleh. Tapi ada sih dulu ya, saya tidak tahu dan yang tahu mas Cahya (Penyusun Laporan dan Pengelola BMN). Kalau boleh dibawa tapi kita harus mengisi formulir, seperti nama barang, kemana, tujuannya.                                                                                                                                                                    |
| A.12.1.1 | Apakah prosedur operasional didokumentasikan dan tersedia untuk semua pengguna yang membutuhkan?                                                                                                                                                                                                                                                                                                                                                             |
|          | Disini kita punya dokumen ISO 9000 yang isinya prosedur-prosedur. Kalau ada mahasiswa yang mau penelitian atau karyawan baru bisa dilihat didalam dokumen ISO-nya.                                                                                                                                                                                                                                                                                           |
| A.12.1.1 | Apakah ada pembaharuan dokumen ISO 9000? Yang sudah ada kan tahun 2014. Saya juga melihat di <i>masterplan</i> bahwa DPTSI-ITS sudah memperbaharui dokumen ISO 9000.                                                                                                                                                                                                                                                                                         |
|          | Tidak ada, dokumen ISO yang ada sudah yang terbaru. Kalau ISO kami sedang mengerjakan ISO 27001. Keamanan informasi.                                                                                                                                                                                                                                                                                                                                         |

|          |                                                                                                                                                                                                                          |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.13.2.3 | Siapa yang termasuk pimpinan yang dapat menggunakan layanan <i>email</i> di Office 365?                                                                                                                                  |
|          | Itu khusus untuk pimpinan dari Kasubag/Kasubdit sampai ke atas. Jadi <i>email</i> -nya pimpinan itu sinkronisasi dengan Office 365.                                                                                      |
| A.13.2.3 | Berapa kapasitas yang diberikan pada layanan <i>email</i> yang bekerjasama dengan Microsoft?                                                                                                                             |
|          | Dulukan standarnya pimpinan di Webmail ITS 1 GB, tapi sekarang dipindah ke Office 365 jadi <i>unlimited</i> .                                                                                                            |
| A.16.1.2 | Apa saja jalur komunikasi yang digunakan untuk pelaporan ke DPTSI-ITS?                                                                                                                                                   |
|          | Bisa melalui telepon, <i>email</i> dan sistem E-Tiket. Untuk E-Tiket sendirikan masih baru tahun lalu dan dalam masa uji coba, jadi layanan pelaporan E-Tiket masih khusus untuk layanan yang disediakan DPTSI-ITS saja. |
| A.18.1.2 | Apakah terdapat daftar aset yang perlu dijaga hak kekayaan intelektualnya?                                                                                                                                               |
|          | Tidak ada dokumen seperti itu disini.                                                                                                                                                                                    |
| A.18.1.2 | Apakah DPTSI-ITS menyadarkan pemangku kepentingan untuk melindungi hak kekayaan intelektual dan menyampaikan sanksi jika melanggar hak kekayaan intelektual?                                                             |
|          | Kalau secara khusus sih tidak kita lakukan. Yang kita lakukan cuma penyediaan portal perangkat lunak asli yang bisa dipakai karyawan, mahasiswa dan dosen ITS.                                                           |

Narasumber : Jainul Arifin

Jabatan : Pranata Komputer Pelaksana (mengurusi administrasi *email* ITS)

Subdit : Subdirektorat Pelayanan Teknologi dan Sistem Informasi

| No Annex | Pertanyaan & Jawaban                |
|----------|-------------------------------------|
| A.8.1.2  | Siapa pengelola sistem Webmail ITS? |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | Sebenarnya untuk urusan <i>administrator</i> akun seperti membuat, me- <i>reset</i> dan menghapus ada dua orang. Tapi karena saya yang sering melakukan, jadi saya terus yang pegang. Untuk sistemnya dipegang mas Jananta (Subdirektorat Infrastruktur).                                                                                                                                                                                |
| A.8.1.2 | Siapa yang bertugas memasang sistem operasi dan perangkat lunaknya?<br><br>Kalau disini biasanya mas Rizky (Subdit Pelayanan) yang memasang, tapi tidak juga sih. Kalau memang bisa dilakukan masing-masing, ya biasanya mereka lakukan sendiri.                                                                                                                                                                                         |
| A.9.2.1 | Apakah proses pendaftaran akun <i>email</i> diterapkan secara formal?<br><br>Kalau pembuatan akun <i>email</i> untuk mahasiswa baru bisa dilakukan melalui <i>website</i> -nya. Kalau pembuatan akun <i>email</i> untuk karyawan atau dosen bisa dilakukan melalui surat permohonan. Isinya nama alamat <i>email</i> dan <i>password</i> sementara. Kadang tidak dikasih tahu mau apa <i>password</i> sementara, jadi saya buat sendiri. |
| A.9.2.1 | Apa ada penolakan pembuatan akun <i>email</i> baru?<br><br>Untuk penolakan tidak ada, adanya kalau alamat <i>email</i> yang diminta tidak sesuai format yang benar. Contohnya ada yang minta alamat <i>email</i> <a href="mailto:ftpro-its@ie.its.ac.id">ftpro-its@ie.its.ac.id</a> yang mana tidak boleh menambahkan kata “its” lagi di alamat <i>email</i> .                                                                           |
| A.9.2.4 | Apakah alokasi informasi <i>password</i> (me- <i>reset password</i> ) pengguna <i>email</i> dikontrol melalui proses formal?<br><br>Untuk aktifitas <i>reset password</i> mahasiswa kan bisa melalui Webmail ITS-nya, masukin informasi akun Integra ITS. Sedangkan untuk karyawan atau dosen harus mengirimkan surat keterangan yang ditanda tangani jurusan.                                                                           |
| A.9.2.4 | Apakah ada cara selain yang disebutkan untuk me- <i>reset password</i> ?<br><br>Waktu itu pernah ada mahasiswa diluar kota yang minta di <i>reset email</i> -nya, karena tidak bisa melalui <i>website</i> -nya. Jadi ya saya bantu asal mengirimkan hasil <i>scan</i> KTM-nya, tapi kasus ini tidak sering sih.                                                                                                                         |
| A.9.2.4 | Apakah sistem memaksa/mengharuskan pengguna untuk mengganti <i>password</i> yang sudah di- <i>reset</i> ?                                                                                                                                                                                                                                                                                                                                |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Sistem tidak memaksa pengguna harus mengganti <i>password</i> sementara yang diberikan. Untuk sistem Integra ITS kan sudah diterapkan, jadi di halaman awal setelah <i>login</i> ada formulir untuk mengganti <i>password</i> .                                                                                                                                                                                              |
| A.9.2.5  | Apakah ada peninjauan hak akses pengguna <i>email</i> (seperti apakah ada akun yang belum terhapus) dalam jangka waktu tertentu?<br><br>Untuk peninjauan seperti itu tidak dilakukan. Karena pas penghapusan akun <i>email</i> kan sebelumnya di cari namanya di sistem dan kelihatan semua akun yang dimiliki sama pengguna itu.                                                                                            |
| A.9.2.6  | Apakah hak akses semua pengguna <i>email</i> dihapuskan ketika pemberhentian kerja atau kontrak/perjanjian, atau kelulusan mahasiswa?<br><br>Biasanya saya dikirim surat pemberitahuan melalui <i>email</i> dengan <i>scan</i> suratnya dari unit atau jurusan untuk penghapusan akun <i>email</i> tertentu.                                                                                                                 |
| A.9.2.6  | Apakah proses penghapusan langsung dilakukan? Dan bagaimana dengan mahasiswa?<br><br>Kalau untuk karyawan atau dosen langsung dilakukan penghapusan, sedangkan kalau untuk mahasiswa diberi waktu 3 bulan.                                                                                                                                                                                                                   |
| A.9.3.1  | Apakah pengguna disyaratkan dan disarankan untuk mengikuti praktek penggunaan <i>password</i> yang aman?<br><br>Sarannya ada, tapi kalau pelaksanaannya dimasing-masing orang. Bahkan ada akun <i>email</i> ITS dan Integra ITS milik karyawan yang dipegang sama unit atau jurusannya. Karena karyawannya sudah sepuh-sepuh jadi dibantu untuk pengisian SKP dan aktifitas lainnya.                                         |
| A.12.4.3 | Apakah setiap aktifitas <i>administrator</i> sistem direkam (membuat, me-reset dan menghapus akun <i>email</i> ) dan setiap <i>log</i> dilindungi dan ditinjau secara berkala?<br><br>Kalau secara otomatis di sistemnya tidak ada, memang kurangnya di sistem itu pencatatan <i>log</i> -nya. Tapi saya membuat laporannya sendiri pakai bantuan Ms. Word yang isinya <i>screenshot</i> setiap <i>email</i> yang saya buat. |
| A.13.2.3 | Berapa kapasitas yang diberikan pada layanan <i>email</i> yang dikelola ITS?                                                                                                                                                                                                                                                                                                                                                 |

|          |                                                                                                                                                                                                                                                                                                                                                 |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Sekarang kapasitas yang diberikan 200 MB. Kalau saya yang menggunakan sih 1 GB biar masuk semua <i>email</i> -nya.                                                                                                                                                                                                                              |
| A.13.2.3 | Masih ada ya karyawan atau dosen yang menggunakan layanan <i>email</i> yang dikelola ITS?                                                                                                                                                                                                                                                       |
|          | Masih banyak yang menggunakan. Bahkan ada dosen yang mengatakan takut kalau datanya disimpan di Google, lebih percaya sama yang di ITS.                                                                                                                                                                                                         |
| A.15.1.3 | Apakah pengguna <i>email</i> yang memilih layanan Google bisa pindah kembali menggunakan layanan <i>email</i> yang dikelola ITS?                                                                                                                                                                                                                |
|          | Bisa mas, pindah dari Google ke ITS asal kapasitas <i>email</i> dari Google yang terisi tidak melebihi 200 MB. Kalau melebihi biasanya ada <i>email</i> yang terhapus. Selain itu semua <i>file attachment</i> harus di- <i>backup</i> dulu sama mereka ditempat lain, karena proses pemindahan tidak sampai memindahkan <i>file</i> -nya juga. |

Narasumber : Dr.Eng. Febriliyan Samopa, S.Kom., M.Kom.

Jabatan : Direktur DPTSI-ITS

Organisasi : DPTSI-ITS

| No Annex | Pertanyaan & Jawaban                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.6.2.2  | Apakah ada kebijakan yang mengatur keamanan pada laptop atau komputer pribadi yang digunakan karyawan?                                                                                                                                                                                                                                                                                                                                                                                                        |
|          | Kalau kebijakan untuk laptop atau sistem pribadi tidak ada.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| A.7.1.1  | Apakah ada prosedur untuk verifikasi latar belakang dan penyaringan karyawan yang dibutuhkan?                                                                                                                                                                                                                                                                                                                                                                                                                 |
|          | Kalau disini tidak dilakukan. Karena yang mengeluarkan pusat, termasuk memperbaharui kontrak dan lain-lainnya itu dilakukan pusat baik untuk karyawan honorer (non-PNS) dan PNS. Karena karyawan itu pada dasarnya karyawan pusat yang menempatkan, jadi ketika merekrut pun kita tidak bisa merekrut. Kita cuma meminta ke Direktorat SDM dan Organisasi, nanti mereka yang buka lowongan, mengetes dan lain-lain. Setelah diterima baru dikirimkan kesini. Kita cuma bisanya kembalikan semua ke Direktorat |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | SDM dan Organisasi, misalnya ada disipliner yang bersangsi berat, apakah dipecat, dirotate atau disuruh jadi satpam saya tidak tahu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| A.7.2.1 | Apakah karyawan dijelaskan tentang peran dan tanggung jawabnya serta kebijakan dan prosedur sebelum bekerja?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|         | Kalau mau kerja disini tidak, yang saya lakukan tiap tahun pengarahan semacam rapat kerja, tahun ini targetnya apa dan harus melakukan apa saja. Terus kalau ada karyawan baru akan kami beritahu, karena yang merekrut karyawan baru kan bukan kami tapi pusat. Kalau ada karyawan baru saya diberitahu pusat lewat surat. Kayak kemarin ada karyawan baru masuk,                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|         | mbak Sofi yang kerja dulu di MMT-ITS. Pas karyawannya datang, saya kasih tahu nanti kerjanya bagaimana, mbak Sofi tanggung jawabnya apa, terus saya serahkan kepada Kasubdit langsungnya. Bawahan langsung saya ada 3 yaitu sekretaris, bendahara sama pembantu umum, Setelah itu bawahan langsung saya adalah Kasubdit Pelayanan, Kasubdit Pengembangan dan Kasubdit Infrastruktur. Dalam hal ini mbak Sofi itu ada dibawahnya Kasubdit Pelayanan jadi saya ajak ke atasan langsungnya biar atasannya yang ngasih tahu dia <i>job desc</i> -nya apa. Terserah apa atasan langsungnya dia mau diberi <i>job desc</i> apa saja.                                                                                                                                                                                                                                                                                                                 |
| A.7.2.1 | Apakah ada sistem pelaporan <i>anonym</i> untuk karyawan yang melanggar kebijakan dan prosedur?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|         | Sistemnya tidak ada, karena biasanya pelaporan itu berjenjang. Jadi karyawan itu laporannya ke atasan langsungnya, AL istilahnya. Jadi atasan langsungnya lapor ke atasan langsungnya lagi dan seterusnya. Jadi kalau tidak bisa diselesaikan di atasan langsungnya, nanti dieskalasi naik. Kalau misalnya laporan sampai ke saya, saya tidak bisa menyelesaikan maka saya langsung ke atasan saya pak Wakil Rektor III, nanti pak Wakil Rektor III yang menyelesaikan. Jadi kalau di PNS itukan sistemnya berjenjang seperti itu. Kalau eskalasinya sudah sampai di levelnya Rektor, nanti ada namanya Bina Aparat. Lembaga khusus menangani dan menindak pelanggaran yang tidak bisa diselesaikan oleh atasannya masing-masing, selama bukan pelanggaran bukan ranah kriminal. Kalau ranah kriminal dilaporkan ke polisi. Pernah ada di unit lain karyawannya menggelapkan dana untuk membeli air minum beberapa bulan, ya dibawa ke polisi. |
| A.7.2.1 | Jadi kalau atasan langsungnya yang bermasalah, lapornya ke diatas atasan langsungnya ya pak?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | Ya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| A.7.2.3             | Apakah proses pendisiplinan dibuat secara formal dan dikomunikasikan untuk menindak karyawan yang melakukan pelanggaran keamanan informasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|                     | Kalau itu ada Direktorat Hukum Organisasi dan Tata Laksana untuk masalah internal, misalnya ini nanti konsekuensi hukumnya apa. Contohnya ada mahasiswa yang meng- <i>hack</i> sistem kita, itu kita serahkan kesana mau diapain. Kalau misalnya mereka bilang “oh lapor polisi”, nanti                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                     | mereka yang lapor polisi. Dulu pernah terjadi <i>password</i> -nya pak Darlis kepala Jurusan Informatika di <i>hack</i> sama mahasiswanya. Ya kan di <i>log</i> tercatat yang akses siapa, dari mana, dan seterusnya. Lalu dicari dari Lab ini dan jam sekian, langsung diintrogasi kan orangnya sedikit tidak banyak. Habis itu saya tidak tahu mahasiswanya disangsi apa. Tapi kalau masalahnya ada orang dari sini entah mahasiswa atau apa yang nge- <i>hack</i> akunnya orang dan mengambil uangnya, nah itu baru Unit Layanan Hukum (ULH-ITS) karena masalah eksternal, jadi pihak luar yang menuntut. Pernah kita dituntut kalau tidak salah 2014, salah satu akun <i>email</i> kita menyebarkan foto-foto yang masuk kategori pornografi. Jadi <i>email</i> kita di <i>hijack</i> orang dan terus dijadikan buat mengirim foto pornografi. Itu ada lembaga yang menuntut kita karena domain kita dianggap menyebarkan foto pornografi itu. Akunnya ternyata setelah kita lacak itu tidak ada di kita, cuma dia pakai domain kita. Untuk mengurus masalah hukum tadi ULH-ITS, kita cuma menyediakan bukti fisik saja. |
| A.8.1.3<br>A.13.1.1 | Apakah ada peraturan tentang penggunaan <i>internet</i> dan komputer?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                     | Kalau kebijakannya tidak ada, tapi cuma penggunaannya saja. Misalnya untuk facebook dan media sosial pada jam kantor kita batasi <i>bandwidth</i> -nya. Karena pada jam kantor diharapkan lebih banyak dipakai untuk mengurus jurnal dan lain-lain.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| A.8.1.3<br>A.13.1.1 | Itu untuk karyawan saja pak?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|                     | Untuk semua, seperti mahasiswa, karyawan, dosen. Jadi kita tidak batasi dari siapa, yang terpenting batasi kemana.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| A.8.2.1             | Apakah informasi diklasifikasikan berdasarkan nilai, kekritisannya, atau kerahasiaan (contohnya rahasia, internal, publik)?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |



|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                     | Klasifikasi resminya itu tidak ada, tapi yang ada arahan dari pak Wakil Rektor III. Jadi pak Wakil Rektor III ngomong “ini untuk konsumsi internal saja, ini boleh ke publik, ini rahasia”. Kita ada beberapa situs yang hanya bisa dibuka internal misalnya SIM Akademik, ada yang pribadi hanya tertentu saja yang boleh melihat misalnya SIM Keuangan, ada juga yang publik misalnya www jadi semuanya orang bisa akses. Setiap kali beliau memintakan kita untuk membuat sesuatu akan saya tanyakan “ini yang boleh akses siapa”, oh kalangan terbatas jadi pribadi.                                                                                                                                                                                                                                                                                                                             |
| A.8.2.1             | Jadi dokumen resminya tidak ada ya pak?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                     | Surat atau dokumen resminya tidak ada. Kami tidak pernah dikasih dokumen resmi sama pak Wakil Rektor III yang isinya ini loh yang boleh dan yang tidak boleh. Kita diarahkan sewaktu rapat.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| A.10.1.1            | Apa jenis kontrak yang dimiliki DPTSI-ITS untuk masalah <i>SSL/TLS</i> ?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                     | <i>SSL</i> itu kita ke DigiCert Inc. dengan lama kontraknya tahunan melalui <i>provider bandwidth</i> . Kita kontrak <i>bandwidth</i> itu sekaligus sama kontrak <i>SSL</i> -nya, jadi satu kontrak. Jadi kalau kita mau beli <i>bandwidth</i> , siapapun <i>provider bandwidth</i> -nya yang menang, sekarangkan yang menang Telkom. Maka didalam kontraknya dia harus menyediakan <i>SSL</i> sekalian. Cuma kita minta kontraknya itu domain ya, jadi semua sub domain yang ada dibawah <a href="http://its.ac.id">its.ac.id</a> harus sudah tersertifikasi dengan <i>SSL</i> tersebut. Akhirnya kita biasanya bilang vendornya sebaiknya DigiCert, karena dia bisa buat sertifikat yang bintang. Jadi <a href="http://*.its.ac.id">*.its.ac.id</a> , didepannya apa saja mau dia. Domainnya satu <a href="http://its.ac.id">its.ac.id</a> , cuma <i>host</i> -nya atau sub domainnya bisa banyak. |
| A.10.1.1<br>A.8.1.1 | Jadi pengadaan dengan pelelangan termasuk <i>ISP</i> juga? Ada tidak pengadaan yang tidak pakai pelelangan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|                     | Ya, karena biayanya sangat besar. Kontraknya saja untuk <i>bandwidth</i> termasuk <i>SSL</i> -nya nilainya lebih dari 4 miliar. Kalau pengadaan yang tidak pakai lelang ya pengadaan barang, kayak ULP-ITS kemarin beli kursi atau kertas. Kalau di inventaris, barang yang bisa habis itu bisa.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| A.10.1.1            | Soalnya saya cek ada beberapa sistem yang <i>SSL</i> -nya menggunakan versi lama, sedangkan sistem yang lain sudah baru. Apa mungkin karena petugasnya lupa mengganti?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Bukan, kalau yang versi lama itu berarti yang dipasang oleh unit-unit sendiri. Kalau yang ditanggung jawab kami seperti akademik, keuangan dan kepegawaian itu saya jamin pasti terbaru. Kalau di unit-unit kan kita cuma kasih <i>virtual private server</i> , dan yang mengisi mereka sendiri. Mungkin saja mereka mengisi versi yang lama, bahkan sudah diisi tapi tidak pernah diperbaharui sama sekali sampai sekarang bisa jadi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| A.13.1.2 | <p>Apakah mekanisme keamanan, tingkat layanan dan kebutuhan manajemen pada semua layanan jaringan dispesifikasikan dan dimasukkan kedalam perjanjian kontrak dengan <i>ISP</i>?</p> <p>Yang paling kita butuhkan untuk keamanan itu <i>anti-virus</i>, <i>anti-spam</i>, <i>anti-DDoS</i>. Karena kita sering dapat paket <i>DDoS</i>, jadi dari mana mau mencoba <i>men-down</i> kan <i>server</i> kita. Kalau misalkan kita cekat disini, kita bisa cuma akibatnya trafik kita disini yang mau keluar berat karena berebutan jalan sama yang mau <i>nge-DDoS</i> walaupun kita sudah tolak disini. Kalau bisa ditolak di <i>ISP</i> berarti <i>bandwidth</i> kita tidak kemakan. Terus <i>anti-spam</i> karena yang paling banyak dan menjadi masalah itu <i>spam</i>. <i>Email</i> kita di <i>spam</i> beratus-ratus tidak karuan. Terus <i>anti-virus</i> karena seringkali virus yang masuk ke jaringan dan kalau bisa sudah di <i>filter</i> di <i>ISP</i>. Jadi <i>ISP</i> sudah ada <i>anti-virus</i> sehingga tidak ada lagi <i>virus</i> yang masuk ke kita, <i>spam</i> juga demikian.</p> |
| A.13.1.2 | <p>Apakah layanan <i>ISP</i> harus <i>up</i> berapa persen sudah termasuk dalam perjanjian kontrak?</p> <p>Itu ada dan biasanya kita memasukkan dalam kontrak bahwa 99.75% harus <i>up</i> kalau tidak salah. Selain itu disalah satu kontraknya juga menyebutkan bahwa Telkom menyediakan <i>disaster recovery center</i> di Gubeng.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| A.13.1.2 | <p>Apakah DPTSI-ITS menggunakan 2 <i>ISP</i> untuk koneksi <i>internet</i>?</p> <p><i>ISP</i> kita cuma ada satu Telkom, cuma ada dua jalur. Jalur yang pertama IP transit yang utama, terus kita juga punya backup yaitu Astine. IP transit itu koneksi langsung keluar. Jadi kita dikasih <i>IP address</i>, dia cuma transit saja jadi koneknya langsung ke kita tidak mampir ke dia.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| A.13.1.2 | Jadi jalurnya beda, kalau yang satu mati atau putus masih bisa konek ya?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | Iya beda, tapi kalau Telkom-nya mati tidak tahu lagi karena sama-sama Telkom. Makanya pak Wakil Rektor IV punya wacana mau berlangganan Indosat. Jumlahnya tidak besar, 100 MB mungkin. Cuma buat <i>backup</i> saja.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| A.13.2.2 | <p>Apakah perjanjian menyinggung pengiriman yang aman pada informasi bisnis diantara organisasi dengan pihak ketiga?</p> <p>Kalau kita biasanya pakai <i>VPN</i>. <i>VPN</i> itu kan terenkripsi tapi <i>sameless</i>. Pokoknya kita konek ke <i>VPN</i>, masukin nama pengguna dan <i>password</i>, lalu kita sudah bisa mengakses seperti jaringan biasa. <i>VPN</i>-nya dikelola disini. Dulukan namanya Speedy Campus sekarang IndiHome Campus, nah itu kita menggunakan <i>VPN</i>. Jadi kalau dari luar mau mengakses kedalam kita gunakan <i>VPN</i>.</p>                                                                                                                                                                                                                          |
| A.15.1.2 | <p>Apakah semua persyaratan keamanan informasi yang terkait dibuat dan disetujui oleh setiap vendor yang akan mengakses, memproses, menyimpan, mengkomunikasikan atau menyediakan komponen infrastruktur TIK untuk organisasi?</p> <p>Ada <i>non-disclosure agreement</i>-nya. Jadi kalau kita kesana pokoknya ada dokumen yang harus ditandatangani banyak. Perjanjian tersebut bagi kedua belah pihak karena masing-masing punya hak dan kewajiban. Misalnya bahwa mereka tidak boleh mengintipi data kita dan ada dendanya juga.</p>                                                                                                                                                                                                                                                   |
| A.15.1.3 | <p>Apakah ada kebergantungan pada vendor tertentu?</p> <p>Bukan bergantung pada vendor tertentu, tapi kita mengusahakan agar tidak terlalu banyak merek. Misalkan untuk <i>server</i> kita lebih memilih HP (Hawlett Packard). Bukan berarti harus HP, tapi kalau HP lebih baik. Kalau perangkat jaringan kita lebih memilih CISCO. Tapi vendornya siapa saja boleh, mau Telkom atau apa. Hal ini dikarenakan berhubungan dengan masalah investasi. Misalkan pelatihan seperti CISCO dari awal sampai akhir ada banyak beberapa level dan harganya mahal-mahal, terus ada merek lain masuk harus pelatihan mahal-mahal lagi. Nah itu kan tidak masuk akal dan tidak investasi <i>friendly</i>. Jadi kita usahakan jangan banyak-banyak merek biar investasi pelatihannya bisa rendah.</p> |
| A.15.1.3 | <p>Saya kira kalau vendornya misalnya HP maka dia sendiri yang melakukan.</p> <p>Karena kalau pengadaanya dibawah 2,5 miliar, maka vendornya sendiri HP misalnya tidak bisa masuk. Karena diakan kelasnya <i>enterprise</i> harus diatas</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | 2,5 miliar. Yang pasti ikut vendor-vendor kelas kecil istilahnya.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| A.15.2.1 | Apakah organisasi mengawasi, meninjau dan mengaudit layanan yang diberikan vendor secara berkala?                                                                                                                                                                                                                                                                                                                                                                                                                            |
|          | Yang melakukan penilaian vendor itu ULP-ITS, karena yang melakukan pengadaan itu mereka.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| A.15.2.1 | Apakah DPTSI-ITS mengawasi dan memastikan secara berkala layanan yang disediakan <i>ISP</i> sesuai dengan apa yang dijanjikan?                                                                                                                                                                                                                                                                                                                                                                                               |
|          | Itu pasti kita monitor. Kayak kemarin “oh lambat” terus kita komplain dan kita <i>capture</i> , ternyata <i>delay</i> -nya tinggi. Kalau kita mengakses ke kita sendiri atau lokal kan cepat dan tidak ada masalah. Tapi begitu ada komplain dari luar “Eh ITS kok di akses dari luar kok lambat?”, baru kita <i>capture</i> dan kita kirimkan dari <i>ISP</i> . Karena kita dari jaringan lokal kan tidak pernah lambat.                                                                                                    |
| A.15.2.2 | Apakah perubahan ketentuan layanan oleh vendor diatur dengan memperhatikan kekritisitas proses, sistem dan informasi bisnis yang terlibat?                                                                                                                                                                                                                                                                                                                                                                                   |
|          | Kalau ada perubahan ketentuan kita tinjau ulang kontraknya. Jadi kalau misalnya masih dapat diterima kondisinya, sesuai dan tidak melanggar isi kontrak biasanya kita biarkan. Kalau misalkan ada yang melanggar tapi tidak berat biasanya kita minta kompensasi saja, contoh kontrak <i>ISP</i> kan 99.75% tapi ternyata “oh tidak bisa, cuma bisa 99%”, ya sudah kita minta kompensasi. Apa kompensasinya kalau begitu? Apa kita dikasih <i>disaster recovery center</i> baru atau apa. Jadi kita negoisasi kompensasinya. |
| A.16.1.4 | Apakah ada penilaian atau pengklasifikasian laporan insiden, jadi bisa tahu mana harus ditangani terlebih dahulu meski kedua-duanya dilaporkan dengan waktu yang sama?                                                                                                                                                                                                                                                                                                                                                       |
|          | Kalau saya tidak pernah berurusan dengan komplain, yang lebih tahu itu bu Hanim (Kasubdit Pelayanan). Selama ini sih belum ada kecuali ada panggilan khusus. Klasifikasinya itu berdasarkan jabatan yang minta, kalau yang mintanya pak Rektor ITS pasti didahulukan dengan pak dosen.                                                                                                                                                                                                                                       |
| A.17.1.1 | Apakah organisasi sudah merencanakan <i>business continuity plan</i> atau <i>disaster recovery plan</i> berikut persyaratannya untuk situasi krisis atau bencana?                                                                                                                                                                                                                                                                                                                                                            |
|          | Kalau <i>disaster recovery</i> kita ada, <i>co-location</i> di Telkom Gubeng.                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.17.1.1 | <p>Apa saja sistem informasi yang di-<i>backup</i> didalam <i>server</i> yang ditaruh di Telkom Gubeng?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|          | <p>Kalau yang di-<i>backup</i> apa saja, saya tidak hapal. <i>Server</i> apa saja dan data apa saja saya tidak tahu pasti, yang tahukan orang teknis. Soalnya kan <i>database</i>-nya banyak. Mungkin bisa ditanyakan ke mas Budi. Yang jelas <i>backup</i>-nya itu dilakukan harian.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| A.17.1.2 | <p>Apakah organisasi membuat, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol keamanan <i>BCP</i> atau <i>DRP</i> untuk situasi krisis atau bencana?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|          | <p>Kalau dokumentasinya ada, tapi kalau prosedurnya bagaimana itu saya kurang jelas. Tapi yang jelas arahnya ada. Jadi kita punya satu rak penuh di Telkom Gubeng yang terdiri atas beberapa <i>server</i> yang digunakan untuk mem-<i>backup</i> data yang ada disini.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| A.17.2.1 | <p>Berapa lama waktu perangkat atau komponen yang dibeli melalui pengadaan sampai?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|          | <p>Biasanya pengadaan alatnya tergantung ketersediaannya. Pernah <i>hardisk</i>-nya <i>server</i> rusak. <i>Hardisk</i>-nya kecil 15.000 rpm pesan di Jakarta tidak ada, Singapura tidak ada, yang ada di Amerika dan perlu nunggu 2 minggu. Kalau ada di Jakarta 1 hari, kalau ada di Singapura 1 minggu, kalau di Amerika 2 minggu.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| A.18.1.2 | <p>Apakah prosedur diterapkan untuk memastikan kepatuhan terhadap undang-undang/peraturan yang berhubungan dengan hak kekayaan intelektual dan penggunaan lisensi perangkat lunak asli?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|          | <p>Kita tidak pernah melakukan karena kita tidak memiliki akses. Pada dasarnya kita kan hanya menyediakan tempat/mesin/<i>VPS</i>, jadi apa yang dipasang disana dan isinya apa kita tidak tahu. Bahkan sering kali kita tidak punya <i>login</i>-nya, ya <i>login</i>-nya ada sama mereka, kecuali yang memang ditangani pekerja kita. Contohnya SIM Keuangan, SIM Kepegawaian atau sistem yang merupakan <i>core bisnis</i> kita, seperti akademik, keuangan dan kepegawaian. Itu kita pastikan tidak ada yang legal, pasti legal semua. Tapi kalau yang unit-unit kan mereka hanya minta <i>VPS</i> saja, itu <i>VPS</i>-nya diisi apa kita tidak tahu. Misalnya di-<i>hack</i> orang, ya sudah kita <i>restore</i> aja <i>VPS</i>-nya. Isinya <i>restore</i>-nya apa kita tidak tahu, pokoknya kita <i>restore</i> aja.</p> |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.9.2.4              | Kalau misalkan mereka lupa <i>password</i> bagaimana itu pak? Di- <i>restore</i> juga?                                                                                                                                                                                                                                                                                                                      |
|                      | Ya, kita <i>restore</i> saja.                                                                                                                                                                                                                                                                                                                                                                               |
| A.18.1.2             | Apakah prosedur diterapkan untuk memastikan setiap komputer menggunakan lisensi perangkat lunak asli?                                                                                                                                                                                                                                                                                                       |
|                      | Kalau yang ada disini itu mestinya bagian yang mengecek itu bu Hanim. Karena perangkat lunak legal ada di bu Hanim. Termasuk juga kalau ada mahasiswa yang meminta Microsoft Office dan lain-lainnya itu di Subdit Pelayanan.                                                                                                                                                                               |
| A.18.1.3<br>A.18.1.4 | Apakah rekaman dan data pribadi dilindungi sesuai undang-undang, peraturan, dan persyaratan kontrak?                                                                                                                                                                                                                                                                                                        |
|                      | Kalau perlindungan rekaman dan data pribadi itu kebijakan yang kita ambil adalah sesuai dengan kebijakan organisasi. Jadi ketika mereka sudah mengisikan data untuk kita pakai, ya berarti kita pakai sesuai dengan kepentingan kita. Tapi apakah mengikuti undang-undang, nantinya iya. Rancangan undang-undang ITE sudah ada, klausul privasi itu. Cuma undang-undangnya masih di DPR, RUU-nya sudah ada. |
| A.18.1.5             | Apakah untuk penggunaan kontrol kriptografi sama ya pak?                                                                                                                                                                                                                                                                                                                                                    |
|                      | Ya.                                                                                                                                                                                                                                                                                                                                                                                                         |
| A.18.2.1             | Apakah pernah dilakukan audit keamanan informasi di organisasi secara independen dalam jangka waktu tertentu atau ketika perubahan signifikan terjadi?                                                                                                                                                                                                                                                      |
|                      | Pada periode saya tahun 2016 ini belum pernah dilakukan. Kalau sebelumnya saya tidak tahu.                                                                                                                                                                                                                                                                                                                  |

Narasumber : Ardi Purwono

Jabatan : Kasi Pemeliharaan Sarana dan Prasarana Lingkungan

Organisasi : Direktorat Sarana dan Prasarana

| No Annex | Pertanyaan & Jawaban                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.11.1.1 | Apakah pintu kebakaran yang ada didalam gedung Research Center ITS diawasi dan diuji <i>alarm</i> -nya?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|          | Kalau pengawasan dan pengujian seperti itu pasti kita lakukan sesuai dengan peraturan kan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| A.11.2.3 | Apakah kabel listrik dan jaringan dilindungi dari gangguan dan kerusakan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|          | Untuk kabel yang menyebrang selokan, tegangan kecil atau jaraknya pendek (contoh dari bangunan ke lampu taman) diberikan pipa pelindung supaya melindungi dari gigitan tikus dan kepiting sawah. Sedangkan untuk kabel yang tegangan besar (20 KV) biasanya dikasih pasir dulu, lalu dikasih beton selokan (U-Ditch). Jadi tujuannya kalau ada orang yang menggali pasti terhalang, tapi banyak kasus juga patoknya ada tapi tetap saja kena. Terakhir dikasih patok sebagai penanda kabel setiap beberapa meter, walaupun tidak ada dana ya dipakai batu bata merah. Kalau ada kerusakan terjadi, kontraktor dikenakan denda perbaikan secara kontrak. |
| A.11.2.3 | Apa penyebab terjadinya resiko kerusakan kabel?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|          | Sebenarnya pencegahannya sudah kuat sekali, tapi dikejadian 2 tahun terakhir ketika memperdalam selokan disisi barat gedung Research Center ITS dan pemasangan <i>paving block</i> jalan, ada orang kerja diluar jam yang diawasi (saat itu jam istirahat). Jadi waktu itu kejadian tapi tidak parah cuma ketekan, tapi itu rentan dan nanti bisa jadi masalah. Sebenarnya tidak masalah kalau ada pengawasan. Pernah kejadian juga dekat patok kebor. Loh kok mati pas dicari ternyata ada kabel kebor.                                                                                                                                                |
| A.11.2.3 | Siapa pengawas tersebut?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|          | Pengawasan itu dilakukan kontraktor, kita cuma mengarahkan misalnya daerah ini tidak aman. Jadi sama kontraktor dan konsultan di terjemahkan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| A.11.2.3 | Apakah kontraktor tersebut dikenakan denda?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|  |                                                                                                                                                                      |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | Ya, harus memperbaiki. Seperti di ITS Research Center ada kasus jalur FO kena dan harus memperbaiki. Sebenarnya kalau tidak ada pekerjaan seperti itu pastinya aman. |
|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Narasumber : Andi Rahmandiansah

Jabatan : Kasi Pengelolaan SDM

Organisasi : Direktorat SDM dan Organisasi

| No Annex | Pertanyaan & Jawaban                                                                                                                                                                                                                                               |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.12.1.3 | Apakah terdapat identifikasi kebutuhan kapasitas SDM minimum di DPTSI-ITS?                                                                                                                                                                                         |
|          | Kalau <i>workload</i> di DPTSI-ITS belum kami lakukan. Jadi kalau mau ditanya berapa kami belum tahu, sekarang saja masih menata. Untuk DPTSI-ITS kami baru meninjau proses bisnisnya apa dan struktur organisasinya bagaimana. Proses bisnisnya saja belum jelas. |
| A.12.1.3 | Misalkan DPTSI-ITS kekurangan karyawan, apakah secara kebijakan Direktorat SDM dan Organisasi mampu menambah karyawan?                                                                                                                                             |
|          | Ya, memang kami yang berwenang mengatur harus ditambah atau dikurangi itu dari Direktorat SDM dan Organisasi.                                                                                                                                                      |
| A.12.1.3 | Apakah ada dokumentasi perencanaan manajemen kapasitas SDM yang memudahkan dalam menyiapkan jumlah karyawan kedepan?                                                                                                                                               |
|          | Untuk hal itu masih belum kami lakukan. Kan mas sendiri sudah tahukan Direktorat SDM dan Organisasi dibentuknya tidak lama. Masih banyak PR yang belum kami selesaikan.                                                                                            |



Narasumber : Zakiyah Duratti

Jabatan : Staf Bagian Kepegawaian

Organisasi : Direktorat SDM dan Organisasi

| No Annex           | Pertanyaan & Jawaban                                                                                                                                                                                         |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.7.1.1            | Apakah verifikasi latar belakang pada semua calon karyawan dilakukan sesuai hukum/peraturan dan kebutuhan organisasi?                                                                                        |
|                    | Untuk penyaringan dilakukan pengecekan keaslian sertifikat atau ijazah, keaslian SKCK, tes kemampuan lewat wawancara dan tertulis. Untuk SKCK diminta yang asli untuk penetapan NIP CPNS.                    |
| A.7.1.1            | Apa nama dokumen kebijakannya? Dan bagaimana dengan yang non-PNS?                                                                                                                                            |
|                    | Bisa dilihat di aturan pengadaan PNS PP 11 tahun 2002, kalau yang non-PNS sedang dibuat dan isinya baru meng-copy dari peraturan PNS.                                                                        |
| A.7.1.2            | Apakah perjanjian kontrak dengan karyawan yang menyatakan tanggung jawab terhadap keamanan informasi?                                                                                                        |
|                    | Disini tidak ada penandatanganan kontrak tentang keamanan informasi. Yang ada sumpah PNS yang berisi janji karyawan untuk menjaga keamanan informasi. Bisa dilihat di PP 53 tahun 2010 tentang disiplin PNS. |
| A.7.2.3            | Apakah proses pendisiplinan dibuat secara formal dan dikomunikasikan untuk menindak karyawan yang melakukan pelanggaran keamanan informasi?                                                                  |
|                    | Ya, ada dan dijelaskan sanksinya di PP 53 tahun 2010 tadi.                                                                                                                                                   |
| A.7.2.3            | Bagaimana dengan tindakan kriminal seperti menyebar informasi rahasia, mencuri dan lainnya? Dan bagaimana dengan karyawan yang absensi?                                                                      |
|                    | Klasifikasi sanksi yang diberikan ada ringan, sedang dan berat. Coba dilihat lebih lengkap di PP 53 tahun 2010. Untuk absensi sama sanksinya, ada juga klasifikasi di PP tadi.                               |
| A.7.1.2<br>A.7.2.3 | Bagaimana dengan yang non-PNS untuk menjaga kerahasiaan informasi dan sanksi bagi yang melanggar?                                                                                                            |

|         |                                                                                                                                                                                          |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | Masih dalam bentuk <i>draft</i> dan belum disahkan. Umumnya sih hampir sama dengan yang PNS, seperti setiap karyawan non-PNS juga harus mengucapkan sumpah PNS dan lainnya.              |
| A.7.3.1 | Apakah tanggung jawab dan tugas-tugas masih berlaku setelah pemberhentian dan penggantian karyawan?                                                                                      |
|         | Kalau tanggung jawab setelah pemberhentian saya rasa tidak ada. Untuk kebijakan pemberhentian karyawan bisa dilihat di PP 32 tahun 1979. Pemberhentian PNS.                              |
| A.7.3.1 | Bagaimana dengan promosi atau mutasi ke unit lain bagi karyawan? Apa dilakukan <i>background check</i> ulang?                                                                            |
|         | Pastinya untuk karyawan yang mutasi kerja atau promosi jabatan dilakukan <i>background check</i> ulang. Aturan mutasi dan promosi bisa dilihat di PP 100 tahun 200 dan PP 13 tahun 2002. |
| A.7.3.1 | Apakah terdapat pemberitahuan ke DPTSI-ITS bahwa karyawan tertentu telah berhenti dan menyuruh agar akunnya seperti Integra dan lainnya dihapus?                                         |
|         | Ya, untuk setiap karyawan yang sudah berhenti pasti kami kirim surat pemberitahuan berikut <i>photocopy</i> SK pemberhentian kerjanya ke DPTSI-ITS.                                      |

*Halaman ini sengaja dikosongkan*

Tabel D.1 Klasifikasi Tingkat Kepatuhan

| Klasifikasi                | Kode      | Keterangan                                                                                                              |
|----------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------|
| <i>Compliant</i>           | <i>C</i>  | DPTSI-ITS patuh secara keseluruhan dengan area tertentu pada SNI ISO/IEC 27001.                                         |
| <i>Partially compliant</i> | <i>PC</i> | DPTSI-ITS telah melakukan berbagai cara untuk patuh, namun masih memerlukan pekerjaan tambahan yang harus dijalankan.   |
| <i>Non-compliant</i>       | <i>NC</i> | DPTSI-ITS tidak memiliki beberapa kontrol keamanan ditempat untuk memenuhi beberapa persyaratan dari SNI ISO/IEC 27001. |
| <i>Not applicable</i>      | <i>NA</i> | Telah ditinjau dan diidentifikasi bahwa kontrol keamanan tidak dapat diterapkan di DPTSI-ITS.                           |

Tabel D.2 Data Analisa Kesenjangan (Sebelum)

| No<br><i>Annex</i>                                               | Pertanyaan                                                                                                                                        | Tingkat<br>Kematangan      |
|------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <b>A.5. Kebijakan Keamanan Informasi</b>                         |                                                                                                                                                   |                            |
| <b>A.5.1. Arahan pihak manajemen terhadap keamanan informasi</b> |                                                                                                                                                   |                            |
| A.5.1.1                                                          | Kebijakan keamanan informasi                                                                                                                      | <i>Partially compliant</i> |
|                                                                  | Apakah kebijakan untuk keamanan informasi dibuat dan dikomunikasikan ke karyawan dan pemangku kepentingan yang terkait?                           |                            |
| <i>NC</i>                                                        | Kebijakan penggunaan perangkat <i>mobile</i> (A.6.2.1) belum didokumentasikan.                                                                    |                            |
| <i>NC</i>                                                        | Kebijakan penggunaan komputer/laptop (A.6.2.2) belum didokumentasikan.                                                                            |                            |
| <i>PC</i>                                                        | Kebijakan penggunaan <i>internet</i> , <i>intranet</i> , <i>email</i> dan media sosial (A.8.1.3) sebagian didokumentasikan (untuk <i>email</i> ). |                            |
| <i>NC</i>                                                        | Kebijakan klasifikasi informasi (A.8.2.1) belum didokumentasikan.                                                                                 |                            |
| <i>PC</i>                                                        | Kebijakan kontrol akses (A.9.1.1) belum didokumentasikan, masih dalam proses perencanaan pembuatan dan format <i>draft</i> .                      |                            |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NC | Kebijakan penggunaan enkripsi (A.10.1.1) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| NC | Kebijakan manajemen kunci enkripsi (A.10.1.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| NC | Kebijakan kontrol akses fisik (A.11.1.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| C  | Kebijakan bekerja di area yang aman (A.11.1.5) sudah didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                |
| NC | Kebijakan merapihkan meja dan membersihkan layar ( <i>clear desk and screen</i> ) (A.11.2.9) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                  |
| NC | Kebijakan manajemen perubahan (A.12.1.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                      |
| NC | Kebijakan pemindahan perangkat lunak (A.12.1.4) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                               |
| NC | Kebijakan penanganan <i>malware</i> (A.12.2.1) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                |
| NC | Kebijakan <i>backup</i> informasi (A.12.3.1) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| NC | Kebijakan pemasangan dan penghapusan perangkat lunak (A.12.5.1) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                               |
| NC | Kebijakan manajemen kerentanan teknis (A.12.6.1) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                              |
| NC | Kebijakan pembatasan penggunaan perangkat lunak (A.12.6.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                    |
| NC | Kebijakan pertukaran informasi (A.13.2.1) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                     |
| PC | Kebijakan pengembangan sistem informasi (A.14.2.1) belum didokumentasikan, masih dalam proses perencanaan pembuatan dan format <i>draft</i> .                                                                                                                                                                                                                                                                                                                                         |
| NC | Kebijakan penggunaan material yang mengandung hak kekayaan intelektual (A.18.1.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                             |
| C  | Untuk komunikasi kebijakan yang berlaku, DPTSI-ITS mengkomunikasikannya melalui rapat jika kebijakan bersifat internal, sedangkan untuk kebijakan yang berlaku untuk seluruh dosen, karyawan dan mahasiswa ITS dikomunikasikan melalui <i>website</i> <a href="https://dptsi.its.ac.id/?page_id=161">https://dptsi.its.ac.id/?page_id=161</a> dan <a href="https://dptsi.its.ac.id/?page_id=156">https://dptsi.its.ac.id/?page_id=156</a> yang dapat dilihat pada <b>Gambar F.1</b> . |

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                     |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| A.5.1.2                                  | Peninjauan kebijakan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Non-compliant       |
|                                          | Apakah kebijakan untuk keamanan informasi ditinjau dalam jangka waktu yang direncanakan atau jika terjadi perubahan dalam organisasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                     |
| NC                                       | DPTSI-ITS tidak memiliki perencanaan untuk memperbaharui kebijakan keamanan yang ada.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                     |
| A.6. Organisasi untuk Keamanan Informasi |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                     |
| A.6.1. Organisasi internal               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                     |
| A.6.1.1                                  | Peran dan tanggung jawab keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Partially compliant |
|                                          | Apakah semua tanggung jawab tentang keamanan informasi didefinisikan dan dialokasikan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                     |
| PC                                       | Untuk peran dan tanggung jawab dalam suatu aset atau informasi spesifik, DPTSI-ITS sudah menetapkan. Namun belum ada dokumentasinya secara jelas berdasarkan kontrol A.8.1.2. Kepemilikan aset.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                     |
| NC                                       | Untuk peran dan tanggung jawab dalam aktifitas manajemen resiko, DPTSI-ITS belum menetapkan karena belum menggunakannya berdasarkan kontrol A.6.1.5. Manajemen proyek untuk keamanan informasi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                     |
| PC                                       | <p>Untuk peran dan tanggung jawab dalam aktifitas keamanan informasi, DPTSI-ITS menetapkan Subdit Infastruktur dalam perumusan kebijakan, pengembangan, pengawasan, pemeliharaan, peninjauan dan pelaporan infrastruktur dan keamanan TIK berdasarkan Peraturan Rektor ITS nomor 10 tahun 2016 tentang ITS. Peraturan Rektor ITS dapat dilihat pada <b>Gambar F.2</b> dan <b>Gambar F.3</b>. Tanggung jawab yang dimiliki Kasubdit didalam dokumen Uraian Tugas adalah:</p> <ul style="list-style-type: none"> <li>• Menyusun rencana program kerja dan mempersiapkan pelaksanaan program kerja DPTSI-ITS.</li> <li>• Menentukan kebijakan internal atau eksternal DPTSI-ITS.</li> <li>• Menentukan/memilih penanggung jawab operasional dalam suatu kegiatan.</li> <li>• Menentukan arah perkembangan dibidang TIK dan jaringan ITS.</li> </ul> |                     |

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <p>PC<br/>(lanj.)</p> | <ul style="list-style-type: none"> <li>• Menerima tugas lain dan memberikan laporan pertanggung jawaban ke Rektor ITS.</li> </ul> <p>Sedangkan tanggung jawab Subdit Infrastruktur (dalam hal ini administrasi jaringan) adalah:</p> <ul style="list-style-type: none"> <li>• Merawat jaringan <i>backbone</i> ITS.</li> <li>• Mengembangkan desain, <i>administrator</i> dan aplikasi jaringan.</li> <li>• Mengembangkan dan merawat jaringan <i>INHERENT</i>.</li> <li>• Membuat modul pelatihan <i>administrator</i> jaringan komputer.</li> <li>• Mengkonfigurasi dan merawat perangkat keras dan perangkat jaringan.</li> <li>• Pemeliharaan <i>website</i> ITS (<a href="https://its.ac.id">https://its.ac.id</a>).</li> </ul> <p>Namun untuk peran dan tanggung jawab dalam aktifitas keamanan informasi secara spesifik, DPTSI-ITS belum menetapkan karena belum mengadopsi standar keamanan tertentu berdasarkan kontrol A.18.2.1. Peninjauan keamanan informasi secara independen.</p>                                                                                                                                          |                                   |
| <p>A.6.1.2</p>        | <p>Pembagian tugas</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <p><i>Partially compliant</i></p> |
| <p>PC</p>             | <p>Apakah beberapa tugas dan area tanggung jawab yang berlawanan dipisahkan untuk mengurangi peluang perubahan dan penyalahgunaan tanpa izin atau tidak disengaja pada aset?</p> <p>DPTSI-ITS memisahkan tugas dan area tanggung jawab kedalam tiga bagian, yaitu infrastruktur jaringan dan keamanannya dilakukan oleh Subdit Infrastruktur, pengembangan sistem informasi terpadu dan pemeliharannya dilakukan oleh Subdit Pengembangan, dan pelayanan dan pelaporan TIK dilakukan oleh Subdit Pelayanan. Dibawah Subdit Pelayanan ada Kasi Layanan Data dan Informasi, dan dibawah Subdit Pengembangan ada Kasi Pengembangan Aplikasi pada Perangkat Bergerak. Masing-masing Subdit dikepalai oleh Kasubdit. Selain itu terdapat tugas dan area tanggung jawab lainnya, seperti Direktur DPTSI-ITS sebagai pimpinan organisasi yang menyusun program kerja dan pengarahannya, sekretaris sebagai pembantu Direktur DPTSI-ITS dalam melaksanakan program kerja, Bendahara Pengeluaran Pembantu sebagai pengelola keuangan organisasi, dan Pembantu Administrasi Umum sebagai pelaksana kebersihan dan membantu tugas-tugas lainnya.</p> |                                   |

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                   |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <p>PC<br/>(lanj.)</p> | <p>Selain yang disebutkan diatas, terdapat pembagian tugas dan area tanggung jawab lainnya seperti:</p> <ul style="list-style-type: none"> <li>• Subdit Infrastruktur memiliki administrasi jaringan, administrasi sistem, administrasi kelistrikan, dan penyusun laporan dan pengelola BMN.</li> <li>• Subdit Pengembangan memiliki analis sistem (sekaligus <i>desainer</i> sistem), <i>programmer</i> (sekaligus <i>administrator database</i>), dokumentator dan penguji sistem.</li> </ul> <p>DPTSI-ITS mendokumentasikan pembagian dan penjelasan tugas apa saja yang harus dilakukan oleh setiap fungsi kerja atau jabatan yang ada berikut standar kompetensi/keahlian yang harus dimiliki untuk melaksanakan tugasnya. Namun terdapat tugas dan area tanggung jawab yang tidak terdokumentasikan didalam dokumen Uraian Tugas, seperti pada Subdit Infrastruktur hanya dijelaskan Kasubdit dan administrasi jaringan saja. Dokumen ini memiliki nama Uraian Tugas yang dapat dilihat pada <b>Gambar F.4</b> dan <b>Gambar F.5</b>.</p>                                                                                                                      |                                   |
| <p>A.6.1.3</p>        | <p>Menghubungi organisasi/pemerintahan</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <p><i>Partially compliant</i></p> |
|                       | <p>Apakah hubungan/kontak yang tepat dengan organisasi/pemerintahan terkait dikelola?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                   |
| <p>C</p>              | <p>Berikut ini adalah hubungan/kontak yang dilakukan oleh DPTSI-ITS:</p> <ul style="list-style-type: none"> <li>• Untuk hubungan dengan organisasi lain diluar lingkungan ITS, DPTSI-ITS menjalin hubungan dengan pemadam kebakaran untuk insiden kebakaran, <i>ISP</i> untuk masalah gangguan jaringan komunikasi, PLN untuk kesalahan arus saat pengecekan arus dan tegangan listrik, atau vendor perangkat untuk masalah pada perangkat tersebut.</li> <li>• Untuk hubungan dengan unit kerja lain didalam lingkungan ITS, DPTSI-ITS menjalin hubungan dengan Direktorat SDM dan Organisasi untuk masalah perekrutan, pemberian sanksi dan pemberhentian karyawan, Unit Layanan Pengadaan (ULP-ITS) untuk masalah pengadaan barang/layanan dan penilaian vendor, Direktorat Sarana dan Prasarana (DSP-ITS) untuk masalah <i>AC</i>, <i>hydrant</i>, PDAM, listrik dan lainnya, Bagian Administrasi Umum Keuangan (BAUK-ITS) untuk masalah pengelolaan keuangan dan barang milik negara, Direktorat Hukum Organisasi dan Tata Laksana (Hukortala-ITS) untuk masalah penanganan dan penyelesaian permasalahan hukum didalam lingkungan ITS, dan lainnya.</li> </ul> |                                   |



|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| NC      | DPTSI-ITS tidak memiliki dokumentasi kontak dukungan dan eskalasi yang berisikan spesifikasi kapan dan siapa yang akan dihubungi (karyawan/ Kasubdit, vendor, pemerintahan, atau unit lain di ITS) jika terjadi masalah teknis dan operasional.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
| A.6.1.4 | Menghubungi kelompok dengan minat tertentu                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <i>Non-compliant</i>       |
|         | Apakah hubungan dengan kelompok dengan minat tertentu atau forum keamanan dikelola dengan tepat?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
| NC      | Beberapa karyawan mengunjungi <i>forum</i> atau <i>website</i> tentang komputer atau keamanan informasi seperti How-To Geek, CHIP <i>online</i> atau lainnya untuk mendapatkan ilmu dan mengatasi masalah yang dihadapi. Namun DPTSI-ITS tidak mengelola <i>forum</i> apa saja yang diikuti karyawan dan mengatur bagaimana tata cara bertukar informasi kepada orang-orang yang ada di <i>forum</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                            |
| A.6.1.5 | Manajemen proyek untuk keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <i>Partially compliant</i> |
|         | Apakah keamanan informasi dirujuk kedalam manajemen proyek tanpa menghiraukan tipe dari proyek?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
| C       | <p>Untuk memasukkan sasaran keamanan informasi kedalam sasaran proyek, DPTSI-ITS selalu merujuk isu keamanan informasi kedalam setiap proyek yang dikerjakan baik dalam pengembangan sistem informasi terpadu, pemasangan/perluasan infrastruktur jaringan, dan lainnya. Berikut ini adalah contoh sasaran keamanan informasi kedalam beberapa aktifitas manajemen proyek:</p> <ul style="list-style-type: none"> <li>• Proyek pemindahan lokasi kantor DPTSI-ITS yang sebelumnya berada di gedung DiLo dan UPT Perpustakaan dilantai 6 ke gedung ITS Research Center dilantai 3. Pemasangan kabel listrik dan jaringan yang dilakukan di gedung sebelumnya tidak dipisahkan, sedangkan di gedung baru sudah dipisahkan. Hal ini dilakukan agar melindungi interferensi elektronik ataupun kerusakan pada data yang ditransmisikan melalui kabel.</li> <li>• Proyek pemasangan <i>server</i> baru dilakukan pembahasan konfigurasi keamanannya, seperti penempatan pada <i>subnet</i> tertentu dan penetapan <i>rule</i>/aturan baru menggunakan <i>firewall</i> untuk <i>port</i> yang boleh lewat didalam infrastruktur jaringan di ITS. Hal ini dilakukan agar perangkat dan jaringan beroperasi secara stabil dan aman.</li> </ul> |                            |

|                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C<br>(lanj.)                                          | <ul style="list-style-type: none"> <li>• Proyek pengembangan sistem informasi baru dilakukan pembahasan masalah keamanan pada sistem seperti pengelolaan manajemen hak akses pengguna, kerahasiaan data, proses <i>backup</i>, pengujian sistem yang akan dilakukan, konfigurasi keamanan sistem (contohnya pemasangan <i>CAPTCHA</i>), atau rujukan lainnya. Hal ini dilakukan agar sistem informasi yang dibangun aman dari proses <i>hacking</i> dan melindungi keamanan data didalamnya.</li> </ul> <p>DPTSI-ITS merencanakan kedepan apa yang harus diterapkan dari tahun ke tahun yang didokumentasikan kedalam Tahapan Implementasi <i>Masterplan</i> 2013-2017. Isi dari rencana ini mencakup organisasi dan SDM, tata kelola TIK, bangunan dan ruang, pusat data, infrastruktur jaringan, <i>database</i> terpadu, sistem informasi, aplikasi layanan, <i>service desk</i>, dan eksternalisasi produk dan layanan TIK. Berdasarkan perencanaan tersebut, DPTSI-ITS berencana mempersiapkan penggunaan standar SNI ISO/IEC 27001 di tahun 2016 dan melakukan sertifikasi oleh badan sertifikasi di tahun 2017. <i>Masterplan</i> dapat dilihat pada <b>Gambar F.6</b>.</p> |
| PC                                                    | <p>Untuk penilaian dan penanganan resiko, DPTSI-ITS belum menerapkan proses manajemen resiko ataupun penggunaan kerangka kerja apapun untuk mengevaluasi resiko dan keefektifan penerapan kontrol keamanannya. Namun beberapa hal terkait pengelolaan resiko yang dilakukan DPTSI-ITS:</p> <ul style="list-style-type: none"> <li>• Mengidentifikasi ancaman dan kerentanan pada aset informasi, namun aktifitas ini belum terdokumentasi.</li> <li>• Menerapkan kontrol keamanan bukan berdasarkan resiko yang sudah dinilai dan diprioritaskan tapi berdasarkan kebutuhan untuk menangani resiko.</li> <li>• Setiap penanganan resiko yang diterapkan dibahas melalui <i>chat</i> dan tidak dilakukan evaluasi ulang untuk mengukur keefektifannya karena sudah ada keyakinan bahwa penanganan sudah baik.</li> </ul>                                                                                                                                                                                                                                                                                                                                                            |
| C                                                     | <p>Untuk peran dan tanggung jawab keamanan informasi dalam proyek, DPTSI-ITS menetapkannya pada setiap proyek. Misalnya proyek pemasangan <i>server</i> baru dimana tanggung jawab untuk pemasangan dan konfigurasi yang aman pada <i>server</i> dilakukan oleh karyawan dari administrasi jaringan dan sistem, keamanan perangkat kelistrikan dilakukan oleh administrasi kelistrikan, dan ketua proyek yang mengelola proyek dilakukan oleh Kasubdit Infrastruktur.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| A.6.2. Perangkat <i>mobile</i> dan <i>teleworking</i> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.6.2.1                            | Kebijakan perangkat <i>mobile</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <i>Non-compliant</i>       |
|                                    | Apakah kebijakan dan kontrol keamanan pendukung dipakai untuk mengelola resiko perangkat <i>mobile</i> ?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |
| NC                                 | DPTSI-ITS tidak memiliki dokumentasi kebijakan baik tertulis maupun tidak tertulis yang mengatur penggunaan perangkat <i>mobile</i> yang dimiliki karyawan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                            |
| A.6.2.2                            | <i>Teleworking</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <i>Non-compliant</i>       |
|                                    | Apakah kebijakan dan kontrol keamanan pendukung diterapkan untuk melindungi informasi yang diakses, diproses atau disimpan pada area <i>teleworking</i> ?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
| NC                                 | DPTSI-ITS tidak memiliki dokumentasi kebijakan baik tertulis maupun tidak tertulis yang mengatur penggunaan laptop/komputer yang dimiliki karyawan ataupun laptop dinas.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |
| A.7. Keamanan Sumber Daya Manusia  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |
| A.7.1. Sebelum perekrutan karyawan |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |
| A.7.1.1                            | Penyaringan karyawan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <i>Partially compliant</i> |
|                                    | Apakah verifikasi latar belakang pada semua calon karyawan dilakukan sesuai hukum/peraturan dan kebutuhan organisasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                            |
| PC                                 | DPTSI-ITS tidak melakukan pelaksanaan penambahan karyawan baru berikut aktifitas <i>background check</i> -nya. Semua aktifitas yang berkaitan dengan pengadaan, pemberian sanksi dan pemberhentian karyawan baik untuk karyawan PNS ataupun karyawan non-PNS/kontrak dilakukan oleh Direktorat SDM dan Organisasi. DPTSI-ITS hanya memberikan informasi ke Direktorat SDM dan Organisasi jika diperlukan penambahan karyawan baru atau terdapat karyawan yang berhenti. <i>Background check</i> yang dilakukan adalah sebelum penerimaan karyawan, mutasi ke unit/direktorat lain dan promosi jabatan. Berdasarkan Peraturan Pemerintah nomor 11 tahun 2002 tentang aturan pengadaan karyawan PNS (Pegawai Negeri Sipil), berikut ini adalah sebagian persyaratan untuk karyawan PNS baru: |                            |

|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                   |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <p>PC<br/>(lanj.)</p> | <ul style="list-style-type: none"> <li>• Tidak pernah dihukum penjara atau kurungan berdasarkan putusan pengadilan.</li> <li>• Tidak pernah diberhentikan dengan hormat baik sebagai karyawan PNS atau swasta.</li> <li>• Mempunyai pendidikan, kecakapan, keahlian dan keterampilan yang diperlukan.</li> </ul> <p>Jika mengacu hal-hal diatas, Direktorat SDM dan Organisasi melakukan pengecekan keaslian sertifikat dan ijazah, penelusuran riwayat pekerjaan karyawan, penyerahan SKCK (surat dari kepolisian) asli, dan surat keterangan tidak mengkonsumsi/menggunakan narkoba, psikotropika, prekursor dan zat adiktif lainnya dari unit pelayanan kesehatan pemerintah. Selain itu diperlukan juga menilai kemampuan karyawan melalui wawancara dan tes tertulis. PP 11 tahun 2002 dapat dilihat pada <b>Gambar F.7</b> dan <b>Gambar F.8</b>. Namun untuk karyawan non-PNS, Direktorat SDM dan Organisasi sudah memiliki kebijakan/aturan tertulis namun masih dalam bentuk <i>draft</i> dan isinya mengikuti sebagian besar peraturan untuk pengadaan karyawan PNS.</p> <p>DPTSI-ITS memiliki dokumen yang bernama Kompetisi Sumber Daya yang berfungsi untuk menjelaskan apa saja persyaratan pekerjaan (<i>job requirement</i>) yang harus dimiliki oleh karyawan di DPTSI-ITS dan dapat membantu dalam penyaringan karyawan baru yang tepat. Dokumen ini berisikan persyaratan minimal jenjang pendidikan, bidang keahlian/keilmuan, minimal pengalaman kerja, kemampuan pengelolaan TIK (contoh menguasai administrasi umum, atau mampu koordinasi dengan tim), dan pelatihan yang diperlukan (contohnya sertifikasi CISCO, atau sistem <i>database</i>). Kompetensi SDM dapat dilihat pada <b>Gambar F.9</b> sampai <b>Gambar F.12</b>.</p> |                                   |
| <p>A.7.1.2</p>        | <p>Syarat dan ketentuan dalam pekerjaan</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <p><i>Partially compliant</i></p> |
|                       | <p>Apakah perjanjian kontrak dengan karyawan menyatakan tanggung jawab terhadap keamanan informasi?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                   |

|                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>PC</i>                             | Untuk perjanjian kerahasiaan informasi, setiap karyawan PNS diharuskan mengucapkan sumpah/janji karyawan PNS dan Subdit Pengembangan diharuskan menandatangani perjanjian kerahasiaan sebelum diberikan akses kedalam sistem informasi yang akan dikelola berdasarkan kontrol A.13.2.4. Perjanjian kerahasiaan atau tidak menyebarkan informasi. Namun hal tersebut tidak melingkupi untuk semua karyawan.                                                                                                                                                                                                          |
| <i>NC</i>                             | Untuk tanggung jawab dalam penjagaan hak kekayaan intelektual, DPTSI-ITS masih belum mengaturnya secara benar berdasarkan kontrol A.18.1.2. Hak kekayaan intelektual dan kontrol A.18.1.4. Kerahasiaan dan perlindungan untuk informasi pribadi.                                                                                                                                                                                                                                                                                                                                                                    |
| <i>NC</i>                             | Untuk tanggung jawab dalam klasifikasi informasi, DPTSI-ITS masih belum mendokumentasikan klasifikasi informasi untuk aset yang ada di DPTSI-ITS berdasarkan kontrol A.8.2.1. Klasifikasi informasi.                                                                                                                                                                                                                                                                                                                                                                                                                |
| <i>C</i>                              | Untuk tindakan jika terjadi pelanggaran terhadap keamanan informasi, DPTSI-ITS memiliki beberapa sanksi yang akan diberikan jika karyawan melanggar peraturan ataupun perjanjian yang sudah diterapkan berdasarkan kontrol A.7.2.3. Proses pendisiplinan.                                                                                                                                                                                                                                                                                                                                                           |
| <i>C</i>                              | Untuk pengarahan peran dan tanggung jawab sebelum penempatan kerja, Direktur DPTSI-ITS memberikan penjelasan terlebih dahulu kepada karyawan baru tentang peran dan tanggung jawab yang akan diemban. Setelah itu karyawan akan diserahkan ke Subdit tempat mereka nanti bekerja, dan kepala Subdit akan menjelaskan lagi secara rinci peran dan tanggung jawab karyawan tersebut. Selain itu DPTSI-ITS memiliki dokumen ISO 9000 yang berisi kumpulan prosedur dan kegiatan yang ada di organisasi, jadi setiap karyawan baru yang masuk diharuskan membaca prosedur-prosedur yang ada sesuai dengan pekerjaannya. |
| <i>NC</i>                             | Untuk tanggung jawab setelah pemberhentian kerja, DPTSI-ITS tidak mendefinisikan tanggung jawab karyawan yang pindah/keluar kerja terhadap keamanan informasi berdasarkan kontrol A.7.3.1. Tanggung jawab pemberhentian dan penggantian karyawan.                                                                                                                                                                                                                                                                                                                                                                   |
| <i>NC</i>                             | Untuk panduan tingkah laku yang berisikan ekspektasi keamanan informasi bagi karyawan didalam organisasi, DPTSI-ITS tidak memilikinya berdasarkan kontrol A.7.2.1. Tanggung jawab manajemen.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>A.7.2. Selama karyawan bekerja</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.7.2.1   | Tanggung jawab manajemen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <i>Partially compliant</i> |
|           | Apakah pihak manajemen mengharuskan semua karyawan dan kontraktor menjalankan keamanan informasi berkenaan dengan kebijakan dan prosedur yang ditetapkan?                                                                                                                                                                                                                                                                                                                                                                                                                             |                            |
| <i>PC</i> | Untuk pengarahan sebelum diberikan akses ke sistem informasi sesuai dengan peran dan tanggung jawab dalam keamanan informasi, DPTSI-ITS tidak mengarahkan secara khusus apa yang harus dilakukan untuk menjaga keamanan informasi. Selain itu untuk Subdit Pengembangan diharuskan menandatangani perjanjian kerahasiaan yang berisikan apa saja tindakan keamanan yang harus dilakukan terhadap informasi organisasi yang diberikan berdasarkan kontrol A.13.2.4. Perjanjian kerahasiaan atau tidak menyebarkan informasi. Namun hal tersebut tidak melingkupi untuk semua karyawan. |                            |
| <i>NC</i> | DPTSI-ITS tidak mendokumentasikan panduan tingkah laku yang berisikan ekspektasi keamanan informasi bagi karyawan didalam organisasi, seperti menyangkut kerahasiaan, perlindungan data, etika, penggunaan yang tepat peralatan dan fasilitas dan lainnya.                                                                                                                                                                                                                                                                                                                            |                            |
| <i>C</i>  | Untuk memastikan tingkat kesadaran akan keamanan informasi, DPTSI-ITS mengadakan program kesadaran keamanan bagi karyawan sesuai dengan peran merka berdasarkan kontrol A.7.2.2. Kesadaran, pendidikan dan pelatihan keamanan informasi.                                                                                                                                                                                                                                                                                                                                              |                            |
| <i>NC</i> | Untuk memastikan kepatuhan karyawan terhadap kebijakan dan prosedur di organisasi, DPTSI-ITS masih belum melakukannya berdasarkan kontrol A.18.2.2. Kepatuhan terhadap kebijakan dan standar keamanan.                                                                                                                                                                                                                                                                                                                                                                                |                            |
| <i>C</i>  | Untuk memastikan peningkatan kemampuan dan kualifikasi pada karyawan, DPTSI-ITS melaksanakan pelatihan kerja bagi karyawan berdasarkan kontrol A.7.2.2. Kesadaran, pendidikan dan pelatihan keamanan informasi.                                                                                                                                                                                                                                                                                                                                                                       |                            |
| <i>PC</i> | Untuk memastikan pelaporan pelanggaran dari karyawan, DPTSI-ITS tidak menyediakan sistem pelaporan secara <i>anonym</i> untuk pelaporan pelanggaran yang dilakukan karyawan. Namun proses pelaporan yang dilakukan jika terdapat karyawan yang melanggar kebijakan, prosedur, etika dan lainnya adalah pelaporan langsung yang bersifat bertingkat. Hal ini dilakukan dengan cara memberitahukan ke atasan langsungnya, nanti atasan tersebut yang akan                                                                                                                               |                            |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                            |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| PC<br>(lanj.) | <p>menyelesaikan. Jika tidak bisa diselesaikan oleh atasan langsungnya, maka atasan tersebut melaporkan ke atasannya lagi. Sedangkan apabila yang melanggar adalah atasan langsungnya bisa melapor ke atasan di atasnya lagi. Jika tidak bisa diselesaikan sampai ke Rektor, nanti akan diserahkan ke Hukortala-ITS selama pelanggaran bukan yang mengarah ke tindak hukum. Jika pelanggaran mengarah ke tindak hukum maka akan dilaporkan ke polisi.</p>                                                                                                                                                                                                                                                                           |                            |
| NC            | <p>Untuk dukungan dari pihak manajemen terhadap kebijakan, prosedur dan kontrol keamanan informasi, DPTSI-ITS masih belum melakukannya secara penuh berdasarkan kontrol A.5.1.1. Kebijakan keamanan informasi dan kontrol A.5.1.2. Peninjauan kebijakan keamanan informasi.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                            |
| A.7.2.2       | Kesadaran, pendidikan dan pelatihan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <i>Partially compliant</i> |
|               | <p>Apakah semua karyawan dan kontraktor menerima program kesadaran keamanan dan pelatihan, serta pembaharuan berkala pada kebijakan dan prosedur yang terkait pekerjaannya?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                            |
| PC            | <p>Untuk program kesadaran keamanan, DPTSI-ITS mengadakan program bagi karyawan, dosen, mahasiswa dan pemangku kepentingan lainnya melalui tiga cara, yaitu pemasangan poster di beberapa tempat mading di lingkungan ITS, melakukan <i>posting</i> ke <i>website</i> DPTSI-ITS, atau acara seminar. Program kesadaran keamanan yang pernah diadakan dapat dilihat pada <b>Gambar F.13</b> dan <b>Gambar F.14</b>. Namun DPTSI-ITS tidak membuat matriks untuk program kesadaran keamanan yang berisikan perencanaan pelatihan tentang keamanan informasi bagi seluruh pemangku kepentingan di dalam ruang lingkup SMKI. Selain itu program kesadaran keamanan tidak langsung dilaksanakan bagi karyawan/mahasiswa magang baru.</p> |                            |
| C             | <p>Berikut ini adalah pelatihan kerja yang diadakan oleh DPTSI-ITS:</p> <ul style="list-style-type: none"> <li>• Untuk sosialisasi pelatihan sistem, DPTSI-ITS melakukan sosialisasi pelatihan sistem untuk sistem informasi atau layanan TIK yang digunakan di dalam lingkungan ITS kepada pemangku kepentingan terkait. Hasil aktifitas sosialisasi pelatihan sistem biasanya didokumentasikan di <i>website</i> DPTSI-ITS. Sosialisasi pelatihan sistem yang pernah diadakan dapat dilihat pada <b>Gambar F.15</b> dan <b>Gambar F.16</b>.</li> <li>• Untuk pelatihan dan sertifikasi kerja, DPTSI-ITS memberikan pelatihan kerja kepada karyawan dan mendokumentasikan perencanaan pelatihan</li> </ul>                         |                            |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                  |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| C<br>(lanj.) | <p>kerja yang akan diberikan kedalam format matriks. Isi dari matriks tersebut adalah nama karyawan, pelatihan yang akan diberikan (contoh audit ISO, atau sertifikasi CISCO), dan jadwal pelatihannya. Nama dokumen tersebut adalah Matriks Kebutuhan Pelatihan SDM. Contoh pelatihan kerja yang pernah diadakan sebelumnya di tahun 2016 adalah pelatihan tentang <i>honeypot</i> yang diadakan oleh KEMENKOMINFO bagi beberapa Subdit Infrastruktur dan pelatihan kerangka kerja Laravel untuk bahasa pemrograman <i>PHP</i> bagi beberapa Subdit Pengembangan. Matriks Kebutuhan Pelatihan SDM dapat dilihat pada <b>Gambar F.17</b>.</p>                                                                                                                                                                                                                                            |                  |
| PC           | <p>Untuk menilai penyerapan ilmu pada pelatihan atau program yang dilakukan ke karyawan, DPTSI-ITS melakukan pengujian untuk pelatihan kerja, seperti terdapat daftar pertanyaan sebelum dilakukan pelatihan dan setelahnya untuk dapat memperkirakan seberapa besar ilmu yang diserap. Selain itu juga pengadaan pelatihan kerja umumnya dilakukan berdasarkan kebutuhan dalam penanganan masalah atau melakukan aktifitas tertentu. Contohnya Subdit Pengembangan mulai menggunakan <i>framework</i> Laravel dan memerlukan pelatihan kerja penggunaan <i>framework</i>. Jadi penilaian dapat dilakukan dengan melihat apakah karyawan tersebut mampu menggunakan <i>framework</i> setelah dilakukan pelatihan. Namun DPTSI-ITS tidak melakukan pengujian tingkat kesadaran terhadap keamanan informasi yang dilakukan ke pemangku kepentingan.</p>                                    |                  |
| A.7.2.3      | Proses pendisiplinan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <i>Compliant</i> |
|              | <p>Apakah proses pendisiplinan dibuat secara formal dan dikomunikasikan untuk menindak karyawan yang melakukan pelanggaran keamanan informasi?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                  |
| C            | <ul style="list-style-type: none"> <li>Berdasarkan Peraturan Pemerintah nomor 53 tahun 2010 tentang disiplin karyawan PNS, karyawan diharuskan memegang rahasia jabatan yang menurut sifatnya atau menurut perintah harus dirahasiakan, melaporkan dengan segera kepada atasannya jika mengetahui hal yang dapat membahayakan atau, menaati ketentuan jam kerja, tidak memanfaatkan BMN untuk kepentingan pribadi secara tidak sah, dan tidak melakukan kegiatan bersama dilingkungan kerja untuk kepentingan pribadi yang merugikan negara. Hukuman untuk karyawan dibagi ketiga bagian yaitu hukuman disiplin ringan, sedang dan berat. Yang membedakan umumnya apakah kerugian dari pelanggaran yang dilakukan karyawan merugikan unit kerja, instansi atau pemerintah, sedangkan untuk pelanggaran tidak menaati waktu kerja yang membedakan adalah banyaknya jumlah hari</li> </ul> |                  |



|                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                       |                      |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|----------------------|
| <p>C<br/>(lanj.)</p>                                        | <p>karyawan tidak masuk kerja. Jenis hukuman disiplin ringan terdiri dari teguran lisan, teguran tertulis dan pernyataan tidak puas secara tertulis. Untuk jenis hukuman disiplin sedang terdiri dari penundaan kenaikan gaji berkala selama satu tahun, penundaan kenaikan pangkat selama satu tahun dan penurunan pangkat setingkat lebih rendah selama satu tahun. Untuk jenis hukuman disiplin berat terdiri dari penurunan pangkat setingkat lebih rendah selama tiga tahun, pemindahan dalam rangka penurunan jabatan setingkat lebih rendah, pembebasan dari jabatan, pemberhentian dengan hormat tidak atas permintaan sendiri sebagai karyawan, dan pemberhentian tidak dengan hormat sebagai karyawan. PP 53/10 dapat dilihat pada <b>Gambar F.18</b> sampai <b>Gambar F.23</b>.</p> <ul style="list-style-type: none"> <li>• Berdasarkan ketentuan penggunaan <i>email</i> di <i>website</i> <a href="https://webmail.its.ac.id/src/login.php?bag=ketentuan">https://webmail.its.ac.id/src/login.php?bag=ketentuan</a>, DPTSI-ITS berhak untuk menghapus keanggotaan <i>email</i> ITS yang dimiliki pengguna apabila pengguna tidak mematuhi ketentuan penggunaan <i>email</i>. Ketentuan tersebut seperti apabila pengguna dengan sengaja mengirim <i>spam</i>, menjual akun <i>email</i>, atau mengirim pesan berbaur sara, pornografi, ancaman, <i>virus/malware</i>. Ketentuan penggunaan <i>email</i> dapat dilihat pada <b>Gambar F.24</b></li> <li>• Berdasarkan kontrol A.13.2.4. Perjanjian kerahasiaan atau tidak menyebarkan informasi, terdapat perjanjian menjaga kerahasiaan untuk Subdit Pengembangan. Menurut perjanjian tersebut DPTSI-ITS akan memberikan sanksi sesuai peraturan yang berlaku di ITS dan sanksi lain sesuai undang-undang ITE yang berlaku jika isi dari perjanjian dilanggar Perjanjian menjaga kerahasiaan untuk Subdit Pengembangan dapat dilihat pada <b>Gambar F.137</b>.</li> </ul> <p>ITS memiliki Direktorat Hukum Organisasi dan Tata Laksana (Hukortala-ITS) yang melaksanakan penanganan dan penyelesaian berbagai permasalahan/pelanggaran etika dan hukum yang terjadi didalam lingkungan ITS. Untuk penanganan yang terkait hukum yang berlaku di ITS bukanlah kewenangan milik DPTSI-ITS. Ditahun 2007 pernah terjadi pelanggaran keamanan informasi yang dilakukan oleh mahasiswa, dan sanksi yang diberikan adalah skors. Jadi DPTSI-ITS hanya menyerahkan mahasiswa tersebut ke Hukortala-ITS, lalu proses penanganan dan pemberian sanksinya dilakukan oleh Hukortala-ITS.</p> |                                                       |                      |
| <p><b>A.7.3. Pemberhentian dan penggantian karyawan</b></p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                       |                      |
| <p>A.7.3.1</p>                                              | <table border="1"> <tr> <td>Tanggung jawab pemberhentian dan penggantian karyawan</td> <td><i>Non-compliant</i></td> </tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Tanggung jawab pemberhentian dan penggantian karyawan | <i>Non-compliant</i> |
| Tanggung jawab pemberhentian dan penggantian karyawan       | <i>Non-compliant</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                       |                      |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                     |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                                     | Apakah tanggung jawab dan tugas-tugas masih berlaku setelah pemberhentian dan penggantian karyawan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                     |
| NC                                  | Berdasarkan Peraturan Pemerintah nomor 32 tahun 1979 dan nomor 65 tahun 2008 tentang pemberhentian karyawan PNS, yang dibahas adalah masalah batas pensiun, perpanjangan pensiun, hal-hal yang menyebabkan pemberhentian (contoh melanggar sumpah/janji karyawan PNS, dihukum penjara, atau sakit yang susah disembuhkan). Tidak dijelaskan tanggung jawab karyawan setelah diberhentikan, contohnya perjanjian ataupun pemberitahuan ulang kepada karyawan bahwa informasi/rahasia organisasi harus dijaga meski karyawan sudah keluar. PP 32/79 dan PP 65/08 dapat dilihat pada <b>Gambar F.25</b> sampai <b>Gambar F.28</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                     |
| A.8. Manajemen Aset                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                     |
| A.8.1. Tanggung jawab terhadap aset |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                     |
| A.8.1.1                             | Inventaris aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Partially compliant |
|                                     | Apakah aset yang berhubungan dengan informasi dan fasilitas pendukungnya diidentifikasi dan daftar inventarisnya didokumentasikan dan dikelola?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                     |
| PC                                  | <ul style="list-style-type: none"> <li>Aset Barang Milik Negara (BMN) didokumentasikan kedalam sistem E-Aset dan <i>file</i> Daftar Inventaris Aset oleh karyawan penyusun laporan dan pengelola BMN dibawah Subdit Infrastruktur. Yang termasuk BMN adalah perangkat keras (komputer, <i>server</i>, <i>printer</i>, komponennya, dan lainnya), perangkat jaringan (<i>router</i>, <i>firewall</i>, <i>switch</i> dan lainnya), perangkat lunak (pengolah gambar, kantor dan lainnya), perangkat perlengkapan (<i>AC</i>, <i>UPS</i>, <i>diesel generator</i>, dan lainnya), dan furnitur (kursi, meja, lemari dan lainnya). Dokumen ini berisikan kode barang, nama barang, merek/tipe, jumlah barang, lokasi barang dan kondisi barang. Daftar Inventaris Aset dapat dilihat pada <b>Gambar F.29</b> dan Daftar Inventaris Ruangan dapat dilihat pada <b>Gambar F.30</b>.</li> <li>Aset SIM didokumentasikan kedalam <i>file</i> Daftar Inventaris SIM oleh Subdit Pengembang. Yang didokumentasikan adalah semua sistem informasi yang dikembangkan di DPTSI-ITS, sedangkan yang dikembangkan masing-masing oleh unit atau jurusan tidak termasuk. Dokumen ini berisikan nama SIM, modul dan fitur yang dimiliki, <i>log</i> aktifitas pengembangan, alamat <i>IP address</i>, <i>server</i> yang dimiliki</li> </ul> |                     |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| PC<br>(lanj.) | <p>(<i>development</i> dan/atau <i>live</i>), yang mengelola sekarang, nama pengembang, tahun berapa dikembangkan, dana yang diperlukan (jika ada). Daftar Inventaris SIM dapat dilihat pada <b>Gambar F.31</b>.</p> <ul style="list-style-type: none"> <li>• Aset data/informasi didokumentasikan kedalam Daftar Rekaman Mutu. Dokumen ini berisikan judul rekaman (contohnya arsip keuangan), masa simpan (dalam tahun), lokasi simpan (contohnya almari kas keuangan), penanggung jawab (Subdit/jabatan), metode indeks (kelompok/urut abjad/urut tanggal). Namun daftar ini tidak menjelaskan secara lengkap, seperti apa saja rincian data dan informasi baik yang <i>softcopy</i> atau <i>hardcopy</i> yang tersebar dimasing-masing Subdit. Daftar Rekaman Mutu dapat dilihat pada <b>Gambar F.32</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                            |
| A.8.1.2       | Kepemilikan aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Partially compliant</i> |
|               | Apakah setiap aset yang dikelola pada inventaris terdapat pemilik atau pengelolanya?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                            |
| PC            | <ul style="list-style-type: none"> <li>• Untuk aset BMN dikelola oleh karyawan penyusun laporan dan pengelola BMN dibawah Subdit Infrastruktur. Sedangkan untuk <i>administrator</i> perangkat <i>server</i> dan jaringan diserahkan dan dikelola oleh Subdit Infrastruktur. Selain itu untuk <i>administrator</i> perangkat lunak berlisensi dan pemasangannya diserahkan dan dikelola oleh Subdit Pelayanan.</li> <li>• Untuk aset sistem informasi terpadu dikelola oleh <i>programmer</i> yang mengembangkan sistem (baik yang membuat dari awal atau yang melanjutkan) dari Subdit Pengembang dan <i>administrator</i> dari masing-masing unit/jurusan.</li> </ul> <p>Untuk aset informasi dikelola oleh masing-masing Subdit yang terkait dengan aset tersebut. Misalnya untuk <i>source code</i>, dokumen <i>user guide</i> atau <i>developer guide</i>, dan lainnya dikelola oleh Subdit Pengembangan. Sedangkan untuk dokumen ISO 9000, persentasi pelatihan SIM, data <i>email</i>, perangkat lunak <i>full version</i>, dan lainnya dikelola oleh Subdit Pelayanan. Selain itu untuk topologi jaringan, dokumen konfigurasi jaringan, <i>file log</i> dan lainnya dikelola oleh Subdit Infrastruktur.</p> <p>Namun tidak adanya dokumentasi pemilik aset secara lengkap berdasarkan daftar asetnya. Hal ini juga dikarenakan pencatatan bukan dari asetnya, namun fungsi/tugas dari masing-masing karyawan/Subdit. Selain itu juga</p> |                            |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| PC<br>(lanj.) | daftar aset informasi masih belum terdokumentasikan dengan baik untuk aset bertipe informasi berdasarkan kontrol A.8.1.1. Inventaris aset.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                            |
| A.8.1.3       | Persyaratan penggunaan aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <i>Partially compliant</i> |
|               | Apakah peraturan dalam menggunakan aset yang berhubungan dengan informasi dan fasilitas pendukungnya didokumentasi dan diterapkan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                            |
| PC            | <ul style="list-style-type: none"> <li>• Untuk Webmail ITS, DPTSI-ITS memiliki kebijakan penggunaan <i>email</i> ITS yang merinci apa yang tidak boleh dilakukan (seperti mengirim <i>spam</i>, menjual akun <i>email</i>, mengirim pesan berbau sara, pornografi, ancaman, <i>virus/malware</i>), sangsi jika melanggar (seperti menghapus keanggotaan <i>email</i> di ITS) dan tanggung jawab pihak DPTSI-ITS terhadap <i>email</i> (seperti menjamin dan menghormati kerahasiaan data pribadi setiap pengguna <i>email</i> dan berhak memberikan informasi kepada pihak ketiga sesuai persetujuan pengguna). Kebijakan ini didokumentasikan di <i>website</i> <a href="https://webmail.its.ac.id/src/login.php?bag=ketentuan">https://webmail.its.ac.id/src/login.php?bag= ketentuan</a>. Pihak DPTSI-ITS tidak bertanggung jawab atas hilangnya data/<i>email</i> yang disimpan pada <i>server</i> dan terjadinya kerusakan perangkat keras/lunak pengguna akibat penggunaan fasilitas ITS. DPTSI-ITS juga berhak mematikan <i>server email</i> ITS untuk perawatan dan menghentikan layanan <i>email</i> tanpa memberitahukan terlebih dahulu. Kebijakan penggunaan <i>email</i> dapat dilihat pada <b>Gambar F.24</b>. Untuk aset lainnya, DPTSI-ITS tidak memiliki dokumentasi kebijakan penggunaan komputer dan laptop dinas, <i>internet/intranet</i> dan media sosial, <i>fax</i>, perangkat lunak, dan perangkat lainnya.</li> <li>• Untuk aset lainnya, DPTSI-ITS memiliki beberapa instruksi kerja didalam dokumen ISO 9000, seperti penggunaan <i>switch/hub</i>, <i>router</i>, <i>server</i>, <i>HT (walkie-talkie)</i> dan <i>scanner</i>. Instruksi kerja dapat dilihat pada <b>Gambar F.33</b> sampai <b>Gambar F.38</b>. Namun instruksi kerja ini merupakan kesalahan pembuatan, dimana instruksi kerja seharusnya menjelaskan secara rinci langkah dan merujuk didalam dokumen prosedur saja. Selain itu terdapat ketidakjelasan langkah yang harus dilakukan didalam instruksi kerja yang ada, seperti didalam instruksi penggunaan <i>server</i> dituliskan “Apabila terjadi <i>trouble</i> lakukan analisa”, tapi tidak menjelaskan bagaimana cara menganalisanya.</li> </ul> |                            |
| A.8.1.4       | Pengembalian aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <i>Partially compliant</i> |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                            |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
|                              | Apakah semua karyawan dan pihak ketiga mengembalikan semua aset yang dimiliki ketika pemberhentian atau kontrak kerja karyawan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                            |
| PC                           | Untuk pengembalian aset yang dipinjam karyawan, DPTSI-ITS mengharuskan karyawan yang keluar mengembalikan aset yang dipinjam (contohnya laptop dinas). Yang mengurus peminjaman dan pengembalian adalah karyawan penyusun laporan dan pengelola BMN. Namun DPTSI-ITS tidak memiliki dokumentasi prosedur pengembalian aset yang dipinjam karyawan yang berhenti atau mutasi kerja.                                                                                                                                                                                                                   |                            |
| NC                           | Untuk penyerapan ilmu karyawan yang dimiliki, DPTSI-ITS tidak menerapkan <i>knowledge management</i> untuk mendokumentasikan ilmu-ilmu yang dimiliki karyawan selama bekerja di DPTSI-ITS.                                                                                                                                                                                                                                                                                                                                                                                                           |                            |
| A.8.2. Klasifikasi informasi |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                            |
| A.8.2.1                      | Klasifikasi informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <i>Partially compliant</i> |
|                              | Apakah informasi diklasifikasikan berdasarkan nilai, kekritisannya, atau kerahasiaan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                            |
| PC                           | DPTSI-ITS sudah mengklasifikasikan kerahasiaan informasi terkait data ataupun informasi yang disimpan di sistem informasi terpadu yang dibangun, namun klasifikasi informasi tidak mencakup dan menjabarkan semua aset informasi yang ada di DPTSI-ITS baik yang <i>softcopy</i> atau <i>hardcopy</i> .<br><br>Namun DPTSI-ITS tidak memiliki dokumentasi klasifikasi informasi, dimana masih berbentuk arahan dari Wakil Rektor III. Selain itu pernah terjadi perbedaan pandangan antara masing-masing Subdit dan Direktur DPTSI-ITS tentang mana aset informasi yang publik, rahasia dan pribadi. |                            |
| A.8.2.2                      | Pemberian <i>label</i> informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <i>Non-compliant</i>       |
|                              | Apakah prosedur untuk memberikan <i>label</i> dibuat dan diterapkan berdasarkan klasifikasi informasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                            |
| NC                           | Tidak adanya aktifitas pemberian <i>label</i> berdasarkan klasifikasi informasi seperti rahasia, internal, publik pada aset informasi baik berupa elektronik dan dokumen. Hal ini juga dikarenakan DPTSI-ITS belum memiliki klasifikasi yang jelas dan terdokumentasikan berdasarkan kontrol A.8.2.1. Klasifikasi informasi.                                                                                                                                                                                                                                                                         |                            |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.8.2.3                 | Penanganan aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Partially compliant</i> |
|                         | Apakah prosedur untuk menangani aset dibuat dan diterapkan berdasarkan klasifikasi informasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                            |
| PC                      | DPTSI-ITS memiliki Daftar Rekaman Mutu yang berisikan penanganan masa simpan, lokasi simpan dan metode indeks berdasarkan kontrol A.8.1.1. Inventaris aset. Namun dokumen tersebut tidak lengkap mendokumentasikan semua aset dan tidak sampai merinci bagaimana metode penyimpanan (baik secara terkomputerisasi dan fisik) dan pengirimannya (baik untuk <i>softcopy</i> dan <i>hardcopy</i> ) yang aman berdasarkan klasifikasi informasi. Hal ini juga dikarenakan DPTSI-ITS belum memiliki klasifikasi yang jelas dan terdokumentasikan berdasarkan kontrol A.8.2.1. Klasifikasi informasi. |                            |
| A.8.3. Penanganan media |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
| A.8.3.1                 | Manajemen <i>removable media</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <i>Non-compliant</i>       |
|                         | Apakah prosedur untuk <i>removable media</i> dibuat dan diterapkan berdasarkan klasifikasi informasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |
| NC                      | DPTSI-ITS tidak memiliki dokumentasi prosedur ataupun panduan yang mengatur penggunaan <i>removable media</i> seperti <i>flashdisk</i> , <i>hardisk</i> eksternal, <i>memory card</i> dan penyimpanan ekstenal lainnya.                                                                                                                                                                                                                                                                                                                                                                          |                            |
| A.8.3.2                 | Pembuangan media                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <i>Partially compliant</i> |
|                         | Apakah media penyimpanan (media kertas atau elektronik) dibuang secara aman ketika tidak diperlukan menggunakan prosedur formal?                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                            |
| PC                      | <ul style="list-style-type: none"> <li>Untuk media kertas, DPTSI-ITS memindahkan arsip/dokumen yang sudah melewati masa simpan sesuai dengan dokumen Daftar Rekaman Mutu ke UPT Kearsipan ITS untuk dimusnahkan. Setiap aktifitas ada dokumentasinya berupa Berita Acara Pemusnahan Arsip yang berisi identitas saksi (dari DPTSI-ITS), petugas yang melakukan dan informasi arsip yang dimusnahkan. Prosedur ini didokumentasikan dengan nama Pemusnahan Dokumen yang dapat dilihat pada <b>Gambar F.39</b>.</li> </ul>                                                                         |                            |

|                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| PC<br>(lanj.)                                  | <ul style="list-style-type: none"> <li>• Untuk media elektronik, DPTSI-ITS hanya membuang yang rusak saja <i>hardisk</i> atau perangkat yang memiliki media penyimpanan dan menyerahkan proses pembuangannya ke BAUK-ITS berdasarkan kontrol A.11.2.7. Pembuangan atau penggunaan kembali peralatan secara aman. Namun tidak adanya dokumentasi prosedur pembuangan media, dan pengelolaan khusus untuk media penyimpanan lain seperti <i>CD/DVD</i>.</li> </ul> |                            |
| A.8.3.3                                        | Pengiriman media fisik                                                                                                                                                                                                                                                                                                                                                                                                                                           | <i>Not applicable</i>      |
|                                                | Apakah media penyimpanan dilindungi dari akses tanpa izin, penyalahgunaan atau kerusakan saat dikirim?                                                                                                                                                                                                                                                                                                                                                           |                            |
| NA                                             | Ruang lingkup dalam <i>website server</i> dan <i>email</i> tidak memerlukan pengamanan untuk pengiriman media fisik. Hal ini dikarenakan tidak ada data yang berada didalam ruang lingkup yang dikirim melalui jasa kurir menggunakan kertas ( <i>print-out</i> atau surat) dan media penyimpanan ( <i>hardisk</i> , <i>CD/DVD</i> atau <i>flashdisk</i> ).                                                                                                      |                            |
| A.9. Kontrol Akses                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
| A.9.1. Kebutuhan bisnis terhadap kontrol akses |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
| A.9.1.1                                        | Kebijakan kontrol akses                                                                                                                                                                                                                                                                                                                                                                                                                                          | <i>Partially compliant</i> |
|                                                | Apakah kebijakan kontrol akses dibuat, didokumentasikan dan ditinjau berdasarkan kebutuhan bisnis dan keamanan informasi?                                                                                                                                                                                                                                                                                                                                        |                            |
| PC                                             | DPTSI-ITS sedang membuat kebijakan kontrol akses dan masih dalam bentuk <i>draft</i> .                                                                                                                                                                                                                                                                                                                                                                           |                            |
| A.9.1.2                                        | Akses ke jaringan dan layanan jaringan                                                                                                                                                                                                                                                                                                                                                                                                                           | <i>Compliant</i>           |
|                                                | Apakah pengguna hanya disediakan dengan akses ke jaringan dan layanan jaringan yang khusus disahkan hanya untuk mereka gunakan?                                                                                                                                                                                                                                                                                                                                  |                            |
| C                                              | Untuk jaringan atau layanan jaringan yang boleh diakses, Subdit-Infrastruktur mengatur agar pengguna yang sudah melakukan autentikasi saja yang dibolehkan mengakses jaringan dan layanan jaringan. Berikut ini yang dilakukan oleh Subdit Infrastruktur untuk autentikasi:                                                                                                                                                                                      |                            |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C<br>(lanj.) | <ul style="list-style-type: none"> <li>• Untuk akses ke jaringan <i>intranet</i> dan <i>internet</i>, Subdit Infrastruktur menyediakan autentikasi <i>Single Sign-On</i> untuk dapat mengakses jaringan ataupun sistem informasi terpadu yang disediakan berdasarkan kontrol A.9.3.1. Penggunaan informasi autentikasi rahasia. Selain itu cara lama yang masih dapat digunakan untuk mengakses jaringan adalah mengubah konfigurasi <i>proxy</i> di <i>browser</i> dengan isian alamat <i>proxy</i>: <a href="http://proxy.its.ac.id">proxy.its.ac.id</a> atau <a href="http://proxy2.its.ac.id">proxy2.its.ac.id</a>, nomor <i>port</i>: 8080, dan akun <i>email</i> ITS. Panduan untuk mengakses jaringan <i>internet</i> dilingkungan ITS dapat dilihat di <i>website</i> <a href="https://dptsi.its.ac.id/?page_id=1052">https://dptsi.its.ac.id/?page_id=1052</a> dan <a href="https://dptsi.its.ac.id/?page_id=1034">https://dptsi.its.ac.id/?page_id=1034</a>. Panduan konfigurasi <i>proxy</i> dapat dilihat pada <b>Gambar F.40</b> dan <b>Gambar F.41</b>.</li> <li>• Untuk akses ke layanan SIM terpadu, setiap SIM memiliki fitur autentikasi pengguna sebelum memberikan akses atau izin untuk melakukan aktifitas <i>input/output</i> terhadap informasi non-publik atau rahasia. Autentikasi umumnya menggunakan akun <i>email</i> ITS atau akun Integra ITS yang dimiliki. Tidak semua sistem informasi terpadu yang disediakan dan diizinkan untuk diakses oleh karyawan, mahasiswa, dosen atau unit/jurusan sama dengan lainnya. Seperti halnya Integra ITS dan Webmail ITS yang bisa digunakan oleh semua karyawan, mahasiswa dan dosen, dimana Git ITS hanya bisa digunakan oleh Subdit Pengembangan saja. Halaman <i>login</i> Webmail ITS dapat dilihat di <b>Gambar 4.1</b>, <b>Gambar 4.4</b> dan <b>Gambar 4.7</b>, dan halaman <i>login</i> Git ITS dapat dilihat pada <b>Gambar F.66</b>.</li> <li>• Untuk akses ke <i>server</i>, DPTSI-ITS menggunakan jalur <i>VPN</i> yang khusus bagi <i>administrator</i> untuk melakukan <i>remote</i> ke <i>server</i> berdasarkan kontrol A.10.1.1. Kebijakan dalam penggunaan kontrol kriptografi. Dalam melakukan login ke <i>server</i>, DPTSI-ITS menggunakan perangkat lunak Putty atau WinSCP. Hal ini dapat dilihat pada <b>Gambar F.42</b>.</li> </ul> |
| C            | <p>Untuk pemberian otorisasi kepada siapa yang dapat mengakses jaringan dan layanan jaringan, DPTSI-ITS memiliki prosedur pendaftaran dan penghapusan akun email yang bisa digunakan untuk alat bantu <i>login</i> berdasarkan kontrol A.9.2.1. Pendaftaran dan penghapusan pengguna.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| C            | <p>Untuk perlindungan akses ke jaringan dan layanan jaringan, DPTSI-ITS menggunakan perangkat <i>firewall</i> dan Sangfor Internet Access Management untuk pembatasan dan kontrolnya berdasarkan kontrol A.13.1.1. Kontrol jaringan.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |



|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |           |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| C                               | Untuk pengawasan penggunaan layanan jaringan, Subdit Infrastruktur mengawasi penggunaan dengan perangkat Sangfor Internet Access Management dan perangkat lunak Cacti berdasarkan kontrol A.13.1.1. Kontrol jaringan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |
| A.9.2. Manajemen akses pengguna |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |           |
| A.9.2.1                         | Pendaftaran dan penghapusan pengguna                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Compliant |
|                                 | Apakah proses pendaftaran dan penghapusan pengguna diterapkan secara formal?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |           |
| C                               | <p>Proses pendaftaran akun <i>email</i> bagi mahasiswa baru dilakukan secara <i>online</i> di <a href="https://mail2.its.ac.id">https://mail2.its.ac.id</a> atau <a href="https://webmail.its.ac.id">https://webmail.its.ac.id</a> dengan memasukkan nomor NRP dan <i>password</i> Integra ITS, lalu Subdit Pelayanan akan melakukan validasi. Sedangkan proses pendaftaran akun <i>email</i> untuk karyawan atau dosen dilakukan dengan cara mengirimkan surat permohonan ke DPTSI-ITS yang ditandatangani oleh kepala jurusan/unit. Subdit Pelayanan akan membuat akun <i>email</i> sesuai dengan isi surat permohonan, seperti nama akun dan <i>password</i> sementara.</p> <p>Nama akun <i>email</i> yang dibuat semuanya unik atau tidak sama, hal ini dikarenakan sistem akan mendeteksi jika akun <i>email</i> baru yang dibuat sama dengan akun <i>email</i> yang ada. Subdit Pelayanan juga memeriksa apakah nama akun <i>email</i> yang diminta karyawan atau dosen tidak melanggar format alamat <i>email</i> yang berlaku di ITS. Proses pendaftaran akun <i>email</i> dosen, karyawan dan mahasiswa secepatnya akan diproses maksimal 1x24 jam kerja. Pendaftaran akun <i>email</i> secara <i>online</i> dapat dilihat pada <b>Gambar F.43</b> dan <b>Gambar F.44</b>, selain itu prosedur pendaftaran akun <i>email</i> juga didokumentasikan dengan nama Layanan <i>Email: Pembuatan Akun</i> yang dapat dilihat pada <b>Gambar F.45</b>.</p> |           |
| C                               | <p>Proses penghapusan akun <i>email</i> bagi dosen, karyawan dan mahasiswa dilakukan ketika pihak Subdit Pelayanan menerima surat keterangan resmi dari unit/jurusan yang bersangkutan yang menyatakan bahwa pengguna akun <i>email</i> sudah keluar atau lulus dari ITS. Untuk penghapusan akun <i>email</i> dosen dan karyawan akan segera diproses maksimal 1x24 jam kerja. Sedangkan untuk penghapusan akun <i>email</i> mahasiswa tidak akan langsung diproses, tapi diberi jangka waktu selama 3 bulan. Layanan <i>email</i> yang bekerjasama dengan Microsoft tidak ada penghapusan akun, yang ada adalah perubahan <i>password</i> karena akun bersifat melekat pada jabatan. Prosedur untuk penghapusan akun</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |

|                     |                                                                                                                                                                                                                                                                                                                                                            |                            |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <i>C</i><br>(lanj.) | <i>email</i> didokumentasikan dengan nama Layanan <i>Email</i> : Penghapusan Akun yang dapat dilihat pada <b>Gambar F.46</b> .                                                                                                                                                                                                                             |                            |
| A.9.2.2             | Penyediaan akses pengguna                                                                                                                                                                                                                                                                                                                                  | <i>Partially compliant</i> |
|                     | Apakah proses penyediaan akses pengguna secara formal diterapkan untuk memberikan dan menghapus hak akses untuk semua tipe pengguna pada semua sistem dan layanan?                                                                                                                                                                                         |                            |
| <i>C</i>            | Untuk otorisasi hak akses pada perangkat, DPTSI-ITS melakukan otorisasi hak akses yang dilakukan oleh pemilik aset pada perangkat tersebut. Contohnya pemilik aset perangkat <i>firewall</i> memberikan otorisasi hak akses kepada karyawan baru yang ditunjuk sebagai salah satu pengelola <i>firewall</i> .                                              |                            |
| <i>PC</i>           | Untuk verifikasi dalam pemberian hak akses, DPTSI-ITS melakukan verifikasi apakah hak akses yang diberikan sesuai dengan tugas yang diemban karyawan tersebut. Namun DPTSI-ITS tidak melakukan verifikasi dengan kebijakan kontrol akses karena kebijakan tersebut masih didalam proses <i>draft</i> berdasarkan kontrol A.9.1.1. Kebijakan kontrol akses. |                            |
| <i>NC</i>           | Untuk pembatasan hak akses yang aktif sebelum prosedur otorisasi, DPTSI-ITS masih belum mengatur pemberian hak akses secara prosedural.                                                                                                                                                                                                                    |                            |
| <i>NC</i>           | Untuk rekaman hak akses yang diberikan, DPTSI-ITS tidak merekam hak akses yang dimiliki karyawan pada <i>server</i> , perangkat lunak dan perangkat jaringan. DPTSI-ITS memiliki manajemen hak akses untuk sistem informasi yang dikembangkan di Integra ITS. Namun manajemen hak akses tidak mencakup sistem yang berada didalam ruang lingkup SMKI.      |                            |
| <i>PC</i>           | Untuk peninjauan hak akses, DPTSI-ITS melakukannya berdasarkan kontrol A.9.2.5. Meninjau hak akses pengguna. Namun tidak semua perangkat yang dilakukan peninjauan.                                                                                                                                                                                        |                            |
| <i>NC</i>           | Untuk dokumentasi prosedur penyediaan hak akses pengguna, DPTSI-ITS tidak memiliki dokumentasi prosedur untuk sistem informasi, <i>server</i> , perangkat jaringan atau komputer/laptop dinas yang berisikan verifikasi tingkatan hak akses sesuai tugas, pemberian persetujuan, dokumentasi hak akses pengguna, dan lainnya.                              |                            |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                            |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| NC      | Untuk dokumentasi prosedur penghapusan hak akses pengguna, DPTSI-ITS tidak memiliki dokumentasi prosedur untuk sistem informasi, <i>server</i> , perangkat jaringan atau komputer/laptop dinas yang berisikan langkah-langkah dalam penghapusan hak akses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                            |
| A.9.2.3 | Manajemen hak akses <i>administrator</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <i>Partially compliant</i> |
|         | Apakah alokasi dan penggunaan hak akses <i>administrator</i> dikontrol dan dibatasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                            |
| NC      | Untuk identifikasi hak akses apa saja yang dimiliki setiap sistem, DPTSI-ITS belum memiliki dokumentasinya baik untuk sistem operasi, <i>DBMS</i> dan aplikasi lainnya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |
| PC      | Untuk persyaratan hak akses minimum ( <i>least privilege</i> ), DPTSI-ITS mengatur semua hak akses yang diberikan berdasarkan peran karyawan. Misalnya hak akses <i>administrator</i> Webmail ITS yang dimiliki oleh Subdit Pelayanan untuk mengelola akun <i>email</i> pengguna, dan hak akses <i>administrator server</i> dimiliki oleh Subdit Infrastruktur untuk mengelola <i>server</i> . Namun tidak adanya pembatasan dan penerapan tingkatan hak akses untuk komputer dan <i>server</i> . Misalnya semua komputer memiliki hak <i>administrator</i> saja dan semua <i>server</i> tidak dibatasi fungsi apa saja yang bisa dilakukan oleh karyawan tertentu (contohnya terdapat tipe hak akses yang dapat mengakses <i>folder/file log</i> dan tidak dapat mengakses, atau tipe hak akses yang tidak bisa menambah atau menghapus aplikasi yang terpasang). |                            |
| NC      | Untuk rekaman hak akses yang diberikan, DPTSI-ITS tidak merekam hak akses yang dimiliki karyawan termasuk hak akses <i>administrator</i> berdasarkan kontrol A.9.2.2. Penyediaan akses pengguna                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                            |
| NC      | Untuk kebutuhan hak akses <i>administrator</i> yang berjangka waktu ( <i>expired</i> ), DPTSI-ITS tidak menerapkan jenis hak akses tersebut.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
| NC      | Untuk pemisahan hak akses <i>administrator</i> dari penggunaan aktifitas biasa, DPTSI-ITS tidak memisahkan penggunaannya antara aktifitas biasa maupun aktifitas <i>administrator</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| C       | Untuk peninjauan apakah karyawan berkompetensi terhadap hak akses <i>administrator</i> yang dimiliki, DPTSI-ITS tidak melakukannya. Namun DPTSI-ITS mengadakan pelatihan kerja untuk meningkatkan kompetensi karyawan dalam melakukan pekerjaannya berdasarkan kontrol A.7.2.2. Kesadaran, pendidikan dan pelatihan keamanan informasi.                                                                                                |                            |
| NC      | Untuk dokumentasi prosedur pengecekan <i>password default</i> vendor, DPTSI-ITS tidak memiliki dokumentasi prosedur yang berisikan langkah-langkah dalam pemeriksaan apakah terdapat <i>password default</i> pada perangkat yang digunakan dan belum diganti.                                                                                                                                                                          |                            |
| NC      | Untuk dokumentasi prosedur pengelolaan <i>sharing password administrator generic</i> , DPTSI-ITS tidak memiliki dokumentasi prosedur yang berisikan langkah-langkah penggantian <i>password</i> secara berkala atau jika terdapat pengguna yang berhenti kerja, pemilihan kekuatan <i>password</i> , dan pengkomunikasian ke pengguna.                                                                                                 |                            |
| A.9.2.4 | Manajemen informasi autentikasi rahasia dari pengguna                                                                                                                                                                                                                                                                                                                                                                                  | <i>Partially compliant</i> |
|         | Apakah alokasi informasi <i>password</i> pengguna dikontrol melalui proses formal?                                                                                                                                                                                                                                                                                                                                                     |                            |
| PC      | Untuk perjanjian kerahasiaan informasi (termasuk <i>password</i> ), setiap karyawan PNS diharuskan mengucapkan sumpah/janji karyawan PNS dan Subdit Pengembangan diharuskan menandatangani perjanjian kerahasiaan sebelum diberikan akses kedalam sistem informasi yang akan dikelola berdasarkan kontrol A.13.2.4. Perjanjian kerahasiaan atau tidak menyebarkan informasi. Namun hal tersebut tidak melingkupi untuk semua karyawan. |                            |
| PC      | Untuk pemaksaan perubahan <i>password</i> sementara yang diberikan saat pemberian <i>password</i> pertama kali atau <i>reset password</i> , hanya <i>server</i> saja yang diatur, dan tidak mencakup Webmail ITS dan komputer/laptop dinas berdasarkan kontrol A.9.4.3. Sistem manajemen <i>password</i> .                                                                                                                             |                            |
| C       | Untuk dokumentasi prosedur <i>reset password</i> , DPTSI-ITS memiliki dokumentasi prosedur untuk Webmail ITS dengan nama Layanan <i>E-Mail: Reset Password</i> dapat dilihat pada <b>Gambar F.48</b> dan <b>Gambar F.49</b> . Untuk melakukan <i>reset password</i> akun <i>email</i> dapat dilakukan dengan mengunjungi DPTSI-ITS dengan membawa tanda pengenalan yang dikeluarkan ITS. Selain                                        |                            |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                            |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| C<br>(lanj.) | <p>itu untuk karyawan dan dosen dapat mengirim surat permohonan dengan identitas diri (nama, NIP, jabatan), alamat <i>email</i>, <i>password</i> baru dan disetujui pimpinan unit/jurusan baik dikirim langsung secara fisik atau hasil <i>scan</i> suratnya melalui <i>email</i>. Subdit Pelayanan memastikan identitas yang diberikan pemohon sesuai dengan yang ada didalam sistem dan mengirimkan konfirmasinya bahwa akun <i>email</i> sudah dibuat.</p> <p>Sedangkan untuk melakukan <i>reset password</i> akun <i>email</i> secara <i>online</i>, tersedia formulir lupa <i>password</i> untuk di <i>website</i> <a href="https://webmail.its.ac.id/src/login.php?bag=lupa">https://webmail.its.ac.id/src/login.php?bag=lupa</a>. Isian yang harus dimasukkan adalah jawaban dari pertanyaan yang digunakan untuk me-<i>reset password</i> (ketika membuat akun, pengguna diharuskan memasukkan pertanyaan beserta jawabannya yang bisa digunakan untuk lupa <i>password</i>), atau khusus untuk mahasiswa aktif dapat mengisi akun Integra ITS. Untuk layanan <i>email</i> yang bekerjasama dengan Microsoft tidak bisa melakukan <i>reset password</i> secara <i>online</i>. Formulir lupa <i>password</i> dapat dilihat pada <b>Gambar F.50</b>.</p> <p>Namun DPTSI-ITS tidak memiliki dokumentasi prosedur <i>reset password</i> untuk sistem informasi lainnya, <i>server</i>, perangkat jaringan atau komputer/laptop dinas didalam ruang lingkup SMKI yang berisikan langkah-langkah dalam <i>reset password</i>.</p> |                            |
| NC           | <p>Untuk pengiriman <i>password</i> sementara secara aman, DPTSI-ITS menggunakan <i>email</i> untuk pengiriman <i>password</i> sementara ke pengguna jika pengguna tidak menspesifikasikan <i>password</i> barunya melalui surat. Bahkan surat permohonan terkadang dikirim melalui <i>email</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                            |
| PC           | <p>Untuk keunikan <i>password</i> sementara yang diberikan, <i>password</i> sementara yang diberikan dengan cara datang langsung ataupun pengiriman surat permohonan tidaklah unik dan mudah ditebak (jika pengguna tidak menspesifikasikan <i>password</i> barunya). Sedangkan <i>password</i> sementara yang diberikan melalui formulir lupa <i>password</i> memiliki kombinasi <i>password</i> acak yang tidak mudah ditebak dan aman.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
| C            | <p>Untuk penggantian <i>password default</i> vendor, DPTSI-ITS menggantinya disaat pemasangan perangkat keras/lunak/jaringan.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |
| A.9.2.5      | Meninjau hak akses pengguna                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <i>Partially compliant</i> |
|              | Apakah pemilik aset meninjau hak akses pengguna dalam jangka waktu tertentu?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |

|                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                        |                            |                                                                                                                                                                                                                |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| PC                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• Untuk kontrol <i>logic</i> (<i>server</i>, perangkat lunak dan perangkat jaringan) dilakukan peninjauan apakah terdapat hak akses karyawan yang sudah keluar, namun tidak terlalu sering dilakukan misalnya satu tahun sekali. Hal ini dikarenakan jumlah karyawan yang memiliki hak akses sedikit seperti tiga orang untuk satu perangkat jaringan, dan tidak adanya hak akses yang dimiliki oleh pihak ketiga. Namun DPTSI-ITS tidak memiliki dokumentasi prosedur peninjauan hak akses pengguna dan tidak ada rekaman dari setiap aktifitas peninjauan. Selain itu juga Webmail ITS tidak dilakukan peninjauan apakah terdapat akun <i>email</i> yang belum terhapus untuk jangka waktu tertentu. Hal ini dikarenakan terdapat keyakinan bahwa semua akun yang ada bukan akun yang harus dihapus.</li> <li>• Untuk kontrol fisik (perangkat <i>fingerprint</i>, rekaman <i>CCTV</i>, dan kunci pintu <i>analog</i>). DPTSI-ITS tidak dilakukan peninjauan apakah terdapat data <i>fingerprint</i> yang belum terhapus dan kunci yang belum dikembalikan. Namun DPTSI-ITS melakukan peninjauan aktifitas mencurigakan pada <i>CCTV</i> untuk jangka waktu tertentu dan terdapat prosedurnya. Prosedur ini dapat dilihat pada <b>Gambar F.113</b>.</li> </ul> |                                        |                            |                                                                                                                                                                                                                |  |
| A.9.2.6                                                                                                                                                                                                        | <table border="1"> <tr> <td data-bbox="391 1003 1158 1115">Penghapusan atau penyesuaian hak akses</td><td data-bbox="1158 1003 1375 1115"><i>Partially compliant</i></td></tr> <tr> <td colspan="2" data-bbox="391 1115 1375 1263">Apakah hak akses semua karyawan, dosen dan mahasiswa pada informasi dan fasilitas pemrosesan informasi dihapuskan ketika pemberhentian kerja atau kontrak, kelulusan mahasiswa, atau disesuaikan jika berubah?</td></tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Penghapusan atau penyesuaian hak akses | <i>Partially compliant</i> | Apakah hak akses semua karyawan, dosen dan mahasiswa pada informasi dan fasilitas pemrosesan informasi dihapuskan ketika pemberhentian kerja atau kontrak, kelulusan mahasiswa, atau disesuaikan jika berubah? |  |
| Penghapusan atau penyesuaian hak akses                                                                                                                                                                         | <i>Partially compliant</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                        |                            |                                                                                                                                                                                                                |  |
| Apakah hak akses semua karyawan, dosen dan mahasiswa pada informasi dan fasilitas pemrosesan informasi dihapuskan ketika pemberhentian kerja atau kontrak, kelulusan mahasiswa, atau disesuaikan jika berubah? |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                        |                            |                                                                                                                                                                                                                |  |
| PC                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• Untuk akses <i>logic</i> (<i>server</i>, perangkat lunak dan perangkat jaringan), DPTSI-ITS melakukan penghapusan hak akses pengguna pada karyawan yang tidak lagi bekerja atau bertugas terhadap aset tersebut. DPTSI-ITS tidak memiliki dokumentasi prosedur penghapusan hak akses <i>logic</i> pada sistem berdasarkan kontrol A.9.2.2. Penyediaan akses pengguna. Namun untuk akses ke Webmail ITS, Subdit Pelayanan melakukan penghapusan akun <i>email</i> bagi dosen, karyawan dan mahasiswa yang tidak lagi bekerja atau kuliah di ITS berdasarkan kontrol A.9.2.1. Pendaftaran dan penghapusan pengguna. DPTSI-ITS memiliki prosedur untuk penghapusan akun <i>email</i>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                        |                            |                                                                                                                                                                                                                |  |

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                     |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| PC<br>(lanj.)                            | <ul style="list-style-type: none"><li>• Untuk akses fisik, DPTSI-ITS melakukan penghapusan hak akses dari perangkat <i>fingerprint</i> dan pengembalian kunci pintu <i>analog</i> yang dipegang oleh karyawan yang tidak lagi bekerja. DPTSI-ITS tidak memiliki dokumentasi prosedur penghapusan hak akses fisik pada kantor DPTSI-ITS.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                     |
| A.9.3. Tanggung jawab pengguna           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                     |
| A.9.3.1                                  | Penggunaan informasi autentikasi rahasia                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Compliant           |
|                                          | Apakah pengguna disarankan untuk mengikuti praktek penggunaan <i>password</i> yang aman?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                     |
| C                                        | Untuk saran penggunaan <i>password</i> yang aman, DPTSI-ITS mendokumentasikannya pada Webmail ITS di <a href="https://webmail.its.ac.id">https://webmail.its.ac.id</a> dan Integra ITS di <a href="https://integra.its.ac.id">https://integra.its.ac.id</a> . Saran yang diberikan seperti <i>password</i> harus yang sulit ditebak (seperti jangan menggunakan nama akun, minimal 8 karakter, menggunakan kombinasi huruf kapital-kecil dan bilangan, jangan menggunakan tanggal lahir atau hal-hal umum lainnya), menjaga kerahasiaan <i>password</i> meski mengatasnamakan <i>administrator</i> , mengubah <i>password</i> secara rutin, dan tidak lupa melakukan <i>log-out</i> setelah menggunakan sistem. Hal ini dapat dilihat pada <b>Gambar 4.1</b> , <b>Gambar F.51</b> , dan <b>Gambar F.52</b> . |                     |
| C                                        | Untuk penggunaan <i>Single Sign On (SSO)</i> , DPTSI-ITS masih menerapkan secara bertahap. <i>SSO</i> ini menggunakan akun Integra ITS untuk <i>login</i> ke beberapa sistem informasi terpadu dan layanan TIK lainnya yang disediakan DPTSI-ITS, termasuk untuk dapat menggunakan layanan <i>internet</i> (jadi pengguna tidak perlu mengatur <i>proxy</i> di <i>browser</i> ). <i>SSO</i> dapat dilihat pada <b>Gambar F.53</b> dan <b>Gambar F.54</b> .                                                                                                                                                                                                                                                                                                                                                   |                     |
| A.9.4. Kontrol akses sistem dan aplikasi |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                     |
| A.9.4.1                                  | Pembatasan akses informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Partially compliant |
|                                          | Apakah akses ke informasi dan fungsi sistem aplikasi (Webmail ITS) dibatasi sesuai dengan kebijakan kontrol akses?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                     |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| NC      | DPTSI-ITS tidak memiliki dokumentasi kebijakan kontrol akses berdasarkan kontrol A.9.1.1. Kebijakan kontrol akses. Jadi masih belum bisa menyesuaikan pembatasan akses ke informasi dan fungsi sistem aplikasi dengan kebijakan kontrol akses.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |
| C       | Untuk mengatur hak akses pengguna, Webmail ITS memiliki dua jenis akun yaitu akun pengguna dan akun <i>administrator</i> . Akun pengguna hanya dapat menggunakan layanan <i>email</i> Webmail ITS, seperti mengirim, menerima dan mengelola <i>email</i> pribadi. Penggunaan akun pengguna Webmail ITS dapat dilihat pada <b>Gambar 4.1</b> sampai <b>Gambar 4.8</b> . Sedangkan akun <i>admistrator</i> dapat sekaligus membuat, me-reset <i>password</i> , dan menghapus akun <i>email</i> . Penggunaan akun <i>admistrator</i> Webmail ITS dapat dilihat pada <b>Gambar F.55</b> sampai <b>Gambar F.60</b> .                                                                                                                                                                                                                                                                                                                                  |                            |
| C       | Untuk membatasi informasi apa saja yang ditampilkan di <i>output</i> , Webmail ITS tidak menampilkan isi <i>email</i> yang diterima atau dikirim oleh akun pengguna dengan menggunakan hak akses <i>administrator</i> . Akun <i>administrator</i> hanya disediakan <i>control panel</i> untuk membuat, me-reset <i>password</i> , dan menghapus akun <i>email</i> saja. Selain itu akun <i>administrator</i> tidak mengetahui <i>password</i> yang digunakan pengguna <i>email</i> sama sekali, kecuali ketika pengguna <i>email</i> meminta <i>reset password</i> ke Subdit Pelayanan. Hal ini dapat dilihat pada <b>Gambar F.58</b> dan <b>Gambar F.59</b> .                                                                                                                                                                                                                                                                                   |                            |
| C       | <p>Berikut ini adalah perlindungan akses kontrol yang dilakukan oleh DPTSI-ITS:</p> <ul style="list-style-type: none"> <li>• Untuk kontrol akses secara fisik, semua aset seperti Webmail ITS, <i>database</i>-nya dan <i>server</i> untuk menjalankannya dilindungi dari akses fisik tanpa izin dengan menaruh perangkat tersebut di ruang pusat data dan diamankan dengan perangkat kunci <i>fingerprint</i>, <i>CCTV</i> dan lainnya berdasarkan kontrol A.11.1.2. Kontrol keluar-masuk fisik dan kontrol A.11.1.3. Pengamanan kantor, ruangan dan fasilitas.</li> <li>• Untuk kontrol akses secara <i>logic</i>, Webmail ITS, <i>database</i>-nya dan <i>server</i> untuk menjalankannya dilindungi dari akses <i>logic</i> tanpa izin menggunakan <i>firewall</i> dan penggunaan <i>VPN</i> untuk akses <i>remote</i> ke <i>server</i> berdasarkan kontrol A.13.1.1. Kontrol jaringan dan kontrol A.10.1.1. Kontrol kriptografi.</li> </ul> |                            |
| A.9.4.2 | Prosedur <i>login</i> yang aman                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Partially compliant</i> |



|    |                                                                                                                                                                                                                                                                                                                                                                     |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Ketika diperlukan oleh kebijakan kontrol akses, apakah akses ke sistem dan aplikasi (Webmail ITS) dikontrol oleh prosedur <i>login</i> yang aman?                                                                                                                                                                                                                   |
| C  | Untuk melindungi sistem dari akses tanpa izin, Webmail ITS tidak menampilkan menu ataupun tampilan halaman awal sebelum sukses melakukan <i>login</i> . Sebelum pengguna dapat mengakses halaman awal Webmail ITS, diperlukan login terlebih dahulu. Hal ini dapat dilihat pada <b>Gambar 4.1</b> .                                                                 |
| NC | Untuk pesan bantuan untuk lupa <i>password</i> , DPTSI-ITS tidak menonaktifkan fitur ini. Webmail ITS menyediakan pesan bantuan agar memudahkan pengguna yang lupa <i>password</i> ketika <i>login</i> bagi layanan <i>email</i> mandiri dan dapat diisi sesuai dengan pengguna <i>email</i> . Hal ini dapat dilihat pada <b>Gambar F.64</b> .                      |
| C  | Untuk melindungi dari penebakan <i>password</i> , Webmail ITS tidak menampilkan pesan <i>error</i> yang menandakan bagian data mana yang salah atau benar (nama <i>user</i> atau <i>password</i> -nya) ketika pengguna salah memasukkan akun saat <i>login</i> . Hal ini dapat dilihat pada <b>Gambar F.61</b> sampai <b>Gambar F.63</b> .                          |
| C  | Untuk perlindungan dari <i>brute-force</i> (percobaan berulang) <i>login</i> , Webmail ITS memiliki fungsi <i>login</i> dengan <i>CAPTCHA</i> yang aktif jika pengguna salah memasukkan <i>password</i> berulang kali. Hal ini dapat dilihat pada <b>Gambar F.65</b> .                                                                                              |
| NC | Untuk riwayat aktifitas <i>login</i> , Webmail ITS tidak ada merakam percobaan <i>login</i> yang berhasil atau gagal dan laporannya ke pengguna <i>email</i> seperti waktu, <i>IP address</i> , nama perangkat, sukses/gagal saat pengguna berhasil <i>login</i> kedalam sistem. Serta Webmail ITS tidak menampilkan informasi tersebut ketika <i>login</i> sukses. |
| NC | Untuk pelaporan informasi <i>login</i> yang berbahaya, Webmail ITS tidak menginformasikan percobaan penerobosan yang berpotensi atau kesuksesan penerobosan <i>login</i> .                                                                                                                                                                                          |
| C  | Untuk melindungi <i>password</i> dilihat ketika dimasukkan, Webmail ITS tidak menampilkan <i>password</i> dengan mengubah <i>input password</i> menjadi <i>asterisk</i> . Hal dapat dilihat pada <b>Gambar 4.1</b> .                                                                                                                                                |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| C       | Untuk melindungi <i>password</i> yang dikirim melalui jaringan ketika sesi <i>login</i> , DPTSI-ITS menggunakan protokol <i>TLS</i> dan akses <i>VPN</i> (khusus untuk <i>administrator</i> yang melakukan <i>remote</i> ke <i>server</i> ). Kontrol keamanan ini membuat informasi <i>password</i> tidak dikirim dalam <i>clear text</i> dan terenkripsi berdasarkan kontrol A.10.1.1. Kebijakan dalam penggunaan kontrol kriptografi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                            |
| C       | Untuk pembatasan waktu <i>session</i> , Webmail ITS membatasi waktu <i>session</i> yang aktif pada jangka waktu tertentu. Jadi Webmail ITS akan <i>logout</i> otomatis setelah tidak digunakan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
| NA      | Untuk pembatasan waktu koneksi, Webmail ITS tidak memerlukan karena sifat dari sistem tersebut yang harus tersedia selama 24x7 hari bagi pengguna.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                            |
| A.9.4.3 | Sistem manajemen <i>password</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <i>Partially compliant</i> |
|         | Apakah terdapat sistem manajemen <i>password</i> yang gencar dan memastikan kualitas <i>password</i> ?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                            |
| PC      | <ul style="list-style-type: none"> <li>• Untuk Webmail ITS sudah diatur agar menggunakan <i>password</i> yang aman, seperti panjang <i>password</i> minimal 8 karakter, mencegah penggunaan <i>password</i> yang sama, dan tidak menampilkan <i>password</i> yang dimasukkan. Namun tidak ada keharusan kualitas kombinasi karakter, mengganti <i>password</i> baru/hasil <i>reset</i> pada saat <i>login</i> pertama kali, dan mengganti <i>password</i> secara berkala.</li> <li>• Untuk <i>server</i> sudah diatur agar menggunakan <i>password</i> yang aman, seperti panjang <i>password</i> minimal 8 karakter, penggunaan kualitas kombinasi karakter, mencegah penggunaan <i>password</i> yang sama, dan tidak menampilkan <i>password</i> yang dimasukkan. Sedangkan <i>password</i> untuk <i>server live</i> ataupun <i>development</i> yang diberikan oleh Subdit Infrastruktur ke Subdit Pengembangan dan unit/jurusan diatur agar diganti saat <i>login</i> pertama kali. Namun tidak ada keharusan mengganti <i>password</i> secara berkala.</li> </ul> |                            |

|               |                                                                                                                                                                                                                                                                                                                                                                                             |                            |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| PC<br>(lanj.) | <ul style="list-style-type: none"> <li>• Untuk komputer dan laptop dinas milik DPTSI-ITS, tidak ada standar konfigurasi agar sistem menggunakan standar <i>password</i> yang aman. Bahkan yang memasang bisa saja bukan karyawan yang bertugas di Subdit Pelayanan, namun karyawan yang bisa memasang sendiri, jadi konfigurasinya dilakukan masing-masing orang dan tidak sama.</li> </ul> |                            |
| A.9.4.4       | Penggunaan aplikasi utilitas yang diizinkan                                                                                                                                                                                                                                                                                                                                                 | <i>Non-compliant</i>       |
|               | Apakah penggunaan aplikasi utilitas yang mampu merubah sistem dan kontrol aplikasi dibatasi dan dikontrol secara ketat?                                                                                                                                                                                                                                                                     |                            |
| NC            | DPTSI-ITS tidak memiliki dokumentasi prosedur pemberian atau penghapusan hak penggunaan aplikasi utilitas yang mampu merubah sistem seperti Regedit, CMD, Terminal dan lainnya.                                                                                                                                                                                                             |                            |
| NC            | Untuk pembatasan penggunaan aplikasi utilitas, DPTSI-ITS tidak membatasi penggunaan aplikasi utilitas dikarenakan tidak adanya tingkatan hak akses pada <i>server</i> dan komputer/laptop dinas berdasarkan kontrol A.9.2.3. Manajemen hak akses administrator.                                                                                                                             |                            |
| NC            | Untuk pemberian izin pada penggunaan aplikasi utilitas, DPTSI-ITS tidak mengizinkan penggunaan aplikasi utilitas secara <i>ad-hoc</i> setelah diizinkan ataupun pembatasan ketersediaan aplikasi utilitas (durasi penggunaan yang telah diizinkan).                                                                                                                                         |                            |
| NC            | Untuk riwayat penggunaan aplikasi utilitas, DPTSI-ITS tidak memperlakukan secara khusus <i>log</i> penggunaan aplikasi utilitas.                                                                                                                                                                                                                                                            |                            |
| NC            | Untuk dokumentasi tingkatan otoritas aplikasi utilitas yang dimiliki karyawan, DPTSI-ITS tidak mendokumentasikannya.                                                                                                                                                                                                                                                                        |                            |
| NC            | Untuk menon-aktifkan atau penghapusan aplikasi utilitas, DPTSI-ITS tidak melakukannya pada sistem atau pengguna tertentu.                                                                                                                                                                                                                                                                   |                            |
| A.9.4.5       | Kontrol akses ke <i>source code</i> perangkat lunak                                                                                                                                                                                                                                                                                                                                         | <i>Partially compliant</i> |
|               | Apakah akses ke <i>source code</i> perangkat lunak dibatasi?                                                                                                                                                                                                                                                                                                                                |                            |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NC | DPTSI-ITS tidak memiliki dokumentasi prosedur pengelolaan <i>source code</i> yang berisikan langkah-langkah dalam pembuatan <i>source code</i> dari awal berikut penempatannya, sampai <i>source code</i> selesai dan dipasang kedalam <i>server</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| C  | Untuk pihak yang dapat mengakses dan mengubah <i>source code</i> , DPTSI-ITS hanya mengizinkan <i>source code</i> diakses dan diubah oleh tim yang mengembangkan sistem dan Kasubdit Subdit Pengembangan saja.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| C  | <p>Untuk manajemen <i>source code</i>, Subdit Pengembangan menyediakan sistem <i>git</i> yang berasal dari GitLab untuk mengelola <i>source code</i> yang dikembangkan di DPTSI-ITS. Sistem ini dijalankan secara lokal yang beralamatkan di <i>website</i> <a href="https://git.its.ac.id">https://git.its.ac.id</a>. Hal dapat dilihat di <b>Gambar F.66</b> dan <b>Gambar F.67</b>. Fitur yang ada didalam sistem <i>git</i> ini adalah:</p> <ul style="list-style-type: none"> <li>• Mengotentikasi pengguna yang akan menggunakan sistem dan memiliki manajemen akses (seperti izin <i>read/write</i> pada bagian <i>source code</i> tertentu) kepada Subdit Pengembangan atau Subdit lainnya yang membantu mengembangkan sistem di ITS. Jadi hanya karyawan yang diizinkan saja yang boleh mengakses <i>source code</i>.</li> <li>• Memudahkan dalam membuat, menyimpan dan menguji <i>source code</i> secara terpusat dan langsung. Jadi hal ini juga mencegah <i>source code</i> yang dibuat dan disimpan di komputer/laptop yang digunakan karyawan hilang/rusak karena tidak ada <i>backup</i> yang memadai. Selain itu juga berguna untuk memisahkan lingkungan pengembangan sistem.</li> <li>• Memiliki perangkat <i>diff</i> untuk menggabungkan dua sumber <i>source code</i> dari dua <i>programmer</i>. Setiap penggabungan <i>source code</i> dikelola dengan cara penandaan bagian/baris pada <i>source code</i> mana yang digabung, pemeriksaan konflik antar <i>source code</i>, dan pengujian terpisah setiap penggabungan yang ada. Jadi hal ini mencegah kesalahan/<i>error</i> pada pembuatan <i>source code</i>.</li> <li>• Mampu memberikan komentar atas <i>source code</i> yang ada baik mengenai masalah ataupun penjelasan <i>source code</i> tersebut. Selain itu juga terdapat <i>dashboard</i> yang dapat digunakan untuk saling berkomunikasi atau diskusi dengan karyawan lainnya tentang masalah pemrograman. Jadi hal ini memudahkan untuk dokumentasi dan pelajaran bagi karyawan terhadap <i>source code</i> yang dibuat.</li> </ul> |

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                     |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| C<br>(lanj.)                | <ul style="list-style-type: none"><li>Merekam <i>log</i> tentang aktifitas yang dilakukan masing-masing karyawan didalam tim pengembang, seperti merubah, mengakses dan mengomentari <i>source code</i>. Jadi hal ini memudahkan untuk melakukan audit atau aktifitas forensik jika diperlukan nanti.</li></ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                     |
| A.10. Kriptografi           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                     |
| A.10.1. Kontrol kriptografi |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                     |
| A.10.1.1                    | Kebijakan dalam penggunaan kontrol kriptografi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Partially compliant |
|                             | Apakah kebijakan mengenai penggunaan kontrol kriptografi untuk perlindungan informasi dibuat dan diterapkan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                     |
| NC                          | Untuk manajemen resiko pada penggunaan kontrol kriptografi, DPTSI-ITS masih belum menggunakan manajemen resiko berdasarkan kontrol A.6.1.5. Manajemen proyek untuk keamanan informasi. Jadi DPTSI-ITS tidak melakukan penanganan resiko dengan pemilihan tipe, kekuatan dan kualitas algoritma enkripsi yang digunakan untuk mengenkripsi aset informasi tertentu.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                     |
| PC                          | <p>Berikut ini adalah penggunaan enkripsi yang dilakukan oleh DPTSI-ITS:</p> <ul style="list-style-type: none"><li>Untuk melindungi jalur komunikasi, DPTSI-ITS menerapkan protokol <i>TLS</i> untuk mengamankan koneksi antara pengguna dengan semua sistem informasi terpadu yang disediakan (seperti Webmail ITS baik yang beralamatkan di <a href="https://mail2.its.ac.id">https://mail2.its.ac.id</a>, <a href="https://login.microsoftonline.com/">https://login.microsoftonline.com/</a> ataupun <a href="https://webmail.its.ac.id">https://webmail.its.ac.id</a>), dan <i>administrator</i> dengan perangkat jaringan yang dikelola (seperti <i>router</i>, <i>firewall</i>, Sangfor Internet Access Management). Protokol <i>TLS</i> yang digunakan adalah protokol yang dikeluarkan oleh DigiCert Inc. Jenis kontraknya adalah semua sub domain dibawah <a href="https://its.ac.id">its.ac.id</a> dapat dilindungi oleh protokol <i>TLS</i>. Penggunaan <i>SSL/TLS</i> dapat dilihat pada <b>Gambar F.68</b> dan <b>Gambar F.72</b>. Selain itu DPTSI-ITS menyediakan koneksi <i>VPN</i> dengan menggunakan perangkat lunak Open VPN. Koneksi ini digunakan khusus bagi <i>administrator</i> dan Subdit Pengembangan untuk melakukan koneksi <i>remote</i> ke <i>server</i>. <i>Firewall</i> sudah mengatur agar semua percobaan koneksi <i>remote</i> ke <i>server</i> yang tidak melewati koneksi <i>VPN</i> yang disediakan akan ditolak. Penggunaan <i>VPN</i> dapat dilihat pada <b>Gambar F.73</b>.</li></ul> |                     |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| PC<br>(lanj.)                       | <ul style="list-style-type: none"> <li>• Untuk melindungi media penyimpanan, sistem informasi terpadu yang dikembangkan oleh Subdit Pengembangan sudah menerapkan enkripsi untuk setiap <i>field password</i> akun yang sudah dienkripsi didalam <i>database</i>. Hal ini dapat dilihat pada <b>Gambar F.74</b>. Namun DPTSI-ITS tidak mengatur secara tertulis bagaimana karyawan menangani aset tertentu milik DPTSI-ITS berdasarkan klasifikasi informasinya (contohnya apakah penyimpanan <i>source code</i> perlu menggunakan enkripsi atau tidak) berdasarkan kontrol A.8.2.3. Penanganan aset. Selain itu juga DPTSI-ITS tidak mengenkripsi media penyimpanan baik satu <i>hardisk</i> ataupun berbentuk <i>image</i> apapun untuk melindungi data.</li> </ul> |                            |
| NC                                  | Untuk pendekatan manajemen kunci, DPTSI-ITS tidak memiliki dokumentasi kebijakan terkait manajemen kunci berdasarkan kontrol A.10.1.2. Manajemen kunci.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                            |
| NC                                  | Untuk peran dan tanggung jawab dalam penerapan enkripsi dan manajemen kunci, DPTSI-ITS belum menetapkannya secara khusus.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                            |
| NC                                  | Untuk acuan standar dalam penerapan enkripsi, DPTSI-ITS tidak mengadopsi standar apapun.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                            |
| NC                                  | DPTSI-ITS tidak memiliki dokumentasi kebijakan penggunaan enkripsi yang berisikan apa saja yang dienkripsi, tugas dan tanggung jawab yang menerapkan kebijakan dan manajemen kuncinya, standar yang digunakan, penilaian dalam pembuatan kunci enkripsi, dan aturan penggunaan enkripsi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                            |
| A.10.1.2                            | Manajemen kunci                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <i>Non-compliant</i>       |
|                                     | Apakah kebijakan mengenai penggunaan, perlindungan dan umur kunci kriptografi dibuat dan diterapkan pada keseluruhan daur hidupnya?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |
| NC                                  | DPTSI-ITS tidak memiliki dokumentasi kebijakan manajemen kunci untuk <i>VPN</i> ataupun <i>file</i> sertifikat <i>TLS</i> untuk pembuatan/pemulihan/penggantian, penyimpanan ( <i>backup</i> ), pendistribusian dan penghapusan. Hal ini dikarenakan semua karyawan dianggap sudah mengetahui hal tersebut.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                            |
| A.11. Keamanan Fisik dan Lingkungan |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
| A.11.1. Area aman                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
| A.11.1.1                            | Perlindungan keamanan fisik                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <i>Partially compliant</i> |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | Apakah perlindungan didefinisikan dan diterapkan untuk melindungi area yang berisi informasi yang kritis dan fasilitas pendukungnya?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| NC | Untuk manajemen resiko pada perlindungan keamanan fisik, DPTSI-ITS masih belum menggunakan manajemen resiko berdasarkan kontrol A.6.1.5. Manajemen proyek untuk keamanan informasi. Jadi DPTSI-ITS tidak melakukan pemilihan dan pendefinisian perlindungan fisik, serta kekuatan dari setiap perlindungannya melalui manajemen resiko.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| C  | Untuk area penerimaan tamu ( <i>receptionist area</i> ), DPTSI-ITS memilikinya dan merupakan lokasi dimana Subdit Pelayanan bekerja. Area tersebut digunakan untuk mengontrol akses fisik pengunjung untuk pergi ke ruangan lain yang hanya dapat diakses karyawan dan yang diizinkan saja, seperti ruangan-ruangan didalam Subdit Pengembangan dan Subdit Infrastruktur. <i>Receptionist area</i> dapat dilihat pada <b>Gambar F.75</b> dan <b>Gambar F.76</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| C  | <p>Untuk penghalang fisik, setiap ruangan memiliki pintu yang memiliki kunci <i>analog</i> dan biasanya akan dikunci jika tidak ada orang didalam. Hal ini dapat dilihat pada <b>Gambar F.84</b>. Selain itu lorong-lorong menuju ruangan Subdit Infrastruktur dan Subdit Pengembangan dikunci dengan perangkat kunci <i>fingerprint</i> yang hak aksesnya dimiliki oleh semua karyawan termasuk yang mahasiswa magang dan kontrak. Sedangkan untuk akses keluar-masuk pada ruangan pusat data juga dikunci dengan perangkat kunci <i>fingerprint</i> yang hak aksesnya hanya dimiliki oleh Subdit Infrastruktur dan Direktur DPTSI-ITS, dan tidak termasuk mahasiswa magang. Jadi ruangan pusat data sudah dilindungi secara fisik lebih dari satu lapis perlindungan. Pintu dengan kunci <i>fingerprint</i> dapat dilihat pada <b>Gambar F.78</b>.</p> <p>Bagi pengunjung yang ingin lewat harus meminta izin ke Subdit Pelayanan dengan menyatakan maksud kedatangannya, lalu Subdit Pelayanan akan membimbing pengunjung ke Subdit/karyawan yang hendak dikunjungi atau ditemui. Sedangkan untuk petugas perbaikan dari vendor yang datang untuk memperbaiki perangkat yang bermasalah atau mengalami gangguan, karyawan DPTSI-ITS selalu mendampingi dan mengawasi terutama jika harus masuk kedalam area sensitif seperti ruang pusat data.</p> |
| C  | Untuk pintu kebakaran, gedung Research Center ITS memilikinya untuk evakuasi jika terjadi bencana kebakaran. Operasional pintu kebakaran diawasi dan diuji secara berkala oleh Direktorat Sarana dan Prasarana. Pintu kebakaran dapat dilihat pada <b>Gambar F.79</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                            |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| NC       | Untuk sistem pendeteksi penyelundup secara fisik, DPTSI-ITS tidak memasang kontrol keamanan berupa <i>alarm</i> disetiap pintu keluar atau jendela yang dapat diakses pada ruangan pusat data atau ruangan lainnya.                                                                                                                                                                                                                                                                                                       |                            |
| NA       | Untuk pemisahan secara fisik fasilitas pemrosesan informasi dari pihak ketiga, DPTSI-ITS tidak memerlukannya karena tidak ada fasilitas pemrosesan informasi di DPTSI-ITS yang dapat diakses oleh vendor atau pihak lain tanpa izin.                                                                                                                                                                                                                                                                                      |                            |
| A.11.1.2 | Kontrol keluar-masuk fisik                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <i>Partially compliant</i> |
|          | Apakah area yang aman dilindungi oleh kontrol keluar-masuk untuk memastikan hanya karyawan yang diizinkan boleh masuk?                                                                                                                                                                                                                                                                                                                                                                                                    |                            |
| NC       | Untuk pengawasan pengunjung (kurir, vendor, petugas perbaikan, mahasiswa, dosen atau pengunjung lainnya), DPTSI-ITS tidak mengautentikasi identitas. Selain itu DPTSI-ITS tidak menyediakan daftar tamu yang mencatat tanggal/waktu dan identitas bagi pengunjung yang hendak masuk kedalam kantor.                                                                                                                                                                                                                       |                            |
| C        | Untuk membatasi agar orang yang diizinkan saja yang boleh mengakses ruangan Subdit Infrastruktur dan Subdit Pengembangan, DPTSI-ITS memasang perangkat kunci <i>fingerprint</i> di pintu masuk berdasarkan kontrol A.11.1.1. Perlindungan keamanan fisik. Selain itu untuk ruangan pusat data dipasang juga perangkat kunci <i>fingerprint</i> di pintu masuk dan <i>CCTV</i> didalam ruangan untuk mengawasi siapa yang masuk dan apa saja aktifitas yang dilakukan. <i>CCTV</i> dapat dilihat pada <b>Gambar F.80</b> . |                            |
| NC       | Untuk pengelolaan dan peninjauan rekaman akses keluar-masuk, DPTSI-ITS tidak melakukannya secara khusus pada data dari kunci <i>finger print</i> maupun <i>CCTV</i> secara berkala.                                                                                                                                                                                                                                                                                                                                       |                            |
| NC       | Untuk tanda pengenalan ( <i>tag</i> ), DPTSI-ITS tidak menyediakannya ataupun identifikasi lainnya yang dapat terlihat bagi setiap karyawan ataupun pengunjung untuk digunakan dikawasan kantor.                                                                                                                                                                                                                                                                                                                          |                            |
| C        | Untuk melakukan akses ke pusat data bagi petugas perbaikan atau vendor, DPTSI-ITS mengharuskan perizinan terlebih dahulu dan setiap akses harus diawasi oleh karyawan Subdit Infrastruktur berdasarkan kontrol A.11.1.1. Perlindungan keamanan fisik.                                                                                                                                                                                                                                                                     |                            |



|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                            |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <i>PC</i> | Untuk perubahan hak akses fisik, DPTSI-ITS tidak melakukan peninjauan hak akses fisik yang dimiliki karyawan, namun DPTSI-ITS melakukan pencabutan/penghapusan hak akses fisik (contohnya data kunci <i>fingerprint</i> atau kunci <i>analog</i> ruangan) berdasarkan kontrol A.9.2.5. Meninjau hak akses pengguna dan kontrol A.9.2.6. Penghapusan atau penyesuaian hak akses.                                                                                                                                                                                                                             |                            |
| <i>NC</i> | DPTSI-ITS tidak memiliki dokumentasi kebijakan kontrol akses fisik yang berisikan aturan keluar masuk kantor dan ruangan, apa saja yang harus dilakukan oleh karyawan untuk menangani pengunjung yang ingin mengakses secara fisik dan lainnya.                                                                                                                                                                                                                                                                                                                                                             |                            |
| A.11.1.3  | Pengamanan kantor, ruangan dan fasilitas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Partially compliant</i> |
|           | Apakah keamanan fisik untuk kantor, ruangan dan fasilitas didesain dan diterapkan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                            |
| <i>C</i>  | Untuk melindungi fasilitas utama seperti <i>server</i> dan perangkat jaringan ( <i>firewall</i> , <i>router</i> , <i>switch</i> , dan lainnya) dari akses publik, Subdit Infrastruktur menaruh perangkat tersebut diruangan khusus yaitu ruangan pusat data. Ruang pusat data dapat dilihat pada <b>Gambar F.81</b> sampai <b>Gambar F.83</b> .                                                                                                                                                                                                                                                             |                            |
| <i>PC</i> | Untuk perlindungan dari memudahkan dalam mengidentifikasi maksud dari ruangan, setiap ruangan diberikan tanda berupa nomor pada pintu yang tidak mengindikasikan maksud dari ruangan tersebut. Hal ini dapat dilihat pada <b>Gambar F.84</b> . Namun ruangan pusat data dibuat agar dapat dilihat dari luar untuk memudahkan karyawan mengawasi jika terjadi perubahan kondisi didalam ruangan. Selain itu hal tersebut memudahkan identifikasi bagi pengunjung untuk menemukan secara cepat dimana lokasi dari pusat data tersebut. Hal ini dapat dilihat pada <b>Gambar F.81</b> dan <b>Gambar F.82</b> . |                            |
| <i>C</i>  | Untuk perlindungan agar informasi rahasia atau aktifitas mudah diketahui dari luar, DPTSI-ITS menempatkan setiap meja kerja karyawan agar layar tampilan dari komputer atau laptop yang digunakan karyawan tidak menghadap keluar agar tidak dapat mudah dilihat oleh pengunjung. Hal ini dapat dilihat pada <b>Gambar F.76</b> , <b>Gambar F.77</b> dan <b>Gambar F.82</b> ,. Selain itu desain ruangan yang ada dibuat agar suara didalam ruangan tidak mudah terdengar dari luar ruangan secara jelas.                                                                                                   |                            |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                  |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| NA       | Untuk perlindungan dokumen internal telepon, DPTSI-ITS tidak memerlukan pengamanan dari akses tanpa izin. Karena jumlah karyawan sedikit dan tidak mungkin terkena aktifitas <i>social engineering</i> dari orang yang menyamar menjadi karyawan melalui telepon.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                  |
| A.11.1.4 | Perlindungan dari ancaman eksternal dan lingkungan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <i>Compliant</i> |
|          | Apakah perlindungan fisik terhadap bencana alam dan tindak kejahatan didesain dan diterapkan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                  |
| C        | <p>Untuk mencegah bencana kebakaran, DPTSI-ITS memiliki beberapa perangkat seperti:</p> <ul style="list-style-type: none"> <li>• <i>Hydrant</i> yang dipasang didinding yang berfungsi sebagai sumber air untuk memadamkan api. Hal ini dapat dilihat pada <b>Gambar F.85</b>.</li> <li>• Perangkat pemadam otomatis dipasang dilangit-langit yang berfungsi mengeluarkan material yang dapat memadamkan api secara otomatis jika terjadi kebakaran. Khusus untuk ruangan pusat data dipasang perangkat pemadam otomatis yang mengeluarkan gas untuk memadamkan api. Hal ini dapat dilihat pada <b>Gambar F.86</b>.</li> <li>• Perangkat pendeteksi asap yang dipasang didinding sebagai pendeteksi dan berbunyi jika muncul asap. Hal ini dapat dilihat pada <b>Gambar F.87</b>.</li> <li>• Perangkat APAR (Alat Pemadam Api Ringan) dipasang didalam ruangan pusat data maupun di beberapa tempat dilingkungan DPTSI-ITS yang mudah dijangkau. APAR dapat dilihat pada <b>Gambar F.88</b>, sedangkan instruksi kerja penggunaannya dapat dilihat pada <b>Gambar F.38</b>.</li> </ul> |                  |
| C        | <p>Untuk mencegah pencurian atau akses tanpa izin, terdapat satpam yang bertugas siang dan malam disekitar gedung ITS Research Center. Selain itu DPTSI-ITS juga memiliki karyawan yang berjaga dan tidur didalam kantor di malam hari. Ruang pusat data tidak memiliki jendela yang terhubung ke luar gedung yang dapat memudahkan pencurian atau pelemparan benda berbahaya. DPTSI-ITS juga mengatur agar ruang pusat data terlindungi dari pencurian ataupun akses tanpa izin menggunakan pintu dengan kunci <i>fingerprint</i>, <i>CCTV</i> dan lainnya berdasarkan A.11.1.1. Perlindungan keamanan fisik dan kontrol A.11.1.2. Kontrol keluar-masuk fisik. Selain itu terdapat beberapa lemari yang memiliki kunci <i>analog</i> yang biasanya digunakan untuk menyimpan dokumen yang tidak boleh diakses tanpa izin. Hal ini dapat dilihat pada <b>Gambar F.89</b> dan <b>Gambar F.90</b>.</p>                                                                                                                                                                                   |                  |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                               |                            |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.11.1.5 | Bekerja di area yang aman                                                                                                                                                                                                                                                                                                                                                                                                                     | <i>Partially compliant</i> |
|          | Apakah prosedur untuk bekerja pada area yang aman didesain dan diterapkan?                                                                                                                                                                                                                                                                                                                                                                    |                            |
| NC       | DPTSI-ITS tidak memiliki dokumentasi prosedur pengelolaan akses ke pusat data yang berisikan langkah-langkah yang dilakukan sebelum akses ke pusat data dan sesudahnya, misalnya permohonan izin sebelum masuk, mengisi <i>logbook</i> , dan lainnya.                                                                                                                                                                                         |                            |
| C        | Untuk menghindari dari pekerjaan yang tidak diawasi, DPTSI memasang <i>CCTV</i> didalam ruangan pusat data berdasarkan kontrol A.11.1.2. Kontrol keluar-masuk fisik.                                                                                                                                                                                                                                                                          |                            |
| PC       | Untuk perlindungan ruangan pusat data, ketika ruangan tidak ada orangnya maka biasanya pintu akan dikunci. Namun DPTSI-ITS tidak meninjau data riwayat akses secara berkala berdasarkan kontrol A.11.1.2. Kontrol keluar-masuk fisik.                                                                                                                                                                                                         |                            |
| C        | DPTSI-ITS memiliki kebijakan bekerja di area yang aman (pusat data) yang ada didalam ruangan pusat data tentang larangan bagi karyawan maupun pengunjung untuk melakukan aktifitas makan-minum, merokok, memfoto atau merekam aktifitas didalam ruangan tanpa izin.                                                                                                                                                                           |                            |
| A.11.1.6 | Area pengiriman dan bongkar-muat                                                                                                                                                                                                                                                                                                                                                                                                              | <i>Partially compliant</i> |
|          | Apakah titik akses seperti area pengiriman dan penerimaan barang dimana non-karyawan dapat masuk dikontrol dan jika bisa diisolasi dari fasilitas pemrosesan informasi dari akses tanpa izin?                                                                                                                                                                                                                                                 |                            |
| NC       | Untuk ruangan khusus bongkar-muat, DPTSI-ITS tidak memiliki ruangan khusus untuk bongkar muat barang yang diterima, jadi setiap kurir yang membawa kiriman (seperti surat, barang atau makanan-minuman) diperlukan untuk mengakses kedalam bagian kantor DPTSI-ITS secara langsung. Hal ini dapat dilihat pada <b>Gambar F.91</b> yang mana satu-satunya pintu masuk yang dilalui karyawan/pengunjung ataupun kurir berikut barang bawaannya. |                            |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                     |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| C                 | Untuk pendaftaran barang yang masuk, DPTSI-ITS merekamnya langsung kedalam Daftar Inventaris Aset untuk BMN berdasarkan kontrol A.8.1.1. Inventaris aset.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                     |
| NC                | Untuk pemisahan lokasi kiriman, DPTSI-ITS tidak memisahkan lokasi kiriman masuk dan keluar barang secara fisik.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                     |
| NC                | DPTSI-ITS tidak memiliki dokumentasi prosedur dan perangkat untuk memeriksa apakah kiriman dari kurir tidak mengandung bahan peledak, benda tajam, kimia/beracun, palsu (dirubah sesuai aslinya) atau yang mengandung bahan berbahaya lainnya kedalam kantor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                     |
| A.11.2. Peralatan |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                     |
| A.11.2.1          | Penempatan dan perlindungan peralatan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Partially compliant |
|                   | Apakah peralatan ditaruh dan dilindungi untuk mengurangi resiko dari ancaman lingkungan dan akses tanpa izin?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                     |
| C                 | Untuk mengurangi akses yang tidak perlu pada perangkat atau dilihat tanpa izin ketika penggunaan perangkat, Subdit Infrastruktur menempatkan <i>server</i> , <i>server backup</i> dan perangkat jaringan utama secara khusus diruangan pusat data agar aman dari akses/perusakan tanpa izin berdasarkan kontrol A.11.1.3. Pengamanan kantor, ruangan dan fasilitas. Ruang pusat data dapat dilihat pada <b>Gambar F.82</b> dan <b>Gambar F.83</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                     |
| PC                | <p>Beberapa kontrol keamanan yang diterapkan untuk mengurangi resiko:</p> <ul style="list-style-type: none"><li>• Untuk melindungi dari pencurian dan akses/perusakan tanpa izin, terdapat beberapa kontrol keamanan seperti karyawan <i>shift malam</i>, satpam, lemari, pintu dengan kunci <i>analog/finger print</i>, dan lainnya berdasarkan kontrol A.11.1.2. Kontrol keluar-masuk fisik dan kontrol A.11.1.4. Perlindungan dari ancaman eksternal dan lingkungan.</li><li>• Untuk melindungi dari kebakaran, terdapat beberapa kontrol keamanan seperti perangkat APAR, perangkat pemadam otomatis, perangkat pendeteksi asap, dan <i>hydrant</i> berdasarkan kontrol A.11.1.4. Perlindungan dari ancaman eksternal dan lingkungan.</li><li>• Untuk melindungi dari kegagalan daya listrik, Subdit Infrastruktur menggunakan <i>UPS</i> dan <i>diesel generator</i> berdasarkan kontrol A.11.2.2. Utilitas pendukung.</li></ul> |                     |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| C<br>(lanj.) | <ul style="list-style-type: none"> <li>• Untuk melindungi dari gangguan/interferensi pada data, DPTSI-ITS memisahkan kabel listrik dengan kabel jaringan ketika pemasangan berdasarkan kontrol A.11.2.3. Keamanan pemasangan kabel. Namun untuk melindungi dari gangguan/interferensi antar sinyal <i>wireless access point (WiFi)</i>, Subdit Infrastruktur masih belum memiliki perangkat untuk mengecek gelombang apakah terdapat interferensi antar beberapa sinyal yang dipancarkan dengan frekuensi yang sama.</li> <li>• Untuk melindungi dari perubahan kondisi lingkungan (suhu dan kelembaban), <i>Air Conditioner (AC)</i> secara <i>default</i> dipasang disetiap ruang kantor di DPTSI-ITS untuk mengatur suhu dan kelembaban ruangan. <i>AC</i> dilengkapi <i>remote</i> yang mampu mengawasi sensor informasi suhu dan kelembaban dari jauh. Selain itu Subdit Infrastruktur memasang <i>AC</i> lebih dari satu agar dapat digunakan sebagai <i>backup</i> jika perangkat tiba-tiba rusak atau mati. Hal ini dapat dilihat pada <b>Gambar F.92</b> dan <b>Gambar F.93</b>.</li> <li>• Untuk melindungi dari petir, Subdit Infrastruktur memasang perangkat <i>grounding</i> untuk mengalirkan lonjakan listrik yang berlebih kedalam tanah. Selain itu terdapat pula kotak panel listrik atau stop kontak dengan dilengkapi fungsi <i>circuit breaker</i> yang menjaga arus listrik dari beban berlebih dan hubungan singkat. Jika terjadi penyimpangan pada aliran listrik, maka <i>circuit breaker</i> akan memutuskan aliran listrik secara otomatis agar perangkat elektronik yang terhubung tidak terbakar. Hal ini dapat dilihat pada <b>Gambar F.94</b> dan <b>Gambar F.96</b>.</li> <li>• Untuk melindungi dari penyingkapan informasi melalui jaringan tanpa kabel, Subdit Infrastruktur menggunakan protokol <i>HTTPS</i> dan jalur <i>VPN</i> berdasarkan kontrol A.10.1.1. Kebijakan dalam penggunaan kontrol kriptografi.</li> </ul> |                            |
| C            | Untuk panduan pada fasilitas pemrosesan informasi, Subdit Infrastruktur membuat larangan makan, minum dan merokok di area pusat data berdasarkan kontrol A.11.1.5. Bekerja di area yang aman.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                            |
| A.11.2.2     | Utilitas pendukung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <i>Partially compliant</i> |
|              | Apakah peralatan dilindungi dari kegagalan daya dan gangguan lainnya yang disebabkan gangguan pada utilitas pendukung?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                            |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C  | Untuk melindungi peralatan dan perangkat dari kegagalan daya, Subdit Infrastruktur menggunakan <i>diesel generator</i> dan <i>UPS</i> . <i>Diesel generator</i> berfungsi untuk menangani kehilangan pasokan listrik yang berjalan secara otomatis ketika terjadi mati listrik. Sedangkan <i>UPS</i> difungsikan untuk membantu jeda waktu perangkat <i>diesel generator</i> untuk aktif dalam memasok listrik, dimana perangkat ini bekerja secara terus menerus ( <i>standby-online</i> ). <i>Diesel generator</i> dan <i>UPS</i> yang dipasang hanya memasok aliran listrik ke semua perangkat yang ada di ruang pusat data, tidak diatur agar memasok ke semua ruangan di DPTSI-ITS. Untuk melindungi perangkat komputer dari kegagalan daya, setiap perangkat juga dipasang <i>UPS</i> dengan daya rendah yang hanya mampu digunakan beberapa menit untuk menyimpan hasil pekerjaan. |
| NC | Untuk memenuhi kapasitas perkembangan bisnis, Subdit Infrastruktur tidak melakukan pengecekan dan perencanaan secara berkala apakah kapasitas sistem baik jaringan dan <i>server</i> saat ini memenuhi perkembangan bisnis kedepannya berdasarkan kontrol A.12.1.3. Manajemen kapasitas.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| C  | Untuk memastikan perangkat berjalan dengan benar, Subdit Infrastruktur juga melakukan perawatan perangkat dan peralatan yang ada agar dapat beroperasi terus menerus berdasarkan kontrol A.11.2.4. Pemeliharaan perlengkapan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| C  | Untuk mendeteksi malfungsi pada perangkat, Subdit Infrastruktur menggunakan Nagios dan ITS Web Monitoring System untuk mengawasi kondisi operasional (hidup-mati atau gangguan) pada perangkat jaringan, absensi <i>fingerprnt</i> dan <i>server</i> berdasarkan kontrol A.13.1.1. Kontrol jaringan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| C  | Untuk macam-macam rute fisik yang berganda, Subdit Infrastruktur menggunakan topologi STAR dan RING pada infrastruktur jaringannya agar memiliki beberapa titik untuk <i>me-routing</i> jika terdapat satu jalur komunikasi yang bermasalah berdasarkan kontrol A.13.1.3. Pemisahan pada jaringan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| C  | Untuk sumber penerangan dan komunikasi cadangan, Subdit Infrastruktur memiliki beberapa senter dan <i>walkie-talkie</i> jika terjadi keadaan darurat.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| C  | Untuk tombol keadaan darurat, Subdit Infrastruktur memiliki kotak panel yang terdapat tombol keadaan darurat untuk sumber daya listrik pada ruangan pusat data berdasarkan kontrol A.11.2.3. Keamanan pemasangan kabel.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                            |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| NC       | Untuk redundansi konektivitas jaringan, meskipun DPTSI-ITS memiliki dua jalur koneksi yaitu IP transit yang utama dan Astine yang dijadikan <i>backup</i> , namun DPTSI-ITS hanya memiliki satu layanan <i>ISP</i> yaitu PT. Telkom berdasarkan kontrol A.13.1.2. Keamanan layanan jaringan.                                                                                                                                                                                                                                                                                                                                                                         |                            |
| A.11.2.3 | Keamanan pemasangan kabel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <i>Partially compliant</i> |
|          | Apakah kabel listrik dan jaringan dilindungi dari gangguan dan kerusakan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |
| C        | Untuk perlindungan kabel didalam gedung, kabel listrik dan jaringan dilindungi oleh pipa pelindung kabel. Hal ini dapat dilihat pada <b>Gambar F.97</b> . Sedangkan untuk perlindungan kabel yang ada diluar gedung, kabel dilindungi oleh pipa pelindung kabel, dan saluran beton bertulang berbentuk penampang huruf U (U-Ditch) didalam tanah. Selain itu di setiap jalur kabel listrik dan jaringan didalam tanah diberikan patok penanda kabel agar memudahkan karyawan proyek menemukan lokasi kabel, seperti "FO" untuk kabel <i>fiber optic</i> dan "2.0 VA" untuk kabel listrik. Hal ini dapat dilihat pada <b>Gambar F.98</b> sampai <b>Gambar F.100</b> . |                            |
| C        | Untuk melindungi dari gangguan/interfensi elektromagnetik pada data, DPTSI-ITS memisahkan kabel listrik dengan kabel jaringan ketika pemasangan. Kabel listrik dipasang didalam lantai, sedangkan untuk kabel jaringan dipasang didalam langit-langit ruangan. Untuk perlindungan tambahan, hal ini tidak diperlukan karena penggunaan kabel <i>fiber optic</i> yang tahan akan interfensi untuk jalur koneksi tertentu.                                                                                                                                                                                                                                             |                            |
| NA       | Untuk perlindungan <i>port</i> koneksi dari akses tanpa izin secara fisik, tidak perlu dilakukan pemasangan. Hal ini dikarenakan berdasarkan kontrol A.9.1.2. Akses ke jaringan dan layanan jaringan, untuk melakukan koneksi ke jaringan di lingkungan ITS diperlukan <i>login</i> ke Integra ITS. Halaman login Integra ITS dapat dilihat pada <b>Gambar F.51</b> .                                                                                                                                                                                                                                                                                                |                            |
| C        | Untuk perlindungan kontrol panel listrik dari akses tanpa izin secara fisik, kontrol panel diletakkan didalam ruangan pusat data. Hal ini dapat dilihat pada <b>Gambar F.95</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                            |
| PC       | Untuk menjaga dari kerusakan kabel, setiap sebulan sekali kabel secara fisik diinspeksi untuk melihat adanya kerusakan kabel dan perangkat tanpa izin yang dipasang pada kabel. Tata cara pengujian apakah kabel tidak putus/rusak juga didokumentasikan kedalam instruksi kerja (seharusnya panduan) <i>Cable</i>                                                                                                                                                                                                                                                                                                                                                   |                            |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                            |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| PC<br>(lanj.) | <p><i>Tester</i> yang dapat dilihat pada <b>Gambar F.101</b>. DPTSI-ITS juga mendokumentasikan instruksi kerja (seharusnya panduan) <i>Crimping Tools</i> untuk memasang kabel jaringan dengan kepala kabelnya (RJ-45 untuk kabel <i>UTP</i>) yang dapat dilihat pada <b>Gambar F.102</b>. Namun DPTSI-ITS masih belum memiliki perangkat, kualifikasi/sertifikasi karyawan dan panduannya untuk pemasangan atau perbaikan kabel <i>fiber optic</i>, hanya ada perangkat pengecek (<i>tester</i>) saja. Apabila terjadi kerusakan atau DPTSI-ITS ingin memasang kabel <i>fiber optic</i> maka yang dilakukan adalah menghubungi vendor. Sedangkan untuk kabel listrik dan kabel <i>UTP</i>, DPTSI-ITS memiliki perangkat pemasang dan pengecek (<i>crimping tool</i>, <i>tester</i>, kabel cadangan, <i>jack</i>, <i>panel</i> dan lainnya), kualifikasi/sertifikasi karyawan dan panduannya.</p>                                                                                                                                                                                                                                                                                                                                           |                            |
| A.11.2.4      | Pemeliharaan perlengkapan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Partially compliant</i> |
|               | Apakah peralatan dipelihara/dirawat secara benar untuk memastikan integritas dan ketersediaanya?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |
| PC            | <p>DPTSI-ITS melakukan aktifitas pemeriksaan serta perawatan perangkat secara fisik dan berkala untuk menjaga kelancaran operasional perangkat. Berikut ini adalah aktifitas pemeriksaan dan perawatan terhadap beberapa perangkat yang dilakukan:</p> <ul style="list-style-type: none"> <li>• <i>Diesel generator</i> dilakukan dengan aktifitas pemanasan mesin selama satu minggu sekali, sekaligus pengecekan air aki dan kondisi radiatornya berdasarkan prosedur dari vendor. Selain itu dilakukan juga penggantian oli mesin selama satu tahun sekali.</li> <li>• <i>UPS</i> dilakukan dengan aktifitas pengecekan tegangan maupun informasi kondisi yang ditampilkan pada indikator/panel perangkat selama dua minggu sekali berdasarkan prosedur dari vendor. Jika baterai <i>UPS</i> sudah habis atau rusak, maka dilakukan penggantian baterai. Prosedur ini didokumentasikan dengan nama Penggantian Baterai <i>UPS</i> yang dapat dilihat pada <b>Gambar F.103</b>.</li> <li>• <i>AC</i> dilakukan dengan aktifitas pembersihan komponen didalam perangkat seperti <i>filter</i> selama 3 bulan sekali. Prosedur ini didokumentasikan dengan nama Perawatan <i>AC</i> yang dapat dilihat pada <b>Gambar F.104</b>.</li> </ul> |                            |



|                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>PC<br/>(lanj.)</p> | <ul style="list-style-type: none"> <li>• Listrik dan perangkat pengamanannya dilakukan dengan aktifitas pemeriksaan tegangan dan arus, lalu melaporkannya ke PLN jika terdapat penyimpangan selama 6 bulan sekali. Sedangkan untuk perangkat <i>grounding</i> dilakukan dengan aktifitas pemeriksaan nilai arus pada perangkat. Prosedur tersebut didokumentasikan dengan nama Perawatan Listrik yang dapat dilihat pada <b>Gambar F.105.</b>, dan Perawatan <i>Grounding</i> yang dapat dilihat pada <b>Gambar F.106.</b></li> <li>• <i>Switch</i> dilakukan dengan aktifitas pembersihan perangkat dari debu dan mengecek kondisi komponen apakah terdapat kerusakan fisik atau tidak selama 6 bulan sekali. Prosedur ini didokumentasikan dengan nama Perawatan <i>Switch</i> yang dapat dilihat pada <b>Gambar F.107.</b></li> </ul> <p>Namun pemeriksaan dan perawatan yang dilakukan tidak mencakup komputer atau laptop dinas yang digunakan karyawan secara khusus dan berkala. Selain itu tidak ada dokumentasi prosedur perawatan <i>server</i>. Selain itu riwayat setiap pemeriksaan dan perawatan perangkat tidak terdokumentasikan (contohnya menggunakan <i>checklist</i> waktu, nama perangkat dan tanggal pemeriksaan/perawatan) yang dapat membantu apakah perangkat sudah dirawat secara terjadwal atau tidak.</p> |
| <p>C</p>              | <p>Untuk karyawan yang merawat perangkat adalah yang bertanggung jawab terhadap aset tersebut, contohnya karyawan Subdit Infrastruktur yang melakukan perawatan <i>server</i> dan <i>router</i>, bukan karyawan Subdit Pengembangan atau Subdit Pelayanan. Apabila terdapat kerusakan pada <i>server</i>, <i>router</i>, <i>switch</i>, <i>access point</i>, <i>firewall</i>, <i>printer/scanner/fax</i>, <i>diesel generator</i>, <i>UPS</i>, pendingin ruangan/<i>AC</i>, komponen perangkat dan lainnya, DPTSI-ITS memanggil vendor untuk memperbaiki jika masih dalam masa garansi setelah diinspeksi dan diperkirakan apa yang rusak (perangkat atau komponen). Sedangkan jika perangkat tersebut sudah melewati masa garansi, maka DPTSI-ITS mengganti perangkat tersebut dengan yang baru.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <p>NC</p>             | <p>Untuk rekaman riwayat perawatan, DPTSI-ITS tidak merekam perawatan pada perangkat yang berisikan semua kesalahan sebenarnya atau yang diperkirakan, dan semua tindakan pencegahan atau perbaikannya.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <p>C</p>              | <p>Untuk melindungi informasi rahasia pada perangkat ketika masa perawatan, karyawan DPTSI-ITS mendampingi petugas perbaikan dari vendor yang akan menginspeksi dan memperbaiki perangkat, terutama jika petugas perbaikan masuk kedalam area sensitif seperti ruangan pusat data berdasarkan kontrol A.11.1.1. Kontrol keluar-masuk fisik. Apabila petugas perbaikan diharuskan</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                            |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <i>C</i><br>(lanj.) | membawa perangkat milik DPTSI-ITS keluar dari kantor setelah diinspeksi, maka yang dibawa hanyalah komponen tertentu didalam perangkat jika kerusakan berada pada komponen tersebut. Sedangkan untuk kerusakan yang terjadi dikeseluruhan perangkat, maka perangkat tersebut akan dilepas media penyimpanannya (jika ada) dan disimpan oleh Subdit Infrastruktur (contohnya <i>server</i> yang mengalami kerusakan pada <i>memory</i> , maka yang dibawa hanya <i>memory</i> saja).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
| <i>NA</i>           | Untuk perawatan yang dibutuhkan oleh kebijakan asuransi, DPTSI-ITS tidak melakukannya karena tidak memiliki kebijakan tersebut.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                            |
| <i>PC</i>           | Untuk inspeksi untuk memastikan perangkat tidak dirubah tanpa izin setelah perawatan, DPTSI-ITS tidak melakukannya dan hanya memeriksa untuk melihat apakah perangkat bisa beroperasi dan tidak <i>malfungsi</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
| A.11.2.5            | Pemindahan aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <i>Partially compliant</i> |
|                     | Apakah perangkat keras/lunak, peralatan dan informasi tidak boleh dibawa keluar organisasi tanpa izin terlebih dahulu?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                            |
| <i>PC</i>           | <p>Untuk perizinan untuk membawa keluar aset, diharuskan mengajukan surat permohonan ke pengelola aset yang bersangkutan di DPTSI-ITS jika dilakukan untuk kepentingan kerja atau aktifitas lainnya. Berikut ini adalah bentuk surat permohonan yang ada:</p> <ul style="list-style-type: none"> <li>• Untuk laptop dinas atau perangkat lainnya bagi karyawan DPTSI-ITS menggunakan Berita Acara Pemakaian Barang Inventaris yang berisikan identitas peminjam, identitas yang mengetahui dalam hal ini Direktur DPTSI-ITS, identitas penyusun laporan dan pengelola BMN, informasi aset, dan ketentuan yang harus dipatuhi (seperti memakai sesuai peruntukan, menjaga dan memelihara aset, dan mengembalikan aset). Namun DPTSI-ITS tidak memiliki dokumentasi prosedur perizinan peminjaman perangkat/peralatan.</li> <li>• Untuk barang dan perangkat bagi unit/jurusan, karyawan dan pemangku kepentingan diluar DPTSI-ITS menggunakan Berita Acara Peminjaman Barang yang berisikan identitas peminjam, identitas penyusun laporan dan pengelola BMN, informasi aset, waktu pengembalian. Namun DPTSI-ITS tidak memiliki dokumentasi prosedur perizinan peminjaman perangkat/peralatan.</li> </ul> |                            |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <i>PC</i><br>(lanj.) | <ul style="list-style-type: none"> <li>• Untuk aset informasi bagi unit/jurusan, karyawan dan pemangku kepentingan diluar DPTSI-ITS menggunakan Surat Permohonan Data. Prosedur permintaan data dapat dilihat pada <b>Gambar F.108</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                            |
| <i>NC</i>            | <p>Untuk pengecekan barang bawaan pada pintu keluar-masuk kantor, DPTSI-ITS tidak melakukan pengecekan untuk melihat apakah terdapat barang curian, berbahaya atau lainnya yang tidak boleh lewat. Hal ini bisa dilihat pada <b>Gambar F.91</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                            |
| A.11.2.6             | Keamanan peralatan dan aset yang dibawa keluar                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Non-compliant</i>       |
|                      | Apakah keamanan diterapkan pada aset yang dibawa keluar kantor?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |
| <i>NC</i>            | <p>DPTSI-ITS memperbolehkan membawa keluar kantor aset (contohnya laptop dinas yang bisa dibawa pulang) jika sudah diizinkan berdasarkan kontrol A.11.2.5. Pemindahan aset. Namun tidak ada aturan keamanan pada perangkat yang dipinjam ataupun yang digunakan diluar kantor berdasarkan kontrol A.6.2.2. <i>Teleworking</i>. Jika laptop dinas tersebut hilang, maka dilakukan pelaporan kehilangan barang ke polisi.</p> <p>Sedangkan untuk aset informasi tidak ada kontrol keamanan yang diterapkan untuk mengamankan aspek <i>confidentiality</i> dan <i>integrity</i>-nya. Hal ini dikarenakan tidak adanya panduan penanganan aset berdasarkan klasifikasi informasi, dan tidak adanya aturan dan prosedur dalam pertukaran informasi berdasarkan kontrol A.8.2.3. Penanganan aset dan kontrol A.13.2.1. Kebijakan dan prosedur pertukaran informasi.</p> |                            |
| A.11.2.7             | Pembuangan atau penggunaan kembali peralatan secara aman                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <i>Partially compliant</i> |
|                      | Apakah semua peralatan yang memiliki media penyimpanan harus dipastikan data sensitif dan lisensi perangkat lunak dihapus secara aman sebelum dibuang?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |
| <i>PC</i>            | <p>Untuk pembuangan perangkat dengan media penyimpanan, Subdit Infrastruktur akan mengirimkan perangkat ke BAUK-ITS ketika suatu perangkat tersebut rusak dan tidak bisa diperbaiki oleh vendor karena sudah melewati masa garansi. Perangkat tersebut nantinya dirusak secara fisik oleh BAUK-ITS. Aktifitas ini ada dokumentasinya berupa Berita Acara Pembuangan Barang yang berisi identitas saksi (dari DPTSI-ITS), petugas yang melakukan dan informasi barang yang dibuang. Namun tidak adanya</p>                                                                                                                                                                                                                                                                                                                                                         |                            |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                            |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| PC<br>(lanj.)              | dokumentasi prosedur pembuangan media elektronik, dan pengelolaan khusus untuk media penyimpanan lain seperti <i>CD/DVD</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                            |
| NC                         | Untuk penilaian resiko pada media penyimpanan yang dibuang, DPTSI-ITS tidak melakukannya, apakah perangkat diperlukan perbaikan oleh vendor atau dihancurkan secara fisik.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                            |
| A.11.2.8                   | Peralatan pengguna yang tidak diawasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <i>Partially compliant</i> |
|                            | Apakah pengguna menjamin bahwa peralatan yang tidak diawasi telah terlindungi (misalnya menggunakan <i>screensaver</i> atau <i>logout</i> otomatis)?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                            |
| PC                         | <ul style="list-style-type: none"> <li>• Untuk Webmail ITS diatur agar melakukan <i>log-out</i> secara otomatis, dimana pengguna tidak dapat mengakses kembali meskipun sebelumnya pengguna tersebut tidak melakukan <i>log-out</i> setelah selesai menggunakan.</li> <li>• Untuk perangkat jaringan dan <i>server</i>, karyawan yang akan mengakses <i>control panel</i> pada perangkat jaringan seperti <i>switch</i>, <i>router</i> dan <i>firewall</i> diperlukan <i>login administrator</i> ulang secara <i>default</i>. Sistem operasi Linux yang dipasang di beberapa <i>server</i> juga memerlukan karyawan untuk <i>login</i> ulang untuk melakukan koneksi <i>remote</i>.</li> <li>• Untuk komputer dan laptop dinas milik DPTSI-ITS, tidak ada standar konfigurasi yang mengatur agar sistem menjalankan <i>screensaver</i> yang diberi <i>password</i> ketika tidak digunakan atau ditinggal. Bahkan yang memasang bisa saja bukan karyawan yang bertugas di Subdit Pelayanan, namun karyawan yang bisa melakukannya sendiri. Jadi konfigurasinya dilakukan masing-masing orang dan tidaklah sama.</li> </ul> |                            |
| A.11.2.9                   | Kebijakan merapihkan meja dan membersihkan layar                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <i>Non-compliant</i>       |
|                            | Apakah kebijakan merapihkan meja untuk kertas dan <i>flashdisk</i> , dan kebijakan membersihkan layar diterapkan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                            |
| NC                         | DPTSI-ITS tidak memiliki dokumentasi kebijakan <i>clear desk and screen</i> yang berisikan aturan terkait kerapihan meja kerja dari dokumen, <i>flashdisk</i> atau media penyimpanan lainnya, maupun membersihkan layar monitor dari catatan terutama informasi akun pengguna.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |
| A.12. Keamanan Operasional |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                            |

| <b>A.12.1. Prosedur operasional dan tanggung jawab</b> |                                                                                                                                                                                                                                                             |                            |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.12.1.1                                               | Mendokumentasikan prosedur operasional                                                                                                                                                                                                                      | <i>Partially compliant</i> |
|                                                        | Apakah prosedur operasional didokumentasikan dan tersedia untuk semua pengguna yang membutuhkan?                                                                                                                                                            |                            |
| <i>C</i>                                               | DPTSI-ITS memiliki dokumen ISO 9000 yang berisi berbagai dokumen, prosedur, instruksi kerja, dan formulir untuk menjalankan aktifitas bisnis di DPTSI-ITS. Dokumen ini disimpan di Subdit Pelayanan, dimana pengguna yang ingin mengakses dapat melihatnya. |                            |
| <i>NC</i>                                              | Prosedur kontak dukungan dan eskalasi (A.6.1.3) belum didokumentasikan.                                                                                                                                                                                     |                            |
| <i>NC</i>                                              | Prosedur pengembalian aset (A.8.1.4) belum didokumentasikan.                                                                                                                                                                                                |                            |
| <i>NC</i>                                              | Prosedur pemberian <i>label</i> klasifikasi informasi (A.8.2.2) belum didokumentasikan.                                                                                                                                                                     |                            |
| <i>NC</i>                                              | Prosedur penanganan aset (A.8.2.3) belum didokumentasikan.                                                                                                                                                                                                  |                            |
| <i>NC</i>                                              | Prosedur <i>removable media</i> (A.8.3.1) belum didokumentasikan.                                                                                                                                                                                           |                            |
| <i>C</i>                                               | Prosedur pemusnahan dokumen (A.8.3.2) sudah didokumentasikan.                                                                                                                                                                                               |                            |
| <i>C</i>                                               | Prosedur pembuatan akun <i>email</i> (A.9.2.1) sudah didokumentasikan.                                                                                                                                                                                      |                            |
| <i>C</i>                                               | Prosedur penghapusan akun <i>email</i> (A.9.2.1) sudah didokumentasikan.                                                                                                                                                                                    |                            |
| <i>NC</i>                                              | Prosedur penyediaan hak akses pengguna (A.9.2.2) belum didokumentasikan.                                                                                                                                                                                    |                            |
| <i>NC</i>                                              | Prosedur penghapusan hak akses pengguna (A.9.2.2) belum didokumentasikan.                                                                                                                                                                                   |                            |
| <i>NC</i>                                              | Prosedur pengecekan <i>password default</i> vendor (A.9.2.3) belum didokumentasikan.                                                                                                                                                                        |                            |
| <i>NC</i>                                              | Prosedur pengelolaan <i>sharing password administrator generic</i> (A.9.2.3) belum didokumentasikan.                                                                                                                                                        |                            |
| <i>PC</i>                                              | Prosedur <i>reset password</i> (A.9.2.4) belum semuanya didokumentasikan.                                                                                                                                                                                   |                            |

|    |                                                                                          |
|----|------------------------------------------------------------------------------------------|
| NC | Prosedur peninjauan hak akses pengguna (A.9.2.5) belum didokumentasikan.                 |
| NC | Prosedur pemberian hak penggunaan aplikasi utilitas (A.9.4.4) belum didokumentasikan.    |
| NC | Prosedur penghapusan hak penggunaan aplikasi utilitas (A.9.4.4) belum didokumentasikan.  |
| NC | Prosedur pengelolaan <i>source code</i> (A.9.4.5) belum didokumentasikan.                |
| NC | Prosedur pengelolaan akses ke pusat data (A.11.1.5) belum didokumentasikan.              |
| PC | Prosedur pemeliharaan perlengkapan (A.11.2.4) belum semuanya didokumentasikan.           |
| NC | Prosedur perizinan peminjaman perangkat/peralatan (A.11.2.5) belum didokumentasikan.     |
| C  | Prosedur perizinan permintaan informasi (A.11.2.5) sudah didokumentasikan.               |
| NC | Prosedur pembuangan media elektronik (A.11.2.7) belum didokumentasikan.                  |
| PC | Prosedur manajemen perubahan (A.12.1.2) belum semuanya didokumentasikan.                 |
| NC | Prosedur pemulihan dari kegagalan perubahan (A.12.1.2) belum didokumentasikan.           |
| NC | Prosedur penanganan <i>malware</i> (A.12.2.1) belum didokumentasikan.                    |
| NC | Prosedur peringatan <i>malware</i> (A.12.2.1) belum didokumentasikan.                    |
| C  | Prosedur <i>backup</i> informasi (A.12.3.1) sudah didokumentasikan.                      |
| NC | Prosedur pengawasan dan pengujian hasil <i>backup</i> (A.12.3.1) belum didokumentasikan. |
| PC | Prosedur pemasangan perangkat lunak (A.12.5.1) belum semuanya didokumentasikan.          |
| NC | Prosedur penghapusan perangkat lunak (A.12.5.1) belum didokumentasikan.                  |

|    |                                                                                                                    |
|----|--------------------------------------------------------------------------------------------------------------------|
| NC | Prosedur manajemen kerentanan teknis (A.12.6.1) belum didokumentasikan.                                            |
| NC | Prosedur audit sistem informasi (A.12.7.1) belum didokumentasikan.                                                 |
| C  | Prosedur pengelolaan jaringan (A.12.1.3 dan A.13.1.1) sudah didokumentasikan.                                      |
| NC | Prosedur pertukaran informasi (A.13.2.1) belum didokumentasikan.                                                   |
| NC | Prosedur Perlindungan Informasi <i>Email</i> Sensitif berupa <i>Attachement</i> (A.13.2.1) belum didokumentasikan. |
| C  | Prosedur pengembangan sistem informasi (A.14.2.2) sudah didokumentasikan.                                          |
| NC | Prosedur modifikasi paket instalasi perangkat lunak (A.14.2.4) belum didokumentasikan.                             |
| NC | Prosedur proses pengembangan di lingkungan pengembangan untuk sistem tertentu (A.14.2.6) belum didokumentasikan.   |
| C  | Prosedur pengujian sistem (A.14.2.9) sudah didokumentasikan.                                                       |
| NC | Prosedur peninjauan kesesuaian layanan TIK (A.15.2.1) belum didokumentasikan.                                      |
| NC | Prosedur perubahan ketentuan layanan TIK (A.15.2.2) belum didokumentasikan.                                        |
| PC | Prosedur penanganan insiden (A.16.1.1) belum semuanya didokumentasikan.                                            |
| C  | Prosedur pelaporan insiden (A.16.1.2) sudah didokumentasikan.                                                      |
| NC | Prosedur penilaian dan pengklasifikasian insiden keamanan informasi (A.16.1.4) belum didokumentasikan.             |
| C  | Prosedur pencatatan aktifitas manajemen insiden (A.16.1.5) sudah didokumentasikan.                                 |
| NC | Prosedur eskalasi dan komunikasi insiden (A.16.1.6) belum didokumentasikan.                                        |
| NC | Prosedur penanganan bukti forensik (A.16.1.7) belum didokumentasikan.                                              |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| NC       | Prosedur <i>business continuity plan</i> atau <i>disaster recovery plan</i> (A.17.1.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
| C        | Prosedur pemasangan perangkat lunak legal (A.18.1.2) sudah didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                            |
| NC       | Prosedur pengawasan perangkat lunak legal (A.18.1.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                            |
| NC       | Prosedur audit keamanan informasi (A.18.2.1) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
| NC       | Prosedur tindakan perbaikan ( <i>corrective action</i> ) dari ketidakpatuhan/ <i>non-conformity</i> (A.18.2.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                            |
| NC       | Prosedur peninjauan kepatuhan teknis (A.18.2.3) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                            |
| A.12.1.2 | Manajemen perubahan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Partially compliant</i> |
|          | Apakah perubahan pada organisasi, proses bisnis dan sistem informasi yang mempengaruhi keamanan informasi dikontrol?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
| PC       | Untuk identifikasi perubahan, DPTSI-ITS melakukan identifikasi terlebih dahulu apa saja yang dirubah. Contohnya perubahan besar seperti pemasangan <i>distribution switch</i> pada infrastruktur jaringan dilakukan diskusi terlebih dahulu seperti konfigurasi, jumlah penggunaan perangkat, dan lainnya. Sedangkan untuk perubahan kecil seperti konfigurasi perangkat yang sudah biasa dilakukan, maka tidak diperlukan identifikasi secara khusus. Semua perubahan yang dilakukan tidak semuanya terekam dengan baik, contohnya perubahan pada <i>port</i> apa saja yang di- <i>block</i> pada <i>firewall</i> tidak ada riwayat perubahannya (seperti siapa yang merubah, apa yang dirubah, waktu, dan lainnya). |                            |
| C        | Untuk perencanaan dan pengujian perubahan, DPTSI-ITS merencanakan apa saja yang akan dilakukan untuk melaksanakan perubahan dan menguji perubahan tersebut. Contohnya saat Subdit Infrastruktur memperbaharui perangkat lunak dengan versi terbaru, maka diuji terlebih dahulu apakah versi terbaru tidak menimbulkan masalah. Jika menimbulkan masalah maka Subdit Infrastruktur tetap menggunakan versi lama.                                                                                                                                                                                                                                                                                                       |                            |



|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NC | Untuk penilaian dampak perubahan, setiap perubahan tidak dilakukan penilaian dampak jika terjadi perubahan termasuk dampak keamanan informasi secara khusus. Hal ini dikarenakan DPTSI-ITS belum menggunakan manajemen resiko untuk melakukan proyek berdasarkan kontrol A.6.1.5. Manajemen proyek untuk keamanan informasi.                                                                                                                                                                                                                                                                                                 |
| C  | Untuk verifikasi kebutuhan keamanan informasi, DPTSI-ITS melakukan verifikasi untuk melihat apakah perubahan sesuai dengan kebutuhan keamanan yang direncanakan. Contohnya kebutuhan agar <i>server</i> tidak bisa diakses dari luar jaringan ITS (dengan memasukkan ke domain <i>private</i> ), maka dilakukan verifikasi dengan melakukan koneksi dari luar.                                                                                                                                                                                                                                                               |
| PC | Untuk persetujuan formal untuk perubahan, DPTSI-ITS memerlukan pada aktifitas tertentu. Contohnya dalam pembuatan SIM dimana perubahannya mengenai proses bisnis, maka diperlukan persetujuan pimpinan dan pembahasan lebih lanjut. Namun tidak semua perubahan disetujui secara formal, contohnya penggunaan algoritma baru pada SIM yang dikembangkan yang lebih baik dari sebelumnya atau perubahan konfigurasi yang diluar kepala pada perangkat keras/lunak/jaringan.                                                                                                                                                   |
| C  | Untuk komunikasi perubahan, DPTSI-ITS selalu menginformasikan kepada dosen, karyawan, dan mahasiswa melalui <i>website</i> ataupun pelatihan TIK jika perubahan melibatkan sistem informasi dan layanan TIK yang digunakan pengguna. Contohnya ketika DPTSI-ITS bekerja sama dengan Google untuk meningkatkan fasilitas <i>email</i> -nya, dimana perubahannya dipublikasikan di <i>website</i> <a href="https://mail2.its.ac.id/infoumum.php">https://mail2.its.ac.id/infoumum.php</a> . Informasi yang ada termasuk prosedur untuk migrasi <i>email</i> yang lama ke Gmail. Hal ini bisa dilihat pada <b>Gambar F.16</b> . |
| NC | Untuk dokumentasi kebijakan manajemen perubahan, DPTSI-ITS tidak memiliki dokumentasi kebijakan yang berisikan aturan dalam perubahan, klasifikasi perubahan, pengujian dan penilaian dampak pada perubahan, cara mengkomunikasikan perubahan, dan lainnya.                                                                                                                                                                                                                                                                                                                                                                  |
| NC | Untuk dokumentasi prosedur pemulihan dari kegagalan perubahan, DPTSI-ITS tidak memiliki dokumentasi prosedur yang berisikan langkah-langkah untuk mengembalikan kondisi sistem ke keadaan semula jika terjadi kegagalan dalam penerapan perubahan baru.                                                                                                                                                                                                                                                                                                                                                                      |

|                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                     |                            |                                                                                                                                                           |  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| PC                                                                                                                                                        | <p>Untuk dokumentasi manajemen perubahan, DPTSI-ITS memilikinya seperti:</p> <ul style="list-style-type: none"> <li>• Prosedur Dokumentasi Konfigurasi Sistem Jaringan yang digunakan untuk membuat dan mendokumentasikan setiap perubahan konfigurasi perangkat jaringan dan <i>server</i>. Langkah prosedurnya adalah membuka lembar worksheet dan mencatat seluruh perubahan. Setelah itu menyimpan perubahan berikut kedalam format <i>PDF</i>, lalu melakukan <i>backup file</i>. Prosedur ini dapat dilihat pada <b>Gambar F.109</b>.</li> <li>• Prosedur perubahan sistem yang dikembangkan yang digunakan untuk mengelola perubahan sistem yang baru atau pembaharuan kontrol A.14.2.2. Prosedur kontrol perubahan sistem.</li> </ul> <p>Namun DPTSI-ITS tidak memiliki dokumentasi prosedur manajemen perubahan yang berisikan langkah-langkah mulai dari perencanaan sampai penyelesaian perubahan untuk semua jenis perubahan (baik perangkat lunak, konfigurasi, infrastruktur, dan lainnya) yang terjadi di DPTSI-ITS.</p> |                     |                            |                                                                                                                                                           |  |
| A.12.1.3                                                                                                                                                  | <table border="1"> <tr> <td data-bbox="384 898 1158 1016">Manajemen kapasitas</td><td data-bbox="1158 898 1386 1016"><i>Partially compliant</i></td></tr> <tr> <td colspan="2" data-bbox="384 1016 1386 1173">Apakah penggunaan sumber daya diawasi, ditingkatkan dan diproyeksikan untuk kebutuhan kapasitas kedepan untuk memastikan performa sistem yang dibutuhkan?</td></tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Manajemen kapasitas | <i>Partially compliant</i> | Apakah penggunaan sumber daya diawasi, ditingkatkan dan diproyeksikan untuk kebutuhan kapasitas kedepan untuk memastikan performa sistem yang dibutuhkan? |  |
| Manajemen kapasitas                                                                                                                                       | <i>Partially compliant</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                     |                            |                                                                                                                                                           |  |
| Apakah penggunaan sumber daya diawasi, ditingkatkan dan diproyeksikan untuk kebutuhan kapasitas kedepan untuk memastikan performa sistem yang dibutuhkan? |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                     |                            |                                                                                                                                                           |  |
| C                                                                                                                                                         | <p>Dalam identifikasi kebutuhan kapisitas pada sumber daya, DPTSI-ITS melakukan:</p> <ul style="list-style-type: none"> <li>• Untuk sumber daya pada sistem dan jaringan, Subdit Infrastruktur memiliki standar spesifikasi sistem (contohnya spesifikasi <i>processor</i>, <i>memory</i>, <i>hardisk</i>, dan lainnya yang diperlukan) dan standar konfigurasi pemasangan jaringan.</li> <li>• Untuk sumber daya pada karyawan, Direktorat SDM dan Organisasi sudah mengidentifikasi kebutuhan minimum jumlah karyawan di DPTSI-ITS dengan menggunakan metode analisis struktur organisasi dan proses bisnis di organisasi.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                 |                     |                            |                                                                                                                                                           |  |
| C                                                                                                                                                         | <p>Dalam pengawasan ketersediaan kapisitas pada sumber daya, DPTSI-ITS melakukan:</p> <ul style="list-style-type: none"> <li>• Untuk sumber daya pada sistem dan jaringan, Subdit Infrastruktur menggunakan Cacti dan <i>Internet Access Management</i> berdasarkan prosedur <i>Monitoring Bandwith</i>. Langkah prosedurnya adalah menjalankn</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                     |                            |                                                                                                                                                           |  |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C<br>(lanj.) | <p>aplikasi dan memantau performa <i>bandwith</i>, jika kecepatan <i>bandwith</i> lambat maka dilakukan pengaturan alokasi <i>bandwith</i>. Cacti merupakan perangkat lunak yang memonitor protokol <i>SNMP</i> dan melaporkan kondisi sistem (seperti penggunaan <i>processor</i>, <i>memory</i>, <i>hardisk</i> untuk <i>server</i>) ataupun beban trafik pada <i>backbone</i> antar jaringan (contohnya jaringan <i>LAN</i> di ITS Sukolilo dengan jaringan <i>LAN</i> di ITS Cokroaminoto), masing-masing <i>server</i> (contohnya Webmail ITS dan Integra ITS), atau perangkat lainnya yang memiliki <i>IP address</i> yang disajikan kedalam grafik yang dikelompokkan berdasarkan waktu. Prosedur <i>Monitoring Bandwith</i> dapat dilihat pada <b>Gambar F.110</b>, dan Cacti dapat dilihat pada <b>Gambar F.111</b>.</p> <ul style="list-style-type: none"> <li>• Untuk sumber daya pada karyawan, Direktorat SDM dan Organisasi menggunakan perangkat absensi <i>fingerprint</i> yang tersebar diseluruh unit/jurusan dilingkungan ITS untuk mengumpulkan data karyawan yang masuk kerja secara <i>realtime</i>. Data tersebut nanti diolah menggunakan SIM Kepegawaian untuk perhitungan jumlah absensi karyawan. Perangkat absensi <i>fingerprint</i> dapat dilihat pada <b>Gambar F.112</b>.</li> </ul>                                                                                      |
| C            | <p>Dalam meningkatkan dan menjaga kapasitas pada sistem (<i>server</i>, aplikasi dan infrastruktur jaringan), atau mengurangi permintaan, DPTSI-ITS melakukan:</p> <ul style="list-style-type: none"> <li>• Untuk menjaga kapasitas <i>hardisk</i> pada <i>server</i>, dilakukan dengan pengaturan logrotate (utilitas untuk mengelola <i>log</i> aktifitas) pada <i>server</i> melakukan penghapusan <i>file log</i> yang lebih dari 3 hari. Berdasarkan kontrol A.12.4.1. Mencatat kejadian, DPTSI-ITS memindahkan <i>file log</i> tersebut secara terpusat ke <i>SIEM</i>.</li> <li>• Untuk menjaga performa <i>server</i>, dilakukan dengan menonaktifkan beberapa aplikasi atau fitur yang tidak digunakan untuk menjalankan proses bisnis yang ada.</li> <li>• Untuk meningkatkan penyelesaian sejumlah proses, DPTSI-ITS melakukan pengukuran setiap aktifitas yang didokumentasikan dalam prosedur ISO 9000 berdasarkan target yang ingin dicapai. Cara pengukuran dan prosedur apa saja yang diukur dapat dilihat pada <b>Gambar F.163</b> dan <b>Gambar F.164</b>.</li> <li>• Untuk meningkatkan performa sistem informasi terpadu, dilakukan dengan mengoptimasi <i>query</i> pada <i>database</i> dan logika pemrograman yang dibangun. Aktifitas ini dilakukan ketika terjadi masalah pada sistem misalnya respon lambat, atau ketika pengajuan untuk pemutakhiran oleh pengguna.</li> </ul> |

|                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                              |                            |                                                                                                                             |  |
|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|----------------------------|-----------------------------------------------------------------------------------------------------------------------------|--|
| C<br>(lanj.)                                                                                                                | <ul style="list-style-type: none"> <li>• Untuk meningkatkan performa jaringan, dilakukan dengan membatasi alokasi <i>bandwidth</i> untuk layanan yang boros atau tidak berhubungan dengan bidang akademik seperti media <i>streaming</i> (Youtube), media sosial (Facebook, Twitter) dan lainnya. Selain itu berdasarkan kontrol A.13.1.1. Kontrol jaringan, terdapat pembatasan protokol <i>P2P</i> untuk torrent yang banyak menghabiskan <i>bandwidth</i>.</li> </ul>                                                                                                                          |                                                              |                            |                                                                                                                             |  |
| NC                                                                                                                          | Untuk proyeksi dan perencanaan kapasitas pada sumber daya, Subdit Infrastruktur tidak mendokumentasikan perencanaan manajemen kapasitas kedepan untuk melihat kebutuhan kapasitas kedepan. Selain itu juga Direktorat SDM dan Organisasi tidak mendokumentasikan perencanaan manajemen kapasitas kedepan untuk karyawan di DPTSI-ITS.                                                                                                                                                                                                                                                             |                                                              |                            |                                                                                                                             |  |
| A.12.1.4                                                                                                                    | <table border="1"> <tr> <td>Pemisahan lingkungan pengembangan, pengujian dan operasional</td><td><i>Partially compliant</i></td></tr> <tr> <td colspan="2">Apakah lingkungan pengembangan, pengujian, dan operasional dipisah untuk mengurangi resiko akses atau perubahan tanpa izin?</td></tr> </table>                                                                                                                                                                                                                                                                                         | Pemisahan lingkungan pengembangan, pengujian dan operasional | <i>Partially compliant</i> | Apakah lingkungan pengembangan, pengujian, dan operasional dipisah untuk mengurangi resiko akses atau perubahan tanpa izin? |  |
| Pemisahan lingkungan pengembangan, pengujian dan operasional                                                                | <i>Partially compliant</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                              |                            |                                                                                                                             |  |
| Apakah lingkungan pengembangan, pengujian, dan operasional dipisah untuk mengurangi resiko akses atau perubahan tanpa izin? |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                              |                            |                                                                                                                             |  |
| NC                                                                                                                          | DPTSI-ITS tidak mendokumentasikan kebijakan untuk pemindahan perangkat lunak yang berisikan aturan memindahkan perangkat lunak dari pengembangan sampai status operasional.                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                              |                            |                                                                                                                             |  |
| C                                                                                                                           | Untuk pembagian lingkungan pengembangan, DPTSI-ITS memisahkan lingkungan untuk pengembangan (komputer/laptop milik DPTSI-ITS atau sendiri), pengujian ( <i>server development</i> ), dan operasional ( <i>server live</i> ) sistem informasi berdasarkan kontrol A.14.2.6. Lingkungan pengembangan yang aman.                                                                                                                                                                                                                                                                                     |                                                              |                            |                                                                                                                             |  |
| C                                                                                                                           | <p>Untuk perubahan pada sistem operasi dan aplikasi, DPTSI-ITS melakukan:</p> <ul style="list-style-type: none"> <li>• Semua perubahan sistem informasi yang dikembangkan diuji terlebih dahulu sebelum dioperasikan dilingkungan yang terpisah dari lingkungan operasional berdasarkan berdasarkan kontrol A.14.2.9. Pengujian penerimaan sistem dan kontrol A.14.2.6. Lingkungan pengembangan yang aman.</li> <li>• Semua perubahan sistem operasi dan aplikasi pendukung lainnya diuji terlebih dahulu sebelum dioperasikan dilingkungan yang terpisah dari lingkungan operasional.</li> </ul> |                                                              |                            |                                                                                                                             |  |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| C                                       | Untuk perangkat pengembangan seperti <i>compiler</i> , <i>editor</i> atau sistem utilitas lainnya, Subdit Pengembangan tidak menambahkannya pada produk jadi didalam <i>server live</i> .                                                                                                                                                                                                                                                                                             |                            |
| C                                       | Untuk pengujian hak akses pada sistem, Subdit Infrastruktur melakukan pengujian pada semua profil pengguna untuk memastikan tidak ada kesalahan macam-macam aturan yang ditetapkan pada setiap profil.                                                                                                                                                                                                                                                                                |                            |
| NA                                      | Untuk pengelolaan data sensitif untuk pengujian, Subdit Pengembangan tidak menggunakan sama sekali data sensitive karena menggunakan data <i>dummy</i> berdasarkan kontrol A.14.3.1. Perlindungan data pengujian.                                                                                                                                                                                                                                                                     |                            |
| A.12.2 Perlindungan dari <i>malware</i> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
| A.12.2.1                                | Kontrol terhadap <i>malware</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <i>Partially compliant</i> |
|                                         | Apakah kontrol pendeteksi, perlindungan dan perbaikan untuk menangani <i>malware</i> diterapkan dengan kombinasi kesadaran pengguna yang tepat?                                                                                                                                                                                                                                                                                                                                       |                            |
| NC                                      | Untuk pembatasan pemasangan perangkat lunak secara <i>administratif</i> , DPTSI-ITS tidak memiliki dokumentasi kebijakan pembatasan penggunaan perangkat lunak yang berisikan rincian perangkat lunak apa saja yang boleh dipasang dan yang tidak boleh dipasang berdasarkan kontrol A.12.6.2. Pembatasan pemasangan perangkat lunak.                                                                                                                                                 |                            |
| NC                                      | Untuk pembatasan pemasangan perangkat lunak secara <i>technical</i> , DPTSI-ITS tidak mengatur sistem komputer dan laptop agar mencegah pemasangan perangkat lunak tanpa izin berdasarkan kontrol A.12.5.1. Pemasangan perangkat lunak pada sistem operasi.                                                                                                                                                                                                                           |                            |
| C                                       | Untuk melindungi <i>website</i> berbahaya ataupun yang melanggar hukum, DPTSI-ITS memanfaatkan fitur dari <i>ISP</i> PT. Telkom yaitu InternetPositif berdasarkan kontrol A.13.1.2. Keamanan layanan jaringan. Hal ini dapat dilihat pada <b>Gambar F.133</b> . DPTSI-ITS juga melakukan pemblokiran <i>website</i> tersebut menggunakan perangkat <i>Internet Access Management</i> berdasarkan kontrol A.13.1.1. Kontrol jaringan. Hal ini dapat dilihat pada <b>Gambar F.134</b> . |                            |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NC | Untuk mengurangi kerentanan yang dapat dieksploitasi oleh <i>malware</i> , DPTSI-ITS kurang melaksanakan aktifitas manajemen kerentanan berdasarkan kontrol A.12.6.1. Manajemen kerentanan teknis.                                                                                                                                                                                                                                                                                                                                        |
| NC | Untuk peninjauan perangkat lunak dan data pada sistem secara berkala, DPTSI-ITS tidak melaksanakan peninjauan apakah terdapat <i>file</i> atau penambahan tanpa izin secara formal dan berkala baik untuk sistem yang kritis.                                                                                                                                                                                                                                                                                                             |
| C  | Untuk melindungi dari <i>malware</i> , DPTSI-ITS menggunakan Honeypot Dionaea dan fitur <i>anti-virus</i> dari layanan <i>ISP</i> untuk melindungi infrastruktur jaringan berdasarkan kontrol A.13.1.1. Kontrol jaringan dan kontrol A.13.1.2. Keamanan layanan jaringan. Selain itu DPTSI-ITS menggunakan perangkat lunak ClamAV untuk melindungi <i>server</i> yang dapat dilihat pada <b>Gambar F.114</b> , dan Windows Defender untuk melindungi komputer dengan sistem operasi Windows yang dapat dilihat pada <b>Gambar F.115</b> . |
| C  | Untuk melindungi data yang dirusak <i>malware</i> , DPTSI-ITS melakukan aktifitas <i>backup</i> secara berkala untuk data didalam <i>server</i> berdasarkan kontrol A.12.3.1. <i>Backup</i> informasi. Sedangkan untuk data yang dipegang karyawan dilakukan masing-masing dengan cara <i>backup</i> secara <i>online</i> ke Google Drive, Office 365 dan lainnya.                                                                                                                                                                        |
| NC | Untuk karantina (lingkungan terpisah) untuk sistem yang terinfeksi, DPTSI-ITS melakukannya jika terdapat infeksi <i>malware</i> pada suatu <i>server</i> agar tidak menyebar ke sistem lain sebelum dibersihkan. Namun hal ini tidak mencakup komputer yang ada di DPTSI-ITS karena tidak adanya penanggung jawab dan prosedur khusus untuk penanganan <i>malware</i> .                                                                                                                                                                   |
| NC | Untuk peran dan tanggung jawab dalam penanganan <i>malware</i> , DPTSI-ITS belum menetapkan untuk penanganan <i>malware</i> pada sistem, pelatihan penggunaan perangkat <i>anti-malware</i> , pelaporan dan pemulihan dari serangan <i>malware</i> .                                                                                                                                                                                                                                                                                      |
| NC | Untuk dokumentasi kebijakan penanganan <i>malware</i> , DPTSI-ITS tidak memiliki dokumentasi kebijakan yang berisikan aturan dalam penanganan <i>malware</i> , dan cara mendapatkan <i>file</i> atau perangkat lunak pada <i>internet</i> atau media lainnya baik untuk pengguna maupun <i>administrator</i> .                                                                                                                                                                                                                            |

|                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                     |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| NC             | Untuk dokumentasi prosedur penanganan <i>malware</i> , DPTSI-ITS tidak memiliki dokumentasi prosedur yang berisikan langkah-langkah pelaporan, penanganan dan pemulihan dari serangan <i>malware</i> .,                                                                                                                                                                                                                                                                              |                     |
| NC             | Untuk dokumentasi prosedur peringatan <i>malware</i> , DPTSI-ITS tidak memiliki dokumentasi prosedur yang berisikan bagaimana pengumpulan informasi mengenai <i>malware</i> baru dari <i>internet</i> , verifikasi kebenaran informasi, dan pemberitahuan informasi kepada pengguna.                                                                                                                                                                                                 |                     |
| A.12.3. Backup |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                     |
| A.12.3.1       | Backup informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Partially compliant |
|                | Apakah salinan informasi, perangkat lunak dan <i>clone</i> dari <i>hardisk</i> diambil dan diuji secara teratur berdasarkan kebijakan <i>backup</i> ?                                                                                                                                                                                                                                                                                                                                |                     |
| NC             | Untuk dokumentasi kebijakan <i>backup</i> , DPTSI-ITS belum mendokumentasikan kebijakan yang berisikan aturan dalam melakukan <i>backup</i> (baik informasi, perangkat lunak dan sistem), banyaknya <i>copy</i> hasil <i>backup</i> , serta cara pengujian dan pengamanannya.                                                                                                                                                                                                        |                     |
| C              | Untuk dokumentasi prosedur <i>backup</i> informasi, DPTSI-ITS memiliki prosedur yang bernama <i>Backup Data</i> dan dapat dilihat pada <b>Gambar F.116</b> .                                                                                                                                                                                                                                                                                                                         |                     |
| C              | Untuk fasilitas <i>backup</i> , Subdit Infrastruktur memiliki dua tipe <i>server backup</i> yaitu yang digunakan untuk menyimpan data <i>server</i> secara otomatis (sinkronisasi <i>database</i> ), dan untuk <i>file</i> konfigurasi dan <i>file log</i> perangkat jaringan. Sedangkan untuk <i>file</i> pekerjaan tertentu yang dimiliki karyawan, biasanya dilakukan <i>backup</i> ke media penyimpanan <i>online</i> seperti Google Drive, Office 365 dan lainnya.              |                     |
| C              | Untuk rekaman riwayat aktifitas <i>backup</i> , setiap <i>backup</i> yang dilakukan dicatat kedalam formulir yang bernama Form Rekap Kegiatan <i>Backup Database</i> dan Sistem SIM, yang berisikan nama sistem informasi yang di- <i>backup</i> , frekuensi <i>backup</i> yang dibedakan antara sistem dan <i>database</i> -nya, lokasi tempat penyimpanan <i>backup</i> , dan <i>checklist</i> apakah sudah dilakukan atau belum. Hal ini dapat dilihat pada <b>Gambar F.117</b> . |                     |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PC                                      | <p>Untuk frekuensi dan jenis <i>backup</i> (sebagian/semua atau satuan/berganda), hal yang dilakukan DPTSI-ITS adalah:</p> <ul style="list-style-type: none"> <li>• Memperhatikan frekuensi dan apa saja yang di <i>backup</i> berdasarkan kebutuhan bisnisnya, seperti melakukan aktifitas <i>backup</i> untuk <i>server</i> Webmail ITS, <i>DNS</i>, <i>SIEM</i> AlienVault dan Git ITS dilakukan setiap hari pada jam 1 malam, sedangkan untuk <i>server proxy</i> ITS, Nagios, ITS Web Monitoring System, dan Open VPN tidak dilakukan <i>backup</i>. Sedangkan aktifitas <i>backup</i> untuk konfigurasi perangkat jaringan dilakukan hanya ketika terjadi perubahan saja.</li> <li>• Tidak menyimpan hasil <i>backup</i> secara berganda untuk mencegah jika satu hasil <i>backup</i> mengalami <i>corrupt</i> pada sistem tertentu yang sudah didefinisikan.</li> </ul> |
| NC                                      | <p>Untuk penempatan hasil <i>backup</i>, DPTSI-ITS menaruh <i>server backup</i> didalam gedung dan ruangan yang sama dengan perangkat yang di-<i>backup</i> (pusat data DPTSI-ITS didalam gedung Research Center ITS). Sedangkan untuk sistem informasi lain yang dikembangkan (seperti SIM Akademik), memiliki hasil <i>backup</i> yang terpisah oleh masing-masing <i>administrator</i> baik dari unit atau Subdit Pengembangan, namun hal ini diluar ruang lingkup SMKI.</p>                                                                                                                                                                                                                                                                                                                                                                                                |
| C                                       | <p>Untuk perlindungan hasil <i>backup</i> secara fisik, DPTSI-ITS menaruh <i>server backup</i> didalam ruangan pusat data yang dilindungi oleh pintu dengan kunci <i>finger print</i>, <i>CCTV</i>, dan lainnya berdasarkan kontrol A.11.1.2. Kontrol keluar-masuk fisik.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| NC                                      | <p>Untuk ujicoba hasil <i>backup</i>, DPTSI-ITS tidak melakukan ujicoba <i>backup</i> secara berkala karena terdapat keyakinan bahwa data yang disimpan dalam media <i>backup</i> dapat melakukan restorasi data secara lengkap jika terjadi masalah. DPTSI-ITS juga tidak memiliki dokumentasi prosedur pengawasan dan pengujian hasil <i>backup</i> yang berisikan pemeriksaan aktifitas <i>backup</i> dan kegagalan yang terjadi, pengujian hasil <i>backup</i> kedalam sistem untuk pengujian, dan penilaian hasil uji coba berdasarkan data yang berhasil dipulihkan.</p>                                                                                                                                                                                                                                                                                                 |
| NC                                      | <p>Untuk perlindungan kriptografi pada hasil <i>backup</i> yang memerlukan kerahasiaan yang tinggi, DPTSI-ITS tidak menggunakan kriptografi pada <i>hardisk</i> didalam <i>server</i> maupun <i>server backup</i> berdasarkan kontrol A.10.1.1. Kebijakan dalam penggunaan kontrol kriptografi.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>A.12.4. Perekaman dan pengawasan</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |



|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                            |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.12.4.1 | Mencatat kejadian                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <i>Partially compliant</i> |
|          | Apakah <i>log</i> yang merekam aktifitas pengguna, <i>error</i> dan kejadian keamanan informasi lainnya dibuat, disimpan dan ditinjau secara berkala?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
| PC       | DPTSI-ITS menggunakan <i>SIEM</i> buatan AlienVault yang beralamatkan di website <a href="https://av.noc.its.ac.id">https://av.noc.its.ac.id</a> . <i>SIEM</i> AlienVault mengumpulkan <i>file log</i> dengan bantuan <i>agent</i> yang dipasang disetiap <i>server</i> baik untuk sistem informasi terpadu, <i>proxy</i> ITS, <i>DNS</i> dan lainnya. <i>Log</i> yang disimpan adalah operasional dan keamanan yang terjadi didalam <i>folder</i> “var/log” pada <i>server</i> , lalu dianalisa dan dilaporkan oleh <i>SIEM</i> secara ringkas melalui <i>dashboard</i> . Laporan tersebut dapat berupa banyaknya serangan <i>cyber</i> dan jenisnya yang terjadi, aktifitas yang dilakukan didalam infrastruktur jaringan ITS, kerentanan sistem yang ada, jumlah <i>error</i> yang terjadi pada sistem, dan lainnya. Lamanya penyimpanan <i>file log</i> adalah 1 tahun yang penghapusannya dilakukan secara otomatis oleh sistem. Namun <i>SIEM</i> tidak mencakup komputer/laptop dinas dan <i>server development</i> . <i>SIEM</i> dapat dilihat pada <b>Gambar F.118</b> sampai <b>Gambar F.122</b> . |                            |
| A.12.4.2 | Perlindungan informasi <i>log</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <i>Compliant</i>           |
|          | Apakah informasi <i>log</i> dan fasilitas pendukungnya dilindungi dari pengubahan dan akses tanpa izin?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                            |
| C        | DPTSI-ITS memiliki <i>SIEM</i> yang menyimpan <i>file log</i> dari berbagai <i>server</i> didalam infrastruktur jaringan ITS secara terpusat berdasarkan kontrol A.12.4.1. Mencatat kejadian. <i>SIEM</i> juga melindungi <i>file log</i> yang disimpan dari perubahan atau penghapusan tanpa izin karena diharuskan autentikasi terlebih dahulu untuk mengakses <i>SIEM</i> yang dapat dilihat pada <b>Gambar F.118</b> , serta memudahkan dalam melakukan <i>backup</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
| A.12.4.3 | <i>Log administrator</i> dan petugas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <i>Non-compliant</i>       |
|          | Apakah setiap aktifitas <i>administrator</i> sistem direkam dan setiap <i>log</i> dilindungi dan ditinjau secara berkala?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                            |
| NC       | <ul style="list-style-type: none"> <li>Tidak adanya rekaman aktifitas <i>administrator</i> pada Webmail ITS seperti menambah, me-reset dan menghapus akun <i>email</i> yang dimiliki pengguna.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                            |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                     |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| NC<br>(lanj.)                               | <ul style="list-style-type: none"> <li>Tidak adanya perlindungan <i>log</i> dari perubahan yang dilakukan <i>administrator</i> ataupun rekaman aktifitas <i>administrator</i> pada <i>server</i> dan perangkat jaringan. Hal ini dikarenakan berdasarkan kontrol A.9.2.3. Manajemen hak akses <i>administrator</i>, DPTSI-ITS tidak mengatur tingkatan hak akses <i>administrator</i> pada setiap <i>server</i> dan perangkat jaringan yang menjadi tanggung jawab masing-masing.</li> </ul>                                                                                                                  |                     |
| A.12.4.4                                    | Sinkronisasi jam                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Partially compliant |
|                                             | Apakah semua jam pada semua sistem pemrosesan informasi disinkronisasikan kedalam satu referensi yang sama?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                     |
| PC                                          | Untuk sinkronisasi jam pada sumber yang sama, semua <i>server</i> baik <i>VPS</i> atau <i>dedicated</i> dan perangkat jaringan seperti <i>firewall</i> , <i>router</i> , dan perangkat jaringan lainnya diatur agar jamnya disinkronisasikan dengan acuan yang sama melalui protokol <i>NTP</i> . Subdit Infrastruktur menjadikan <i>server DNS</i> yang digunakan sebagai acuan sinkronisasi jam. . <i>Server DNS</i> menggunakan perangkat lunak BIND yang berlisensi <i>open source</i> . Namun tidak semua diatur oleh protokol <i>NTP</i> , seperti <i>server development</i> dan komputer/laptop dinas. |                     |
| NA                                          | Untuk dokumentasi persyaratan yang dibuat untuk pengaturan, sinkronisasi dan keakuratan jam (berdasarkan peraturan/hukum, perjanjian kontrak, standar atau kebutuhan internal), DPTSI-ITS tidak mendokumentasikannya karena tidak ada sumber acuan yang mengharuskannya.                                                                                                                                                                                                                                                                                                                                      |                     |
| A.12.5. Kontrol perangkat lunak operasional |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                     |
| A.12.5.1                                    | Pemasangan perangkat lunak pada sistem operasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Partially compliant |
|                                             | Apakah prosedur diterapkan untuk mengontrol pemasangan perangkat lunak pada sistem operasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                     |
| PC                                          | Untuk peran dan tanggung jawab dalam pemasangan perangkat lunak, DPTSI-ITS mengizinkan hanya untuk orang tertentu saja pada <i>server</i> . Misalnya <i>administrator</i> baik dari Subdit Infrastruktur, Subdit Pengembangan atau/dan unit lain di ITS yang memiliki akses ke <i>server dedicated</i> atau <i>VPS</i> . Namun untuk pemasangan perangkat lunak pada komputer/laptop dinas, siapapun bisa memasang, memperbaharui atau menghapus perangkat lunak pada komputer yang digunakan.                                                                                                                |                     |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NA | Untuk pembatasan <i>development code</i> atau <i>compiler</i> aplikasi yang dikembangkan berjalan di sistem operasional, DPTSI-ITS hanya mengembangkan sistem informasi berbasis <i>web</i> . Jadi kode program dapat dilihat baik didalam <i>server live</i> atau <i>server development</i> jika pengguna memiliki hak aksesnya.                                                                                                                      |
| C  | Untuk pengujian sistem, DPTSI-ITS melakukan pengujian secara terpisah yang dilakukan di <i>server development</i> berdasarkan kontrol A.14.2.9. Pengujian penerimaan sistem. Selain itu semua perubahan sistem operasi dan aplikasi pendukung lainnya diuji terlebih dahulu sebelum dioperasikan dilingkungan yang terpisah dari lingkungan operasional berdasarkan kontrol A.14.2.3. Tinjauan teknis pada aplikasi setelah dilakukan perubahan dasar. |
| NC | Untuk sistem manajemen konfigurasi, DPTSI-ITS tidak menggunakan perangkat lunak apapun untuk mengontrol semua konfigurasi sistem.                                                                                                                                                                                                                                                                                                                      |
| C  | Untuk strategi pengembalian kekeadaan semula, DPTSI-ITS melakukan pemasangan kembali versi lama perangkat lunak jika perangkat lunak baru tidak sesuai dengan yang diharapkan atau terdapat <i>error</i> /konflik terhadap sistem lainnya.                                                                                                                                                                                                             |
| C  | Untuk rekaman riwayat pembaharuan <i>program library</i> untuk sistem yang dikembangkan, DPTSI-ITS menggunakan sistem Git ITS yang memiliki fungsi penyimpanan perubahan <i>source code</i> dan file pendukung lainnya berdasarkan kontrol A.9.4.5. Kontrol akses ke <i>source code</i> perangkat lunak.                                                                                                                                               |
| PC | Untuk penyimpanan perangkat lunak sebelumnya, DPTSI-ITS menyimpan perangkat lunak sebelumnya. Namun tidak adanya catatan lengkap yang berisikan informasi perangkat lunak, prosedur, dan rincian konfigurasi.                                                                                                                                                                                                                                          |
| NC | DPTSI-ITS tidak memiliki dokumentasi kebijakan pemasangan dan penghapusan perangkat lunak yang berisikan peran dan tanggung jawab karyawan, aturan pemasangan perangkat lunak pada komputer dan <i>server</i> , apa yang harus disimpan dan dilakukan ketika pemasangan, dan lainnya.                                                                                                                                                                  |
| PC | DPTSI-ITS memiliki prosedur untuk pemasangan sistem informasi baru/perubahan berdasarkan kontrol A.14.2.2. Prosedur kontrol perubahan sistem. Namun DPTSI-ITS tidak memiliki dokumentasi prosedur pemasangan atau penghapusan perangkat lunak yang tidak dikembangkan DPTSI-ITS yang berisikan langkah-langkah dalam pemasangan, pengujian atau penghapusan perangkat lunak pada komputer dan <i>server</i> .                                          |

| A.12.6. Manajemen kerentanan teknis |                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                            |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.12.6.1                            | Manajemen kerentanan teknis                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Partially compliant</i> |
|                                     | Apakah informasi tentang kerentanan teknis pada sistem informasi didapatkan pada waktu tertentu dan dilakukan tindak lanjutnya (seperti <i>patch</i> ) untuk mengacu pada resiko yang terkait?                                                                                                                                                                                                                                                                               |                            |
| NC                                  | Untuk peran dan tanggung jawab dalam manajemen kerentanan teknis, DPTSI-ITS belum menetapkannya secara khusus (manajemen <i>patch/update</i> pada perangkat keras/lunak/jaringan), namun tanggung jawab secara <i>default</i> sudah melekat ke karyawan masing-masing yang mengurus atau memiliki akses kedalam perangkat tersebut. Misalnya karyawan yang bertanggung jawab terhadap <i>firewall</i> , maka dia yang bertanggung jawab terhadap <i>patch firmware</i> -nya. |                            |
| NC                                  | Untuk identifikasi kerentanan, DPTSI-ITS tidak mengawasi kerentanan baru melalui forum/ <i>website</i> keamanan informasi ataupun mengawasi rilis terbaru <i>patch/update</i> dari <i>website</i> vendor (baik menggunakan perangkat lunak yang memberitahukan <i>patch/update</i> terbaru atau dilakukan manual) secara berkala dan terjadwal.                                                                                                                              |                            |
| NC                                  | Untuk identifikasi dan penanganan resiko terkait kerentanan yang ditemukan, DPTSI-ITS tidak melakukan identifikasi dan penanganan resiko ketika kerentanan telah teridentifikasi. Hal ini dikarenakan DPTSI-ITS masih belum menggunakan manajemen resiko berdasarkan kontrol A.6.1.5. Manajemen proyek untuk keamanan informasi.                                                                                                                                             |                            |
| NC                                  | Untuk resiko yang ada ketika memasang <i>patch</i> , DPTSI-ITS tidak membandingkan resiko yang ada ketika memasang <i>patch</i> dengan kerentanan yang ada.                                                                                                                                                                                                                                                                                                                  |                            |
| C                                   | Untuk pengujian <i>patch</i> , DPTSI-ITS melakukan ujicoba sebelum pemasangan <i>patch</i> untuk melihat apakah <i>patch</i> terbaru memiliki efek samping. Jika terdapat efek samping sampai mengganggu sistem informasi yang penting maka tetap menggunakan versi yang lama.                                                                                                                                                                                               |                            |

|                                             |                                                                                                                                                                                                                                                                                                  |                      |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| NC                                          | Untuk riwayat aktifitas pemasangan <i>patch</i> , DPTSI-ITS tidak merekam perangkat lunak apa saja yang sudah dan yang belum diberikan <i>patch</i> , serta yang bermasalah dalam pemberian <i>patch</i> (memiliki efek samping) dan penanggulangannya.                                          |                      |
| NC                                          | Untuk penyamaan antara aktifitas manajemen kerentanan teknis dengan aktifitas manajemen insiden, DPTSI-ITS belum melakukannya karena dokumen kebijakan dan prosedur manajemen kerentanan teknis masih belum didokumentasikan dan direncanakan untuk penambahan informasi ketika terjadi insiden. |                      |
| NC                                          | Untuk dokumentasi kebijakan manajemen kerentanan teknis, DPTSI-ITS tidak memiliki dokumentasi kebijakan yang berisikan peran dan tanggung jawab karyawan, aturan pengawasan kerentanan dan pembaharuan <i>patch</i> , dan lainnya.                                                               |                      |
| NC                                          | Untuk dokumentasi prosedur manajemen kerentanan teknis, DPTSI-ITS tidak memiliki dokumentasi prosedur yang berisikan langkah-langkah dalam manajemen <i>patch</i> (termasuk kerentanan yang telah teridentifikasi namun belum memenuhi penanganan yang tepat).                                   |                      |
| A.12.6.2                                    | Pembatasan pemasangan perangkat lunak                                                                                                                                                                                                                                                            | <i>Non-compliant</i> |
|                                             | Apakah peraturan untuk mengatur pemasangan perangkat lunak oleh pengguna dibuat dan diterapkan?                                                                                                                                                                                                  |                      |
| NC                                          | DPTSI-ITS tidak memiliki dokumentasi kebijakan pembatasan penggunaan perangkat lunak yang berisikan rincian perangkat lunak apa saja yang boleh dipasang dan yang tidak boleh dipasang, jadi setiap karyawan dapat bebas memasang dan menghapus perangkat lunak.                                 |                      |
| A.12.7. Pertimbangan audit sistem informasi |                                                                                                                                                                                                                                                                                                  |                      |
| A.12.7.1                                    | Kontrol audit sistem informasi                                                                                                                                                                                                                                                                   | <i>Non-compliant</i> |
|                                             | Apakah persyaratan dan aktifitas audit termasuk memastikan sistem operasional (audit sistem informasi) untuk mengurangi gangguan pada proses bisnis?                                                                                                                                             |                      |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |           |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| NC                                  | DPTSI-ITS tidak pernah mengadakan aktifitas audit atau evaluasi terhadap sistem informasi yang dimiliki, selain itu juga DPTSI-ITS tidak memiliki dokumentasi prosedur audit sistem informasi yang berisikan langkah-langkah dalam audit sistem informasi secara internal.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |           |
| A.13. Keamanan Komunikasi           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |           |
| A.13.1. Manajemen keamanan jaringan |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |           |
| A.13.1.1                            | Kontrol jaringan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Compliant |
|                                     | Apakah jaringan diurus dan dikontrol untuk melindungi informasi didalam sistem dan aplikasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |
| C                                   | Untuk peran dan tanggung jawab dalam manajemen dan operasional infrastruktur jaringan, DPTSI-ITS menetapkan Subdit Infrastruktur secara khusus. Jumlah Subdit Infrastruktur adalah 8 orang yang terdiri dari Kasubdit Infrastruktur, karyawan pengembang jaringan dan pangkalan data (yang dibagi menjadi administrasi jaringan, administrasi sistem, dan administrasi kelistrikan), dan karyawan penyusun laporan dan pengelola BMN.                                                                                                                                                                                                                                                                                                                                                                                                                                       |           |
| C                                   | Untuk pemisahan peran dan tanggung jawab dalam operasional infrastruktur jaringan dengan operasional komputer, Subdit Infrastruktur tidak bertanggung jawab terhadap operasional komputer dan laptop yang ada, seperti pemasangan sistem dan pengaturannya. Hal ini dikarenakan yang bertanggung jawab adalah Subdit Pelayanan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |           |
| C                                   | <p>Untuk dokumentasi prosedur pengelolaan jaringan, Subdit infrastruktur memiliki:</p> <ul style="list-style-type: none"> <li>• Prosedur Instalasi Jaringan Baru yang digunakan untuk pemasangan jaringan baru di lingkungan ITS. Prosedur ini dapat dilihat pada <b>Gambar F.160</b>.</li> <li>• Prosedur <i>Monitoring</i> Jaringan yang digunakan untuk mengawasi kondisi jaringan. Aktifitas pengawasan dilakukan dengan bantuan Nagios dan ITS Web Monitoring System. Jika terdapat gangguan maka Subdit Infrastruktur akan melakukan <i>troubleshooting</i> seperti jika perangkat tidak menyala maka akan dinyalakan, jika terjadi <i>error</i> pada perangkat maka akan dilakukan <i>reset</i>, jika kabel tidak terpasang maka akan dipasang, dan jika layanan aplikasi mati maka akan dilaporkan. Prosedur ini dapat dilihat pada <b>Gambar F.123</b>.</li> </ul> |           |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C<br>(lanj.) | <ul style="list-style-type: none"> <li>• Prosedur Pemeriksaan Jaringan Setelah Listrik Mati yang digunakan untuk memeriksa <i>server</i>, sistem informasi dan perangkat jaringan setelah terjadi pemadaman listrik. Prosedur ini dapat dilihat pada <b>Gambar F.153</b>.</li> <li>• Prosedur Instalasi <i>Access Point</i> yang digunakan untuk memasang <i>access point</i>/Wifi secara benar di setiap unit/jurusan. Prosedur ini dapat dilihat pada <b>Gambar F.161</b>. Prosedur Pelebaran <i>Bandwith</i> yang digunakan untuk menambah <i>bandwith internet</i> bagi pengguna yang memerlukan <i>bandwith</i> lebih untuk acara khusus. Prosedur ini dapat dilihat pada <b>Gambar F.162</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| C            | <p>Untuk melindungi jaringan <i>intranet</i> dan <i>internet</i> dilingkungan ITS dari ancaman akses tanpa izin, <i>malware</i>, <i>hacking</i> dan lainnya, Subdit Infrastruktur menggunakan kontrol keamanan berlapis seperti:</p> <ul style="list-style-type: none"> <li>• CISCO ASA Firewall 5540 adalah perangkat jaringan <i>firewall</i> yang diatur agar <i>default</i>-nya membatasi semua <i>port</i> dan hanya memperbolehkan <i>port</i> tertentu saja, seperti memperbolehkan <i>port</i> yang digunakan <i>HTTP/HTTPS</i>, <i>SMTP</i>, <i>POP3</i>, <i>IMAP</i>, <i>SNMP</i>, <i>NTP</i>, dan lainnya yang digunakan. Sedangkan untuk <i>port</i> aneh dan tidak aman digunakan seperti <i>FTP</i>, <i>P2P</i> dan lainnya tidak diperbolehkan. Perangkat ini hanya berfungsi sebagai <i>firewall</i>, meskipun terdapat fitur <i>VPN</i>, <i>anti-virus</i>, <i>anti-spam</i>, <i>IPS</i> dan <i>IDS</i> yang perlu dibeli masing-masing lisensinya. Selain itu Subdit infrastruktur juga menggunakan <i>firewall</i> berupa perangkat lunak yang berjalan pada sistem operasi Linux bernama ShoreWall, namun penggunaanya hanya untuk mengamankan SIM saja. CISCO ASA Firewall dapat dilihat pada <b>Gambar F.124</b> dan <b>Gambar F.125</b>.</li> <li>• <i>Honeypot</i> Dionaee adalah <i>server</i> yang menangani dan mengkarantina serangan <i>malware</i> yang mengeksploitasi kerentanan pada layanan yang disediakan melalui jaringan ITS. Perangkat ini melakukan aktifitas pengawasan secara <i>realtime</i> pada setiap asal koneksi dan <i>IP address</i> yang terhubung dan penanganan secara langsung jika terjadi serangan. <i>Honeypot</i> merupakan kerjasama dengan KEMENKOMINFO dan dapat dilihat pada <b>Gambar F.126</b>.</li> <li>• Tsubame (<i>internet threat monitoring system</i>) adalah <i>server</i> untuk sensor <i>CSIRT</i> dikawasan Asia Pasifik yang berfungsi untuk pengawasan ancaman <i>internet</i> (contohnya infeksi <i>worm</i> ataupun investigasi kerentanan sistem), saling berbagi informasi dan analisisnya, dan meningkatkan kolaborasi antara <i>CSIRT</i> dengan menggunakan <i>platform</i> yang sama. Jika terjadi serangan <i>cyber</i> didalam infrastruktur jaringan ITS maka akan dikirimkan</li> </ul> |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C | <p>informasinya melalui <i>email</i> ke Subdit Infrastruktur. <i>CSIRT</i> juga menyampaikan tren kondisi jaringan secara umum dikawasan Asia Pasifik, informasi untuk meningkatkan kewaspadaan, dan daftar kerentanan berikut penanganannya yang berdasarkan hasil analisa semua data dari organisasi yang bekerjasama dengan tim <i>CSIRT</i>. Tsubame merupakan kerjasama dengan KEMENKOMINFO dan dapat dilihat pada <b>Gambar F.127</b>.</p> <ul style="list-style-type: none"> <li>• Sangfor Internet Access Management (<i>IAM</i>) adalah perangkat jaringan yang digunakan untuk mengatur dan memaksimalkan penggunaan <i>bandwith</i> yang digunakan, serta melihat laporan penggunaan/kebiasaan pada trafik <i>internet</i>, seperti <i>email</i>, aplikasi <i>chat</i>, media sosial. Berdasarkan kontrol A.12.1.3. Manajemen kapasitas, Subdit Infrastruktur membatasi <i>bandwith</i> media sosial dan media <i>streaming</i> dengan perangkat ini. Selain itu perangkat ini digunakan untuk memblokir <i>website</i> yang berbahaya ataupun yang melanggar hukum. <i>IAM</i> dapat dilihat pada <b>Gambar F.128</b> dan <b>Gambar F.129</b>.</li> <li>• <i>Proxy</i> ITS adalah <i>server</i> yang berfungsi sebagai perantara jaringan ITS dengan koneksi luar, pemblokiran <i>IP address</i> tertentu, dan penyimpanan <i>cache</i> riwayat halaman <i>website</i>. Semua sistem yang ingin mendapatkan koneksi <i>internet</i> diarea kampus dapat mengatur pengaturan <i>proxy</i> di <i>browser</i> dan memasukkan alamat dan <i>password email</i> ITS. <i>Proxy</i> ITS menggunakan perangkat lunak Squid yang berlisensi <i>open source</i>. <i>Proxy</i> ITS dapat dilihat pada <b>Gambar F.130</b>.</li> </ul> |
| C | <p>Untuk menjaga <i>confidentiality</i> dan <i>integrity</i> dari data melalui jaringan <i>intranet</i> dan <i>internet</i> dilingkungan ITS, Subdit Infrastruktur menggunakan koneksi <i>VPN</i> dan protokol <i>TLS</i> berdasarkan kontrol A.10.1.1. Kebijakan dalam penggunaan kontrol kriptografi.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| C | <p>Untuk menjaga <i>availability</i> dari jaringan <i>intranet</i> dan <i>internet</i> dilingkungan ITS, Subdit Infrastruktur menggunakan beberapa kontrol keamanan seperti:</p> <ul style="list-style-type: none"> <li>• Nagios merupakan sistem informasi yang mengawasi kondisi operasional keseluruhan perangkat jaringan seperti <i>switch</i> dan <i>fingerprint</i> yang dipasang di setiap unit/jurusan didalam lingkungan ITS secara <i>realtime</i>. Hasil dari laporan ditampilkan menggunakan TV LCD yang diletakkan didalam ruangan Subdit Infrastruktur. Nagios dapat dilihat pada <b>Gambar F.131</b>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                  |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| C<br>(lanj.) | <ul style="list-style-type: none"> <li>• ITS Web Monitoring System merupakan sistem informasi yang digunakan untuk menampilkan kondisi <i>up</i> atau <i>down</i> perangkat <i>server</i> yang dikelola oleh DPTSI-ITS secara <i>realtime</i>. Hasil dari laporan perangkat tersebut ditampilkan menggunakan TV LCD yang diletakkan didalam ruangan Subdit Pelayanan. ITS Web Monitoring System dapat dilihat pada <b>Gambar F.132</b>.</li> <li>• Cacti merupakan sistem informasi yang memonitor dan melaporkan kondisi ataupun beban trafik didalam infrastruktur jaringan di ITS yang disajikan kedalam grafik yang dikelompokkan berdasarkan waktu berdasarkan kontrol A.12.1.3. Manajemen kapasitas. Cacti dapat dilihat pada <b>Gambar F.111</b>.</li> </ul> |                  |
| C            | <p>Untuk perekaman <i>log</i> dan pengawasan untuk merekam dan mendeteksi aktifitas, DPTSI-ITS menggunakan <i>SIEM</i> AlienVault yang merupakan sistem informasi yang menyimpan <i>file log</i> dari berbagai <i>server</i> secara terpusat berdasarkan kontrol A.12.4.1. Mencatat kejadian. <i>Log</i> yang disimpan tadi dianalisa dan dilaporkan secara ringkas, seperti serangan <i>cyber</i> yang terjadi, aktifitas yang dilakukan didalam infrastruktur jaringan ITS, kerentanan sistem yang ada, jumlah <i>error</i> yang terjadi pada sistem, dan lainnya. <i>SIEM</i> dapat dilihat pada <b>Gambar F.118</b> sampai <b>Gambar F.122</b>.</p>                                                                                                             |                  |
| C            | <p>Untuk meningkatkan layanan dan memastikan kontrol keamanan terpasang secara konsisten pada infrastruktur TIK, Subdt Infrastruktur bekerjasama dengan Subdit Pelayanan dalam masalah penerimaan keluhan pada sistem dan jaringan, dan penanganannya.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                  |
| C            | <p>Untuk mengautentikasi sistem didalam jaringan, pengguna diperlukan aktifitas autentikasi dengan <i>SSO</i> atau pengaturan <i>proxy</i> pada perangkat yang dimiliki berdasarkan kontrol A.9.1.2. Akses ke jaringan dan layanan jaringan.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                  |
| C            | <p>Untuk membatasi koneksi ke jaringan ITS, Subdit Infrastruktur menggunakan CISCO ASA Firewall 5540. Pembatasannya seperti siapa yang boleh mengakses berdasarkan <i>IP address</i>, dan apa saja sistem atau perangkat yang bisa diakses berdasarkan jenis domain (<i>DMZ</i> atau <i>private</i>).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                  |
| A.13.1.2     | Keamanan layanan jaringan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <i>Compliant</i> |
|              | <p>Apakah mekanisme keamanan, tingkat layanan dan kebutuhan manajemen dispesifikasikan dan dimasukkan kedalam perjanjian kontrak dengan <i>Internet Service Provider (ISP)</i>?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                  |

|                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                         |                  |                                                                                                  |  |
|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|------------------|--------------------------------------------------------------------------------------------------|--|
| C                                                                                                | <p>Untuk keamanan yang diperlukan oleh DPTSI-ITS pada layanan <i>ISP</i>, DPTSI-ITS sudah mengidentifikasi dan memasukkannya pada <i>Service Level Agreement (SLA)</i>. DPTSI-ITS menggunakan satu <i>ISP</i> yaitu PT. Telkom. <i>ISP</i> yang digunakan memiliki dua jalur, yaitu IP transit yang utama dan Astine sebagai <i>backup</i> jika yang utama gagal. Didalam <i>SLA</i> yang dibuat DPTSI-ITS dengan PT. Telkom mensyaratkan layanan <i>ISP</i> harus mampu memberikan layanan <i>up</i> sebesar 99.75% dan tempat untuk <i>disaster recovery center</i>. Selain itu fitur keamanan yang disyaratkan adalah <i>anti-virus</i>, <i>anti-spam</i> dan <i>anti-DDoS</i>. Jadi ancaman <i>spam</i>, <i>virus</i> dan paket <i>DDoS</i> yang dikirimkan dari luar kedalam jaringan ITS melalui <i>ISP</i> disyaratkan untuk dilakukan <i>filter</i> oleh <i>ISP</i>. Jadi ancaman tersebut tidak akan memakan <i>bandwidth</i> dan mengganggu jaringan ITS meskipun DPTSI-ITS bisa melakukan <i>filter</i> sendiri.</p> <p>Selain itu layanan lain yang sudah termasuk dalam paket <i>ISP</i> adalah InternetPositif dan <i>VPN</i> IndiHome. InternetPositif merupakan fitur yang memblokir <i>website</i> yang mengandung muatan berbahaya seperti <i>malware</i>, penipuan/<i>fraud</i> dan lainnya, dan yang mengandung muatan yang melanggar peraturan/hukum di Indonesia dan negatif seperti berbau pornografi, pelanggaran hak cipta, sara dan lainnya. Sedangkan <i>VPN</i> IndiHome merupakan layanan untuk jalur koneksi aman dengan enkripsi yang tersedia didalam infrastruktur jaringan ITS. InternetPositif dapat dilihat pada <b>Gambar F.133</b>.</p> |                         |                  |                                                                                                  |  |
| C                                                                                                | <p>Untuk penentuan kemampuan dan peninjauan berkala layanan <i>ISP</i> vendor, DPTSI-ITS penentuan kemampuan layanan <i>ISP</i> sudah dilakukan berdasarkan hal diatas, sedangkan peninjauan atau audit juga dilakukan berdasarkan kontrol A.15.2.1. Mengawasi dan meninjau layanan vendor.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                         |                  |                                                                                                  |  |
| A.13.1.3                                                                                         | <table border="1"> <tr> <td data-bbox="391 1370 1157 1435">Pemisahan pada jaringan</td><td data-bbox="1157 1370 1375 1435"><i>Compliant</i></td></tr> <tr> <td colspan="2" data-bbox="391 1435 1375 1543">Apakah beberapa grup layanan informasi, pengguna dan sistem informasi dipisahkan dalam jaringan?</td></tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Pemisahan pada jaringan | <i>Compliant</i> | Apakah beberapa grup layanan informasi, pengguna dan sistem informasi dipisahkan dalam jaringan? |  |
| Pemisahan pada jaringan                                                                          | <i>Compliant</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                         |                  |                                                                                                  |  |
| Apakah beberapa grup layanan informasi, pengguna dan sistem informasi dipisahkan dalam jaringan? |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                         |                  |                                                                                                  |  |
|                                                                                                  | <p>Banyak domain yang dibuat pada infrastruktur jaringan di ITS, contohnya adalah domain <i>server farm</i> (untuk tempat <i>server co-location</i>), domain <i>DMZ</i> (untuk <i>server DNS</i>, <i>proxy</i> ITS, Webmail ITS, ITS Web Monitoring System, <i>SIEM</i> AlienVault, Open <i>VPN</i>, Git ITS, dan lainnya), domain rektorat, domain arsitektur, domain sistem informasi, domain informatika, domain siskal, domain teknik fisika, domain statistika dan lainnya. Selain itu Subdit Infrastruktur mengatur agar sistem tertentu hanya bisa diakses melalui jaringan ITS (tidak bisa diakses dari luar) dengan sebutan <i>private</i>. Contoh</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                         |                  |                                                                                                  |  |

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                     |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| C<br>(lanj.)                 | <p>sistem yang menggunakan konfigurasi <i>privat</i> adalah Nagios, sinkronisasi <i>database server</i>, sinkronisasi <i>database</i> jaringan, dan lainnya. Contoh akses dari luar ke sistem dengan domain <i>privat</i> dapat dilihat pada <b>Gambar F.135</b>.</p> <p>Konfigurasi <i>subnet</i> jaringan terbesar berada pada 10.x.0.0/16 dengan <i>subnet mask</i> 255.255.0.0 yang kemudian dibagi-bagi lagi sesuai kebutuhan, sehingga unit/jurusan di ITS memiliki <i>subnet</i> tersendiri dan dapat mengembangkan jaringannya. Topologi jaringan ITS mengadopsi topologi STAR dan RING, dokumentasinya dapat dilihat pada <b>Gambar 4.10</b>.</p> |                     |
| A.13.2. Pertukaran informasi |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                     |
| A.13.2.1                     | Kebijakan dan prosedur pertukaran informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Partially compliant |
|                              | Apakah kebijakan, prosedur dan kontrol keamanan diterapkan untuk melindungi pertukaran informasi melalui semua tipe fasilitas komunikasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                     |
| NC                           | DPTSI-ITS tidak memiliki dokumentasi kebijakan pertukaran informasi yang berisikan aturan bertukar informasi yang aman (cara pertukaran informasi, saran untuk mencegah agar tidak menyingkap informasi rahasia, larangan berbincang masalah kantor yang rahasia di public, dan lainnya).                                                                                                                                                                                                                                                                                                                                                                  |                     |
| NC                           | DPTSI-ITS tidak memiliki dokumentasi prosedur pertukaran informasi yang melindungi informasi dari intersepsi, penyalinan, modifikasi, pengalihan dan perusakan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                     |
| NC                           | DPTSI-ITS tidak memiliki dokumentasi prosedur perlindungan informasi <i>email</i> sensitif berupa <i>attachement</i> yang berisikan langkah-langkah dalam pengamanan <i>attachement</i> sebelum dikirimkan ke penerima.                                                                                                                                                                                                                                                                                                                                                                                                                                    |                     |
| C                            | Untuk melindungi pertukaran informasi dari ancaman <i>virus/malware</i> berdasarkan kontrol A.12.2.1. Kontrol terhadap <i>malware</i> , DPTSI-ITS menggunakan ClamAV dan Windows Defender. Selain itu berdasarkan kontrol A.13.1.2. Keamanan layanan jaringan, ISP yang dipakai memiliki fitur <i>anti-spam</i> dan <i>anti-virus</i> .                                                                                                                                                                                                                                                                                                                    |                     |
| C                            | Untuk pembatasan fitur meneruskan pesan ke alamat <i>email</i> eksternal secara otomatis, Webmail ITS tidak memiliki fitur tersebut.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                     |

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                            |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <i>C</i>  | Untuk melindungi <i>confidentiality</i> dan <i>integrity</i> dari pertukaran informasi berdasarkan kontrol A.10.1.1. Kebijakan dalam penggunaan kontrol kriptografi, DPTSI-ITS menggunakan koneksi <i>VPS</i> dan protokol <i>TLS</i> .                                                                                                                                                                                                                                                                                                                  |                            |
| <i>NC</i> | Untuk perlindungan melalui perangkat <i>fax</i> , DPTSI-ITS tidak memiliki kebijakan penggunaan perangkat <i>fax</i> berdasarkan kontrol A.8.1.3. Persyaratan penggunaan aset.                                                                                                                                                                                                                                                                                                                                                                           |                            |
| A.13.2.2  | Perjanjian dalam pertukaran informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Non-compliant</i>       |
|           | Apakah perjanjian menyinggung pengiriman yang aman pada informasi bisnis diantara organisasi dengan pihak ketiga?                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
| <i>NC</i> | Tidak adanya perjanjian khusus untuk pertukaran informasi yang aman antara DPTSI-ITS dengan pihak ketiga. Meskipun terdapat sistem LPSE yang menjembatani pertukaran informasi yang aman antara ULP-ITS yang melakukan pengadaan barang/layanan yang dibutuhkan DPTSI-ITS dengan beberapa vendor barang/layanan, namun hal ini merupakan diluar ruang lingkup SMKI.                                                                                                                                                                                      |                            |
| A.13.2.3  | Pesan elektronik                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <i>Partially compliant</i> |
|           | Apakah informasi yang berhubungan dengan pesan elektronik dilindungi secara tepat?                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                            |
| <i>C</i>  | DPTSI-ITS memiliki layanan <i>email</i> yang dikelola mandiri oleh DPTSI-ITS, layanan <i>email</i> yang bekerjasama dengan Google dan layanan <i>email</i> yang bekerjasama dengan Microsoft. Untuk layanan <i>email</i> yang merupakan hasil kerjasama, maka standar keamanannya akan mengikuti yang disediakan oleh Google/Microsoft, seperti halaman <i>login</i> (khusus untuk Microsoft), protokol <i>TLS</i> yang digunakan, manajemen <i>password</i> , <i>backup</i> untuk data <i>email</i> , <i>anti-spam</i> , <i>anti-virus</i> dan lainnya. |                            |
| <i>PC</i> | Untuk melindungi layanan <i>email</i> dari <i>spam</i> , DPTSI-ITS memiliki beberapa kontrol keamanan seperti: <ul style="list-style-type: none"> <li>• Fortigate Anti-Spam adalah perangkat jaringan yang memiliki kemampuan menyaring semua <i>email</i> masuk yang dicurigai <i>spam</i> dan juga berbahaya. Fortigate Anti-Spam dapat dilihat pada <b>Gambar F.136</b>.</li> </ul>                                                                                                                                                                   |                            |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PC<br>(lanj.) | <ul style="list-style-type: none"> <li>• Layanan <i>ISP</i> yang digunakan sudah memiliki fitur <i>anti-spam</i> berdasarkan kontrol A.13.1.2. Keamanan layanan jaringan.</li> </ul> <p>Namun untuk mencegah <i>email spam</i> yang masuk pada Webmail ITS (khusus untuk <a href="https://webmail.its.ac.id">https://webmail.its.ac.id</a>) dari sisi aplikasinya tidak ada, seperti <i>filter</i> yang otomatis memasukkan <i>email</i> yang dicurigai <i>spam</i> kedalam <i>folder</i> khusus <i>spam</i>, ataupun tombol penanda <i>email spam</i> untuk pengguna gunakan yang dapat memasukkan <i>email</i> kedalam <i>folder</i> khusus <i>spam</i> dan memberitahukan <i>administrator</i>. Hal ini dapat dilihat pada <b>Gambar 4.3</b>.</p>                                                                                                                                                       |
| C             | <p>Untuk melindungi <i>integrity</i> dari layanan <i>email</i> (contohnya akses dan modifikasi tanpa izin), DPTSI-ITS memiliki beberapa kontrol keamanan seperti:</p> <ul style="list-style-type: none"> <li>• Mengatur agar Webmail ITS melakukan autentikasi terhadap pengguna berdasarkan kontrol A.9.1.2. Akses ke jaringan dan layanan jaringan.</li> <li>• Menggunakan protokol <i>TLS</i> untuk melindungi halaman <i>login</i> pada Webmail ITS berdasarkan kontrol A.10.1.1. Kebijakan dalam penggunaan kontrol kriptografi. Selain itu <i>port</i> yang digunakan <i>email client</i> atau perangkat <i>mobile</i> agar bisa terkoneksi dengan Webmail ITS juga terenkripsi, seperti untuk <i>server SMTP</i> adalah <i>TLS port</i> 465 atau <i>STARTTLS port</i> 587, untuk <i>server POP3</i> adalah <i>TLS port</i> 995, dan untuk <i>server IMAP</i> adalah <i>TLS port</i> 993.</li> </ul> |
| C             | <p>Untuk melindungi <i>availability</i> dari layanan <i>email</i> (contohnya <i>denial of service</i>), DPTSI-ITS memiliki beberapa kontrol keamanan seperti:</p> <ul style="list-style-type: none"> <li>• Melakukan <i>backup</i> terhadap <i>email</i> yang disimpan didalam <i>server</i>, serta terdapat <i>disaster recovery center</i> dan menggunakan konfigurasi komponen yang redundan pada <i>hardisk</i> dan <i>memory</i> didalam <i>server</i> tersebut berdasarkan kontrol A.12.3.1. <i>Backup</i> informasi dan kontrol A.17.2.1. Ketersediaan dari fasilitas pemrosesan informasi.</li> <li>• Menjaga <i>server</i> dan perangkat jaringan dari terhentinya pasokan listrik dengan <i>UPS</i> dan <i>diesel generator</i>, serta mengawasi hidup matinya perangkat tersebut dengan Nagios dan ITS Web Monitoring System berdasarkan kontrol A.11.2.2. Utilitas pendukung.</li> </ul>       |
| C             | <p>Untuk memastikan alamat penerima <i>email</i> benar dan kepastian pesan terkirim, Webmail ITS memiliki pemberitahuan jika alamat penerima <i>email</i> salah baik layanan <i>email</i> mandiri, Google dan Microsoft. Hal ini dapat dilihat pada <b>Gambar F.165</b>, <b>Gambar F.166</b> dan <b>Gambar F.167</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                            |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| NA       | Untuk penggunaan <i>digital signature</i> berdasarkan peraturan hukum, DPTSI-ITS tidak diharuskan menggunakannya karena tidak ada peraturan yang mengikat berdasarkan kontrol A.18.1.5. Peraturan untuk kontrol kriptografi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |
| NC       | Untuk perizinan penggunaan media sosial, DPTSI-ITS tidak memerlukan perizinan sebelum menggunakan layanan seperti Facebook, Twitter, WhatsApp, dan lainnya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                            |
| NC       | Untuk penggunaan autentikasi yang lebih kuat, DPTSI-ITS tidak memiliki autentikasi tambahan untuk mengontrol akses dari koneksi jaringan publik.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                            |
| A.13.2.4 | Perjanjian kerahasiaan atau tidak menyebarkan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <i>Partially compliant</i> |
|          | Apakah persyaratan untuk perjanjian kerahasiaan dan tidak-menyingskap informasi untuk melindungi informasi diidentifikasi, ditinjau dan didokumentasikan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                            |
| PC       | <p>Berdasarkan Peraturan Pemerintah nomor 53 tahun 2010 tentang disiplin karyawan PNS, setiap karyawan PNS diharuskan mengucapkan sumpah/janji sebelum penempatan kerja yang sebagian kalimatnya menyebut “bahwa saya akan memegang rahasia sesuatu yang menurut sifatnya atau menurut perintah harus saya rahasiakan”. PP 53/10 dapat dilihat pada <b>Gambar F.18</b> sampai <b>Gambar F.23</b>.</p> <p>Selain itu Subdit Pengembangan memiliki dokumen Kesepakatan Bersama Menjaga Kerahasiaan Aset Sistem Informasi Institusi Dilingkungan Kampus ITS yang membahas perjanjian kerahasiaan yang ditandatangani diatas materai oleh karyawan. Isi perjanjian kerahasiaan tersebut adalah informasi penanda tangan, sistem informasi yang dikelola, ketentuan/tanggung jawab penanda tangan, yang mengetahui (Kasubdit Pengembangan), dan sangsi jika melanggar. Tanggung jawab tersebut adalah mengharuskan karyawan menjaga kerahasiaan akun, data, <i>IP address</i> atau media yang berhubungan dengan informasi ke pihak yang tidak diizinkan, menjaga integritas dan keaslian data pada sistem informasi, menjaga agar akses pengguna yang legal tidak ditolak sistem informasi, dan menghapus dengan segera jika data tidak dipergunakan lagi. Dokumen ini dapat dilihat pada <b>Gambar F.137</b>.</p> |                            |

|                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                     |
|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| PC<br>(lanj.)                                      | Namun perjanjian menjaga kerahasiaan yang ada hanyalah sumpah/janji PNS bagi karyawan PNS dan dokumen Kesepakatan Bersama Menjaga Kerahasiaan Aset Sistem Informasi Institusi Dilingkungan Kampus ITS bagi Subdit Pengembangan. Tidak ada perjanjian menjaga kerahasiaan secara formal bagi karyawan lainnya.                                                                                                                                                                                                |                     |
| NC                                                 | Untuk peninjauan perjanjian kerahasiaan atau tidak menyebarkan informasi, Kesepakatan Bersama Menjaga Kerahasiaan Aset Sistem Informasi Institusi Dilingkungan Kampus ITS tidak ditinjau secara berkala, sedangkan peninjauan PP 53/10 merupakan tanggung jawab dari pemerintah.                                                                                                                                                                                                                             |                     |
| A.14. Akusisi, Pengembangan, Pemeliharaan Sistem   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                     |
| A.14.1. Persyaratan keamanan pada sistem informasi |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                     |
| A.14.1.1                                           | Analisa dan spesifikasi persyaratan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Partially compliant |
|                                                    | Apakah keamanan informasi yang berhubungan dengan persyaratan dimasukkan untuk sistem informasi baru atau pembaharuan?                                                                                                                                                                                                                                                                                                                                                                                       |                     |
| PC                                                 | Untuk isu keamanan yang dirujuk pada sistem baru atau pembaharuan, DPTSI-ITS merujuk beberapa isu keamanan informasi kedalam aktifitas manajemen proyek pengembangan sistem informasi berdasarkan kontrol A.6.1.5. Manajemen proyek untuk keamanan informasi. Selain itu metode                                                                                                                                                                                                                              |                     |
| PC<br>(lanj.)                                      | yang digunakan untuk mengidentifikasi persyaratan keamanan adalah mematuhi kebijakan atau hukum yang berlaku, peninjauan insiden yang pernah terjadi, kerentanan yang ditemukan atau dicurigai, dan wawancara dengan pengguna atau pelanggan.<br>Namun DPTSI-ITS tidak menggunakan manajemen resiko dan standar tertentu berdasarkan kontrol A.6.1.5. Manajemen proyek untuk keamanan informasi, ataupun memodelkan ancaman yang mungkin terjadi sebagai metode untuk mengidentifikasi persyaratan keamanan. |                     |
| PC                                                 | Untuk merefleksikan nilai bisnis dari informasi yang terkait, DPTSI-ITS memasukkan persyaratan keamanan informasi pada informasi sesuai klasifikasi yang dibuat berdasarkan kontrol A.8.2.1. Klasifikasi informasi. Namun klasifikasi tersebut belum terdokumentasikan.                                                                                                                                                                                                                                      |                     |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C | <p>Untuk waktu identifikasi persyaratan keamanan informasi, DPTSI-ITS melakukannya diawal proyek pengembangan ketika analis SI melakukan analisis proses bisnis, rancangan <i>database</i>, dan <i>user interface</i> dari data <i>user requirements</i> yang didapat.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| C | <p>Untuk identifikasi persyaratan keamanan, pengguna sistem biasanya tidak terlalu didefinisikan persyaratan keamanan. Hal ini karena yang banyak didefinisikan adalah proses bisnis dan fungsionalitas dari sistem. Prosedur untuk melihat persyaratan sistem dalam pembuatan sistem dapat dilihat pada <b>Gambar F.138</b>. Semua persyaratan yang didefinisikan oleh pengguna sudah memenuhi kebijakan atau hukum yang berlaku didalam dan diluar ITS, seperti SIM Keuangan harus mematuhi peraturan perpajakan, remunerasi, dan lainnya. Pengguna kebanyakan menyerahkan semua persyaratan keamanan kepada Subdit Pengembangan. Adapun persyaratan keamanan yang didefinisikan namun tidak sering terjadi seperti penggunaan <i>CAPTCHA</i> pada <i>form login</i>. Dalam hal ini, persyaratan yang dimasukkan kedalam sistem informasi baru atau pembaharuan oleh Subdit Pengembangan adalah:</p> <ul style="list-style-type: none"> <li>• Untuk menjaga tingkat kepercayaan pada identitas pengguna yang menggunakan sistem, dimasukkan persyaratan autentikasi hak akses pengguna dengan cara <i>login</i> berdasarkan kontrol A.9.1.2. Akses ke jaringan dan layanan jaringan.</li> <li>• Untuk proses menyediakan hak akses, dimasukkan manajemen hak akses pengguna yang mengatur hak akses yang tersedia pada sistem dan juga proses pemberian hak akses ke pengguna.</li> <li>• Untuk menginformasikan pengguna dalam penggunaan sistem, dimasukkan persyaratan aktifitas sosialisasi pelatihan sistem dan pembuatan <i>User Guide</i> berdasarkan berdasarkan kontrol A.7.2.2. Kesadaran, pendidikan dan pelatihan keamanan informasi dan kontrol A.14.2.2. Prosedur kontrol perubahan sistem.</li> <li>• Untuk menjaga dari kesalahan/<i>bug</i> pada <i>source code</i>, dimasukkan persyaratan pembuatan <i>Developer Guide</i> yang berisikan penjelasan <i>source code</i> dan <i>database</i> dengan penggambaran diagramnya yang membantu <i>programmer</i> selanjutnya dalam pengembangan sistem berdasarkan kontrol A.14.2.2. Prosedur kontrol perubahan sistem.</li> </ul> |



|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                       |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| C<br>(lanj.) | <ul style="list-style-type: none"> <li>• Untuk menjaga <i>confidentiality</i> dan <i>integrity</i> informasi, dimasukkan persyaratan klasifikasi informasi, termasuk data/informasi mana saja yang boleh diakses atau dirubah, atau <i>form</i> atau menu pada sistem mana saja yang tersedia untuk pengguna dengan hak akses tertentu.</li> <li>• Untuk menjaga <i>availability</i> informasi, dimasukkan persyaratan fitur <i>backup</i> data pada sistem informasi.</li> <li>• Untuk menjaga sistem informasi dari kesalahan/<i>bug</i> pada <i>source code</i> berdasarkan kontrol A.14.2.9. Pengujian penerimaan sistem, dimasukkan persyaratan pengujian sistem.</li> <li>• Untuk menjaga sistem informasi dari kesalahan dan ancaman lain saat pengembangan berdasarkan kontrol A.14.2.6. Lingkungan pengembangan yang aman, dimasukkan persyaratan pemisahan lingkungan pengembangan sistem yang dibagi menjadi lingkungan pengembangan, pengujian dan operasional.</li> </ul> |                       |
| NA           | Untuk perlindungan layanan melalui jaringan yang melibatkan transaksi, ruang lingkup SMKI tidak mencakup berdasarkan kontrol A.14.1.2. Pengamanan layanan aplikasi di jaringan publik dan kontrol A.14.1.3. Melindungi layanan transaksi aplikasi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                       |
| NA           | Untuk perlindungan produk yang dikembangkan oleh vendor sesuai dengan permintaan, DPTSI-ITS sudah mulai mengembangkan sendiri perangkat lunak yang digunakan untuk aktifitas organisasi oleh Subdit Pengembangan berdasarkan kontrol A.14.2.7. Pengembangan oleh pihak ketiga.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                       |
| C            | Untuk kriteria penerimaan sistem, DPTSI-ITS menggunakan kriteria yang didefinisikan sebelumnya oleh pengguna, seperti proses bisnis dan fungsionalitas dari sistem. Kriteria ini didokumentasikan dan ditinjau oleh beberapa pemangku kepentingan, dan digunakan sebagai acuan untuk pengujian sistem.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                       |
| A.14.1.2     | Pengamanan layanan aplikasi di jaringan publik                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <i>Not applicable</i> |
|              | Apakah informasi yang berkaitan dengan sistem informasi <i>online</i> dilindungi untuk mencegah aktifitas penipuan, perselisihan kontrak dan penyingkapan dan modifikasi tanpa izin?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                       |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                        |                            |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| NA                                                      | Ruang lingkup dalam <i>website server</i> dan <i>email</i> tidak memerlukan pengamanan layanan aplikasi di jaringan publik. Hal ini dikarenakan Webmail ITS tidak ada aktifitas transaksi dengan pengguna yang berkaitan dengan keuangan.                                                                                                                                              |                            |
| A.14.1.3                                                | Melindungi layanan transaksi aplikasi                                                                                                                                                                                                                                                                                                                                                  | <i>Not applicable</i>      |
|                                                         | Apakah informasi yang berkaitan dengan aplikasi layanan transaksi dilindungi untuk mencegah transmisi tidak lengkap, <i>mis-routing</i> , perubahan pesan, penyingkapan tanpa izin, duplikasi pesan atau membalas tanpa izin?                                                                                                                                                          |                            |
| NA                                                      | Ruang lingkup dalam <i>website server</i> dan <i>email</i> tidak memerlukan perlindungan layanan transaksi aplikasi. Berdasarkan kontrol A.14.1.2. Pengamanan layanan aplikasi di jaringan publik, Webmail ITS tidak memiliki fitur transaksi.                                                                                                                                         |                            |
| A.14.2. Keamanan dalam proses pengembangan dan dukungan |                                                                                                                                                                                                                                                                                                                                                                                        |                            |
| A.14.2.1                                                | Kebijakan pengembangan yang aman                                                                                                                                                                                                                                                                                                                                                       | <i>Partially compliant</i> |
|                                                         | Apakah aturan untuk membangun perangkat lunak atau sistem dibangun dan diterapkan dalam organisasi?                                                                                                                                                                                                                                                                                    |                            |
| PC                                                      | DPTSI-ITS sedang membuat pengembangan sistem informasi dan masih dalam bentuk <i>draft</i> .                                                                                                                                                                                                                                                                                           |                            |
| A.14.2.2                                                | Prosedur kontrol perubahan sistem                                                                                                                                                                                                                                                                                                                                                      | <i>Partially compliant</i> |
|                                                         | Apakah perubahan pada sistem dalam daur hidup pengembangan dikontrol dengan menggunakan prosedur formal yang mengontrol perubahan?                                                                                                                                                                                                                                                     |                            |
| C                                                       | Untuk dokumentasi prosedur pengembangan sistem informasi: <ul style="list-style-type: none"><li>• Prosedur Layanan Perbaikan Sistem Informasi (Intern) yang digunakan untuk membuat pelayanan kepada pengguna layanan DPTSI-ITS yang ingin mengajukan perbaikan ataupun pembaruan pada sistem informasi yang telah ada. Prosedur ini dapat dilihat pada <b>Gambar F.139</b>.</li></ul> |                            |

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>C<br/>(lanj.)</p> | <ul style="list-style-type: none"> <li>• Prosedur Pemutakhiran/Perbaikan Sistem Informasi yang berisikan proses pembuatan/pengembangan sistem informasi dari sisi pengembang sistem (<i>desainer, programmer</i> dan <i>dokumentator</i>). Prosedur ini dapat dilihat pada <b>Gambar F.140</b>.</li> <li>• Prosedur Proses Pengujian Sistem Informasi yang berisikan proses pengujian sistem informasi oleh tim penguji dan pengguna. Prosedur ini dapat dilihat pada <b>Gambar F.141</b>.</li> <li>• Prosedur Proses Instalasi Sistem Informasi yang berisikan proses instalasi sistem informasi, yang telah selesai diuji coba kedalam <i>server live</i>. Prosedur ini dapat dilihat pada <b>Gambar F.142</b>.</li> <li>• Prosedur Layanan Sosialisasi Sistem Informasi (Intern) yang berisikan proses penyelenggaraan kegiatan sosialisasi sistem informasi baru yang telah dibuat dan diuji coba, sebelum nantinya diaplikasikan/digunakan secara penuh. Prosedur ini dapat dilihat pada <b>Gambar F.143</b>. Sosialisasi yang dilakukan dipublikasikan melalui <i>website</i> <a href="https://dptsi.its.ac.id/?cat=8">https://dptsi.its.ac.id/?cat=8</a>.</li> </ul> |
| <p>NC</p>            | <p>Untuk manajemen resiko pada perubahan sistem, DPTSI-ITS masih belum menggunakan manajemen resiko berdasarkan kontrol A.6.1.5. Manajemen proyek untuk keamanan informasi. Jadi Subdit Pengembangan tidak melakukan analisis dampak dari perubahan dan kontrol keamanan yang diperlukan.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p>C</p>             | <p>Untuk tingkat hak akses pada sistem, Subdit Pengembangan menyesuaikan dengan <i>user requirement</i> dari pengguna sistem dan merekamnya pada dokumen <i>Developer Guide</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p>C</p>             | <p>Untuk peran dan tanggung jawab dalam perubahan sistem, Subdit Pengembangan hanya mengizinkan karyawan yang bertugas dalam pengembangan sistem tersebut saja.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <p>C</p>             | <p>Untuk peninjauan konflik jika terjadi perubahan, Subdit Pengembangan melakukan pengujian untuk melihat apakah sistem tersebut sesuai kebutuhan dan diterima oleh pengguna berdasarkan kontrol A.14.2.9. Pengujian penerimaan sistem.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C  | Untuk identifikasi perangkat lunak, informasi, entitas <i>database</i> dan perangkat keras yang harus dikembangkan, Subdit Pengembangan mengidentifikasi semua yang perlu dikembangkan ketika sistem informasi dirubah untuk menyesuaikan dengan <i>user requirement</i> .                                                                                                                                                                                                                                                                                                                                                                                                        |
| NC | Untuk identifikasi dan pengecekan keamanan <i>coding</i> pada <i>source code</i> , Subdit Pengembangan tidak melakukan peninjauan <i>source code</i> untuk mengurangi kemungkinan kerentanan berdasarkan kontrol A.14.2.9. Pengujian penerimaan sistem.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| C  | Untuk persetujuan formal dalam perubahan sebelum aktifitas dilakukan, Subdit Pengembangan mendapatkannya ketika pengguna sistem menyampaikan <i>user requirement</i> -nya berupa <i>flowchart</i> , proses bisnis, rancangan <i>database</i> dan <i>user interface</i> .                                                                                                                                                                                                                                                                                                                                                                                                          |
| C  | Untuk penerimaan perubahan oleh pengguna, pengguna sistem menerima perubahan sistem setelah pengguna sistem mengujinya berdasarkan kontrol A.14.2.9. Pengujian penerimaan sistem.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| C  | Untuk dokumentasi sistem, Subdit Pelayanan memiliki <i>User Guide</i> dan <i>Developer Guide</i> yang dibuat oleh dokumentator. <i>User Guide</i> merupakan buku panduan bagi pengguna yang berisikan penjelasan penggunaan perangkat lunak yang digunakan di DPTSI-ITS. <i>User Guide</i> dapat dilihat pada <b>Gambar F.145</b> . Sedangkan <i>Developer Guide</i> merupakan buku panduan bagi Subdit Pengembang yang berisikan penjelasan <i>source code</i> dan <i>database</i> dengan penggambaran diagramnya yang membantu <i>programmer</i> selanjutnya dalam pengembangan sistem. <i>Developer Guide</i> dapat dilihat pada <b>Gambar F.146</b> dan <b>Gambar F.147</b> . |
| C  | Untuk penyimpanan semua versi perubahan sistem yang dikembangkan, Subdit Pengembangan menggunakan Git ITS untuk sistem manajemen <i>source code</i> berdasarkan kontrol A.9.4.5. Kontrol akses ke <i>source code</i> perangkat lunak.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| C  | Untuk riwayat rekaman pengembangan sistem, DPTSI-ITS menyimpan surat permohonan dari pengguna yang menginginkan pembuatan atau pembaharuan sistem.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                            |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| C        | Untuk waktu penerapan perubahan, Subdit Pengembangan melakukan pada waktu dimana tidak terlalu sibuk akan proses bisnis. Misalkan terdapat perubahan pada SIM Akademik, maka perubahan tidak dilakukan diwaktu mahasiswa mengisi FRS.                                                                                                                                                                                                                                                                                                                    |                            |
| A.14.2.3 | Tinjauan teknis pada aplikasi setelah dilakukan perubahan dasar                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <i>Partially compliant</i> |
|          | Apakah aplikasi bisnis yang kritis ditinjau dan diuji ketika <i>platform</i> operasional dirubah (sistem operasi, <i>database</i> , <i>middleware</i> ) untuk memastikan tidak ada dampak yang merugikan pada operasional dan keamanan organisasi?                                                                                                                                                                                                                                                                                                       |                            |
| C        | Untuk peninjauan apakah terjadi konflik ketika terjadi perubahan <i>platform</i> , DPTSI-ITS melakukan peninjauan sistem yang dirubah pada <i>server</i> . Contohnya ketika sistem operasi (Linux), aplikasi manajemen <i>database</i> (MySQL), aplikasi <i>website server</i> (Apache HTTP Server) dan lainnya dirubah ditempat berbeda terlebih dahulu, lalu dilakukan peninjauan. Jika terdapat masalah baik perubahan ditempat pengujian ataupun <i>server live</i> , maka dilakukan penggunaan versi lama dan menunggu untuk dilakukan pembaharuan. |                            |
| C        | Untuk notifikasi setiap perubahan <i>platform</i> , DPTSI-ITS menginformasikan kepada pengguna dan <i>administrator</i> yang terlibat agar diberikan waktu untuk pengujian, dan peninjauan sebelum penerapan.                                                                                                                                                                                                                                                                                                                                            |                            |
| NC       | Untuk penggunaan <i>BCP</i> ketika perubahan <i>platform</i> , DPTSI-ITS masih belum menggunakannya berdasarkan kontrol A.17.1.1. Merencanakan keberlangsungan keamanan informasi.                                                                                                                                                                                                                                                                                                                                                                       |                            |
| A.14.2.4 | Pembatasan pada perubahan paket perangkat lunak                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <i>Non-compliant</i>       |
|          | Apakah modifikasi pada paket perangkat lunak diurungkan, dibatasi untuk perubahan yang diperlukan dan semua perubahan harus dikontrol secara ketat?                                                                                                                                                                                                                                                                                                                                                                                                      |                            |
| NC       | Untuk pembatasan aktifitas modifikasi paket instalasi perangkat lunak, DPTSI-ITS tidak membatasinya melakukan modifikasi paket instalasi perangkat lunak yang dipasang kedalam sistem dengan cara tidak memasang bagian atau <i>plug-in</i> yang tidak diperlukan karena alasan performa. Selain itu                                                                                                                                                                                                                                                     |                            |

|               |                                                                                                                                                                                                                                                                                                                                                                                   |                            |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| NC<br>(lanj.) | setiap aktifitas tidak didokumentasikan riwayatnya untuk menjelaskan apa yang dimodifikasi.                                                                                                                                                                                                                                                                                       |                            |
| NC            | Untuk pengujian hasil dari modifikasi paket instalasi perangkat lunak, secara formal, DPTSI-ITS tidak melakukannya secara formal dan dilakukan oleh masing-masing karyawan secara individual.                                                                                                                                                                                     |                            |
| NC            | Untuk dokumentasi prosedur modifikasi paket instalasi perangkat lunak, DPTSI-ITS tidak memiliki dokumen tersebut yang berisikan perencanaan, pengujian dan pendokumentasian perubahan paket instalasi perangkat lunak.                                                                                                                                                            |                            |
| A.14.2.5      | Prinsip keahlian teknis yang aman                                                                                                                                                                                                                                                                                                                                                 | <i>Non-compliant</i>       |
|               | Apakah panduan keamanan teknis untuk pemrograman yang aman dibangun, didokumentasikan, dirawat dan diterapkan pada setiap penerapan sistem informasi?                                                                                                                                                                                                                             |                            |
| NC            | Untuk penggunaan standar teknis dan <i>source code</i> , DPTSI-ITS belum memiliki standar teknis untuk pemrograman dan standar <i>source code</i> yang aman, namun mencontoh dari sistem informasi yang sudah pernah dibuat. <i>PHP</i> dan <i>Ms.SQL Server</i> merupakan bahasa pemrograman standar dan sistem <i>database</i> yang digunakan untuk program yang akan dibangun. |                            |
| NC            | Untuk pembaharuan standar teknis dan <i>source code</i> secara berkala, DPTSI-ITS belum melaksanakannya dikarenakan masih belum memilikinya.                                                                                                                                                                                                                                      |                            |
| A.14.2.6      | Lingkungan pengembangan yang aman                                                                                                                                                                                                                                                                                                                                                 | <i>Partially compliant</i> |
|               | Apakah organisasi membangun dan melindungi lingkungan pengembangan yang aman untuk pengembangan sistem yang mencakup keseluruhan daur hidup pengembangan sistem?                                                                                                                                                                                                                  |                            |
| NC            | Untuk manajemen resiko pada lingkungan pengembangan yang aman, DPTSI-ITS masih belum menggunakan manajemen resiko berdasarkan kontrol A.6.1.5. Manajemen proyek untuk keamanan informasi. Jadi DPTSI-ITS tidak melakukan pengidentifikasian resiko pada pengembangan sistem tertentu dan memilih penanganan resiko secara spesifik.                                               |                            |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NC | Untuk melihat kesensitifan data yang diproses, disimpan dan ditransmisikan oleh SIM yang dibangun masih belum bisa dilakukan. Hal ini dikarenakan klasifikasi informasi belum terdokumentasikan berdasarkan kontrol A.8.2.1. Klasifikasi informasi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| C  | Untuk melihat kepercayaan terhadap karyawan didalam lingkungan pengembangan sistem, Direktorat SDM dan Organisasi melakukan <i>background check</i> terhadap karyawan baru berdasarkan kontrol A.7.1.1. Penyaringan karyawan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| C  | Untuk pembagian lingkungan pengembangan sistem, Subdit Pengembangan membagi lingkungan pengembangan sistem menjadi tempat pembuatan dan pengujian. Tempat pembuatan umumnya berada pada komputer atau laptop yang digunakan oleh <i>programmer</i> . Sedangkan untuk tempat pengujian berada pada <i>server development</i> , dimana sistem yang berada ditempat pembuatan dipindahkan ke <i>server development</i> . Subdit Pengembangan juga tidak menggabungkan lingkungan pengembangan sistem dengan lingkungan operasional sistem, dimana sistem yang berada pada <i>server development</i> dipindahkan ke <i>server live</i> setelah diuji.                                                                         |
| C  | Untuk kontrol akses didalam lingkungan pengembangan sistem, terdapat pemisahan untuk mengakses kedalam <i>server development</i> dan <i>live</i> . Contohnya mahasiswa magang dan <i>programmer</i> dari luar Subdit Pengembangan hanya bisa mengakses ke <i>server development</i> saja, sedangkan Subdit Pengembangan bisa mengakses ke <i>server development</i> dan <i>live</i> untuk memindahkan sistem yang dikembangkan dari <i>server development</i> ke <i>server live</i> setelah dilakukan pengujian. Hal ini dapat dilihat pada formulir Permintaan <i>Server</i> yang berisikan pilihan permintaan <i>server development</i> atau/dan <i>server live</i> . Formulir dapat dilihat pada <b>Gambar F.148</b> . |
| C  | Untuk mengawasi perubahan dan mengatur <i>source code</i> , Subdit Pengembangan menggunakan Git ITS untuk sistem manajemen <i>source code</i> berdasarkan kontrol A.9.4.5. Kontrol akses ke <i>source code</i> perangkat lunak.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| NC | Untuk <i>backup</i> data pengembangan, DPTSI-ITS tidak memiliki lokasi <i>backup</i> ditempat terpisah antara <i>server</i> yang berisikan Git ITS dengan hasil <i>backup</i> -nya berdasarkan kontrol A.12.3.1. <i>Backup</i> informasi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                            |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| NC       | DPTSI-ITS tidak memiliki dokumentasi prosedur proses pengembangan di lingkungan pengembangan sistem untuk SIM tertentu yang berisikan langkah-langkah dari awal pembuatan <i>source code</i> sampai selesainya SIM tersebut didalam lingkungan pengembangan sistem.                                                                                                                                                                             |                            |
| A.14.2.7 | Pengembangan oleh pihak ketiga                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Not applicable</i>      |
|          | Apakah organisasi mengawasi aktifitas pengembangan sistem oleh pengembang/vendor luar?                                                                                                                                                                                                                                                                                                                                                          |                            |
| NA       | DPTSI-ITS tidak menggunakan sistem informasi yang dikembangkan oleh pengembang/vendor dari luar. Semua sistem informasi yang ada di ITS adalah hasil pengembangan Subdit Pengembangan di DPTSI-ITS.                                                                                                                                                                                                                                             |                            |
| A.14.2.8 | Pengujian keamanan sistem                                                                                                                                                                                                                                                                                                                                                                                                                       | <i>Compliant</i>           |
|          | Apakah pengujian fungsi keamanan dilakukan selama pengembangan?                                                                                                                                                                                                                                                                                                                                                                                 |                            |
| C        | Untuk pengujian dan verifikasi sistem baru atau pembaharuan, Subdit Pengembangan melakukan pengujian sistem didalam proses pengembangan sistem, seperti menyesuaikan apakah <i>input</i> data dan hasil yang diharapkan pada kondisi tertentu sesuai dengan kebutuhan sistem yang sudah didefinisikan diawal pengembangan sistem.                                                                                                               |                            |
| C        | Untuk peran dan tanggung jawab dalam pengujian sistem, DPTSI-ITS menetapkan tim pengembang sistem di Subdit Pengembangan yang terlibat dalam pengembangan.                                                                                                                                                                                                                                                                                      |                            |
| A.14.2.9 | Pengujian penerimaan sistem                                                                                                                                                                                                                                                                                                                                                                                                                     | <i>Partially compliant</i> |
|          | Apakah program pengujian dan kriteria yang berhubungan dengan penerimaan sistem dibangun untuk sistem informasi baru atau versi pembaharuan?                                                                                                                                                                                                                                                                                                    |                            |
| C        | Untuk pengujian penerimaan sistem baru atau pembaharuan, Subdit Pengembangan melakukan dua kali, yaitu dilakukan oleh tim penguji sistem dan pengguna (unit/jurusan). Subdit Pengembangan memiliki <i>server development</i> ataupun Git ITS yang dikhususkan untuk melakukan aktifitas pengujian sistem yang dibangun berdasarkan kontrol A.14.2.6. Lingkungan pengembangan yang aman dan kontrol A.9.4.5. Kontrol akses ke <i>source code</i> |                            |



|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| C<br>(lanj.)                                            | perangkat lunak. Hal yang diuji mencakup fungsi, <i>accessability</i> , manajemen pengguna (hak akses) dan <i>usability</i> . Setiap aktifitas pengujian dicatat dan jika terdapat masalah maka dilakukan pelaporan kepada <i>programmer</i> untuk segera direvisi. Git ITS juga dapat memudahkan pencatatan dan kolaborasi pengujian dan perbaikan sistem antara <i>programmer</i> dan penguji sistem. Prosedur pengujian penerimaan sistem dapat dilihat pada <b>Gambar F.141</b> .                                                 |                       |
| NC                                                      | Untuk penggunaan alat bantu dalam pengujian penerimaan sistem, DPTSI-ITS tidak menggunakan standar, alat ukur, metode (seperti peninjauan <i>source code</i> yang meninjau apakah terdapat kode berbahaya atau kerentanan yang dimasukkan sengaja atau tidak yang dilakukan karyawan lain), dan perangkat uji sistem (seperti tes penetrasi atau pemindaian kerentanan) apapun.                                                                                                                                                       |                       |
| A.14.3. Pengujian data                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |
| A.14.3.1                                                | Perlindungan data pengujian                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <i>Not applicable</i> |
|                                                         | Apakah pengujian menggunakan data yang asli dilindungi dan dikontrol?                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                       |
| NA                                                      | DPTSI-ITS tidak menggunakan data asli untuk menguji sistem informasi yang dibangun, melainkan menggunakan data <i>dummy</i> . Jadi DPTSI-ITS tidak memerlukan aturan/kebijakan untuk melindungi data pengujian.                                                                                                                                                                                                                                                                                                                       |                       |
| A.15. Relasi dengan Vendor                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |
| A.15.1. Keamanan informasi dalam hubungan dengan vendor |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |
| A.15.1.1                                                | Kebijakan keamanan informasi untuk hubungan dengan vendor                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | <i>Compliant</i>      |
|                                                         | Apakah persyaratan keamanan informasi untuk menangani resiko berkaitan dengan akses vendor ke aset informasi disetujui oleh vendor dan didokumentasikan?                                                                                                                                                                                                                                                                                                                                                                              |                       |
| C                                                       | Vendor tidak memiliki akses kedalam ruangan pusat data dan ruangan didalam DPTSI-ITS berdasarkan kontrol A.11.1.1. Perlindungan keamanan fisik. Jika ada vendor yang memasang perangkat jaringan dan <i>server</i> maka setelah pemasangan akun <i>default</i> yang digunakan oleh vendor akan dihapus didalam sistem. DPTSI-ITS memiliki <i>server</i> di Telkom Gubeng sebagai <i>disaster recovery center</i> berdasarkan kontrol A.17.1.1. Merencanakan keberlangsungan keamanan informasi. Dalam penggunaan <i>DRC</i> , DPTSI - |                       |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                       |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| C<br>(lanj.) | ITS memiliki dokumen perjanjian menjaga kerahasiaan dengan vendor untuk melindungi kerahasiaan informasi yang disimpan di <i>DRC</i> berdasarkan kontrol A.15.1.2. Merujuk keamanan dengan perjanjian vendor.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                       |
| A.15.1.2     | Merujuk keamanan dengan perjanjian vendor                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <i>Compliant</i>      |
|              | Apakah semua persyaratan keamanan informasi yang terkait dibuat dan disetujui oleh setiap vendor yang akan mengakses, memproses, menyimpan informasi organisasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |
| C            | PT. Telkom dapat mengakses ke aset informasi yang dimiliki DPTSI-ITS berdasarkan kontrol A.15.1.1. Kebijakan keamanan informasi untuk hubungan dengan vendor,. Akses tersebut dilindungi oleh perjanjian menjaga kerahasiaan ( <i>non-disclosure agreement</i> ) yang harus dipenuhi oleh PT. Telkom seperti tidak boleh mengakses data didalam <i>server</i> , denda jika melanggar ketentuan tersebut, dan lainnya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                       |
| A.15.1.3     | Rantai pasok teknologi informasi dan komunikasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <i>Not applicable</i> |
|              | Apakah perjanjian dengan vendor termasuk persyaratan untuk merujuk resiko keamanan informasi yang berkaitan dengan informasi, dan rantai pasok layanan TIK dan produk?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                       |
| NA           | <p>DPTSI-ITS tidak memiliki ketergantungan terhadap suatu layanan TIK atau produk pada merek dan vendor tertentu. DPTSI-ITS tidak memiliki merek favorit atau kebergantungan untuk produk, namun yang ada adalah prioritas seperti merek Hawlett Packard untuk produk <i>server</i> dan CISCO untuk produk perangkat jaringan. Sedangkan untuk vendor bisa siapa saja ketika pengadaan asalkan sesuai dengan spesifikasi yang didefinisikan.</p> <p>Selain itu DPTSI-ITS juga tidak memiliki keergantungan terhadap layanan TIK tertentu, seperti layanan <i>email</i> dengan Google dan Microsoft. Hal ini dikarenakan pada halaman rubah data menggunakan akun <i>administrator</i> Webmail ITS terdapat fitur pemindahan/migrasi layanan <i>email</i> (pada pilihan “lokasi <i>mailbox</i>”) dari Google ataupun Microsoft ke layanan <i>email</i> mandiri asalkan tidak melebihi kapasitas Webmail ITS yaitu 200 MB. Untuk semua <i>file attachment</i> harus di-<i>backup</i> terlebih dahulu oleh pengguna secara manual karena pemindahan tidak termasuk <i>attachement</i>. Hal ini dapat dilihat pada <b>Gambar F.59</b>.</p> |                       |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                   |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------|
| <p>NA<br/>(lanj.)</p>                                   | <p>Jika terdapat komponen/perangkat atau layanan yang tidak lagi tersedia karena vendor/merek tersebut bangkrut atau tidak dapat menyediakan karena sudah didiskontinyu maka DPTSI-ITS tidak terkena dampak dari ketidaktersediaan rantai pasok dari komponen/perangkat atau layanan tersebut, kecuali dampak dari biaya pelatihan (contohnya jika merek X bangkrut maka untuk dapat menggunakan merek Y harus dilakukan pelatihan) dan waktu untuk melakukan migrasi (untuk perangkat dan layanan TIK terdapat waktu pemasangan dan konfigurasinya).</p> |                                   |
| <p><b>A.15.2. Manajemen kualitas layanan vendor</b></p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                   |
| <p>A.15.2.1</p>                                         | <p>Mengawasi dan meninjau layanan vendor</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <p><i>Partially compliant</i></p> |
|                                                         | <p>Apakah organisasi mengawasi, meninjau dan mengaudit layanan yang diberikan vendor secara berkala?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                   |
| <p>C</p>                                                | <p>Untuk mengawasi kesesuaian performa tingkat layanan dengan perjanjian kontrak, Subdit Infrastruktur mengawasi <i>availability</i> layanan yang disediakan <i>ISP</i> berjalan tanpa adanya gangguan. Misalkan terjadi koneksi lambat maka dilakukan <i>capture</i> kecepatan dan kondisi <i>internet</i> dengan aplikasi lalu mengirimkannya beserta keluhan ke <i>ISP</i>. Selain itu dilakukan peninjauan apakah semua jumlah kondisi hidup dan matinya koneksi <i>internet</i> sesuai dengan yang dijanjikan didalam kontrak.</p>                   |                                   |
| <p>C</p>                                                | <p>Untuk peninjauan laporan layanan oleh vendor, DPTSI-ITS mengadakan rapat dengan vendor terkait yang membahas tentang operasional layanan <i>ISP</i> yang digunakan.</p>                                                                                                                                                                                                                                                                                                                                                                                |                                   |
| <p>C</p>                                                | <p>Untuk audit vendor, DPTSI-ITS melakukannya secara berkala setiap tahun sekali sekaligus membahas isu-isu yang teridentifikasi pada layanan <i>ISP</i> yang diberikan oleh vendor.</p>                                                                                                                                                                                                                                                                                                                                                                  |                                   |
| <p>C</p>                                                | <p>Untuk informasi yang disediakan tentang insiden keamanan informasi, DPTSI-ITS menyimpan jumlah laporan yang diterima Subdit Pelayanan dan <i>file log</i> yang berisikan kondisi hidup dan matinya koneksi <i>internet</i> pada perangkat Sangfor <i>Internet Access Management</i>.</p>                                                                                                                                                                                                                                                               |                                   |
| <p>C</p>                                                | <p>Untuk peran dan tanggung jawab dalam manajemen hubungan dengan vendor, DPTSI-ITS tidak melakukannya karena dilakukan oleh unit lain di ITS yaitu ULP-ITS.</p>                                                                                                                                                                                                                                                                                                                                                                                          |                                   |

|                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                     |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| NC                                                              | DPTSI-ITS tidak memiliki dokumentasi prosedur peninjauan kesesuaian layanan TIK yang berisikan pengawasan jumlah ketidaksesuaian layanan dengan kontrak, pengajuan keluhan dan kompensasi ke vendor, dan penindak lanjutan penanganannya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                     |
| A.15.2.2                                                        | Mengatur perubahan pada layanan vendor                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Partially compliant |
|                                                                 | Apakah perubahan ketentuan layanan oleh vendor diatur dengan memperhatikan kekritisian proses, sistem dan informasi bisnis yang terlibat?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                     |
| PC                                                              | <p>Ketika terjadi perubahan ketentuan layanan oleh vendor, DPTSI-ITS melakukan tinjauan ulang kontraknya. Jika masih dapat diterima kondisinya dan tidak melanggar maka akan dibiarkan. Sedangkan jika terdapat pelanggaran maka akan dimintai kompensasi ke vendor. Misalnya <i>ISP</i> didalam kontraknya memiliki kewajiban menyediakan layanan yang hidup 99.75% dan pihak <i>ISP</i> merubah ketentuan layanan yang mana tidak bisa memenuhi kewajiban, maka DPTSI-ITS bisa meminta kompensasi yang sesuai, bisa saja tempat <i>disaster recovery center</i> atau lainnya.</p> <p>Namun DPTSI-ITS tidak memiliki dokumentasi perubahan ketentuan layanan TIK yang berisikan langkah-langkah yang diambil ketika terjadi perubahan ketentuan layanan oleh vendor.</p> |                     |
| A.16. Manajemen Insiden Keamanan Informasi                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                     |
| A.16.1. Manajemen insiden keamanan informasi dan peningkatannya |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                     |
| A.16.1.1                                                        | Tanggung jawab dan prosedur                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Partially compliant |
|                                                                 | Apakah tanggung jawab dan prosedur pihak manajemen dibangun untuk memastikan umpan balik yang cepat dan efektif terhadap setiap insiden keamanan informasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                     |
| C                                                               | Untuk peran dan tanggung jawab dalam menangani umpan balik, DPTSI-ITS memiliki Subdit Pelayanan yang menerima dan menangani setiap laporan insiden keamanan informasi, gangguan/keluhan atau permohonan yang masuk. Prosesnya adalah pengguna mengirimkan laporan ke Subdit Pelayanan, lalu Subdit Pelayanan akan menanyakan informasi selengkapnya                                                                                                                                                                                                                                                                                                                                                                                                                       |                     |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| C<br>(lanj.) | jika laporan belum jelas. Setiap laporan akan di <i>follow-up</i> ke karyawan/subdit yang bertugas untuk menyelesaikannya. Prosedur untuk pelaporan dan penanganan keluhan dapat dilihat pada <b>Gambar F.149</b> , serta untuk pelaporan melalui sistem E-Tiket dapat dilihat pada <b>Gambar F.150</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                      |
| PC           | <p>Untuk dokumentasi prosedur penanganan insiden:</p> <ul style="list-style-type: none"> <li>• Prosedur Perbaikan Komponen Rusak yang digunakan untuk menangani perangkat yang komponen/<i>sparepart</i>-nya rusak. Prosedur ini dapat dilihat pada <b>Gambar F.151</b>.</li> <li>• Prosedur Instalasi Jaringan Rusak yang digunakan untuk memasang/mengganti perangkat jaringan yang rusak. Prosedur ini dapat dilihat pada <b>Gambar F.152</b>.</li> </ul> <p>DPTSI-ITS tidak memiliki dokumentasi prosedur pemulihan sistem dan data, seperti prosedur <i>recovery</i> data yang rusak/hilang, prosedur <i>restore</i> data <i>backup</i>, prosedur <i>restore clone VPS</i>, atau prosedur <i>restore</i> konfigurasi jaringan. Selain itu juga DPTSI-ITS tidak memiliki dokumentasi prosedur <i>troubleshooting</i> perangkat keras/lunak yang berisikan penanganan masalah tertentu pada beberapa perangkat yang pernah ditangani.</p> |                      |
| A.16.1.2     | Pelaporan insiden keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | <i>Compliant</i>     |
|              | Apakah setiap kejadian keamanan informasi dilaporkan secepatnya melalui jalur komunikasi kepihak manajemen?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                      |
| C            | DPTSI-ITS memiliki Subdit Pelayanan yang berfungsi untuk melayani pelaporan keluhan dan permohonan yang terkait TIK di lingkungan ITS ( <i>service desk</i> ). Terdapat 4 cara dalam cara pemberian pelaporan yaitu mengunjungi langsung kantor DPTSI-ITS, menghubungi lewat telepon PABX 1132 atau 031-5947270, mengirim <i>email</i> ke <a href="mailto:dptsi@its.ac.id">dptsi@its.ac.id</a> dengan subjek “Keluhan Pelanggan”, atau menggunakan sistem E-Tiket yang dapat diakses di alamat <a href="https://umpanbalik.its.ac.id">https://umpanbalik.its.ac.id</a> . Sistem E-Tiket memiliki fasilitas penggolongan prioritas laporan dan pengiriman <i>screenshot</i> masalah pada sistem. Sistem E-Tiket dapat dilihat pada <b>Gambar F.154</b> dan <b>Gambar F.155</b> . Prosedur untuk pelaporan melalui sistem E-Tiket dapat dilihat pada <b>Gambar F.150</b> .                                                                     |                      |
| A.16.1.3     | Pelaporan kelemahan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <i>Non-compliant</i> |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                            |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
|          | Apakah karyawan dan kontraktor yang menggunakan sistem informasi dan layanan diharuskan untuk melaporkan setiap kelemahan pada keamanan informasi yang dicurigai dan diobservasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |
| NC       | DPTSI-ITS tidak mensosialisasikan ataupun memberitahukan dosen, karyawan atau mahasiswa yang menggunakan sistem informasi dan layanan yang disediakan DPTSI-ITS agar dapat mengidentifikasi dan melaporkan setiap kelemahan pada keamanan informasi yang ditemukan.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                            |
| A.16.1.4 | Penilaian dan keputusan dalam insiden keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <i>Partially compliant</i> |
|          | Apakah kejadian keamanan informasi dinilai, serta diputuskan apakah diklasifikasikan sebagai insiden keamanan informasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                            |
| PC       | DPTSI-ITS mempertimbangkan mana laporan kejadian yang dikerjakan terlebih dahulu berdasarkan waktu laporan masuk atau jabatan pelapor, contohnya Rektor ITS lebih didahulukan daripada dosen. Namun tidak adanya klasifikasi berdasarkan jenis insiden (contohnya <i>denial of service</i> atau <i>malware</i> ), kisaran waktu penyelesaian (contohnya <1 jam atau 1-2 jam), tingkat urgensi insiden, aset yang bermasalah, dan dampak yang ada (contohnya besar, menengah, kecil). Selain itu juga DPTSI-ITS tidak memiliki dokumentasi prosedur penilaian dan pengklasifikasian insiden keamanan informasi yang berisikan cara penilaian berdasarkan klasifikasinya untuk menentukan mana yang terlebih dahulu ditangani. |                            |
| A.16.1.5 | Menanggapi insiden keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <i>Partially compliant</i> |
|          | Apakah setiap insiden keamanan informasi ditanggapi sesuai dengan prosedur yang terdokumentasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                            |
| C        | Untuk pengumpulan insiden, DPTSI-ITS melakukan pengumpulan bukti jika terjadi insiden. Misalkan terjadi aktifitas <i>DDoS</i> , maka Subdit Infrastruktur memeriksa <i>file log</i> pada SIEM AlienVault, <i>firewall</i> , <i>router</i> dan lainnya untuk melihat <i>IP address</i> sumber <i>DDoS</i> .                                                                                                                                                                                                                                                                                                                                                                                                                   |                            |
| PC       | Untuk analisa forensik, DPTSI-ITS melakukan aktifitas tersebut. Namun hal ini tidak didukung dengan dokumentasi prosedur untuk melakukannya berdasarkan kontrol A.16.1.7. Pengumpulan bukti.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                            |

|           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <i>C</i>  | Untuk eskalasi insiden jika diperlukan, DPTSI-ITS melakukan eskalasi sesuai dengan jenis insidennya. Contohnya jika terjadi insiden pencurian <i>password</i> yang dilakukan oleh mahasiswa, maka akan dieskalasi ke Hukortala-ITS untuk ditangani.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                            |
| <i>C</i>  | Untuk rekaman riwayat insiden dan aktifitas penanganannya, semua insiden didokumentasikan riwayatnya melalui sistem E-Tiket berdasarkan kontrol A.16.1.1. Tanggung jawab dan prosedur.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                            |
| <i>C</i>  | Untuk komunikasi tentang insiden, DPTSI-ITS melakukan pemberitahuan tentang adanya insiden berikut rinciannya kepada pemangku kepentingan yang terkait dengan insiden berdasarkan kontrol A.16.1.6. Pembelajaran dari insiden keamanan informasi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                            |
| <i>PC</i> | Untuk penemuan kelemahan ketika insiden, DPTSI-ITS melakukan perbaikan pada kelemahan yang teridentifikasi seperti pembaharuan <i>patch</i> atau perubahan konfigurasi. Namun prosedur dan kebijakan untuk manajemen kerentanan teknis belum terdokumentasikan dengan baik berdasarkan kontrol A.12.6.1. Manajemen kerentanan teknis.                                                                                                                                                                                                                                                                                                                                                                                                                                  |                            |
| A.16.1.6  | Pembelajaran dari insiden keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <i>Partially compliant</i> |
|           | Apakah ilmu yang didapat dari analisa dan penanganan insiden keamanan informasi didiskusikan dan digunakan untuk mengurangi kemungkinan dan dampak pada insiden kedepan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                            |
| <i>PC</i> | Setelah penanganan insiden keamanan informasi ataupun masalah yang ada biasanya diadakan diskusi dengan karyawan lain yang tergantung dari jenis insidennya. Jika penanganan insiden yang biasa dilakukan oleh Subdit Infrastruktur dan lainnya, maka diskusi tidak terlalu diperlukan. Sedangkan untuk insiden yang penanganannya tidak biasa dilakukan dan beresiko tinggi, maka dilakukan diskusi serta meningkatkan atau/dan menerapkan kontrol keamanan (kebijakan, prosedur, konfigurasi perangkat dan lainnya) untuk mengurangi kemungkinan atau dampaknya. DPTSI-ITS juga pernah menginformasikan kepada pemangku kepentingan di ITS melalui <i>website</i> , seperti apa yang terjadi, bagaimana meresponnya dan bagaimana untuk mencegahnya dikemudian hari. |                            |

|               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| PC<br>(lanj.) | <p>Misalnya ketika terjadi pencurian akun <i>password</i> yang mengatasnamakan <i>administrator</i> ITS, DPTSI-ITS memberi saran agar semua pengguna segera mengganti <i>password</i> karena semua akun akan diblokir untuk yang tidak mengganti. Hal ini dilakukan agar pencuri akun tidak bisa menggunakan akun yang dicurinya. Informasi pengingatnya untuk mencegah agar pengguna tidak memberikan <i>password</i> dikemudian hari ditempatkan dihalaman <i>login</i> Webmail ITS di <a href="https://webmail.its.ac.id">https://webmail.its.ac.id</a> yang dapat dilihat di <b>Gambar 4.1</b>.</p> <p>Namun DPTSI-ITS tidak memiliki dokumentasi prosedur eskalasi dan komunikasi insiden yang berisikan langkah-langkah peningkatan atau penambahan kontrol keamanan, dan komunikasi dengan pemangku kepentingan yang terkait.</p>                                                                                                                                                                                                                                                                                                               |                            |
| A.16.1.7      | Pengumpulan bukti                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <i>Partially compliant</i> |
|               | Apakah organisasi mendefinisikan dan menerapkan prosedur untuk identifikasi, mengumpulkan, dan memelihara informasi yang dapat dijadikan bukti?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
| PC            | <p>Untuk aktifitas pengumpulan bukti, DPTSI-ITS melakukan aktifitas pengumpulan dan pemeliharaan bukti forensik yang dapat dijadikan bukti hukum dan pemberian sanksi. DPTSI-ITS memiliki <i>SIEM</i> sebagai alat bantu untuk mengumpulkan bukti forensik karena <i>SIEM</i> menyimpan secara terpusat <i>file log</i> dari berbagai <i>server</i> berdasarkan kontrol A.13.1.1. Kontrol jaringan. Contohnya pernah terjadi <i>password</i> milik kepala jurusan Informatika terkena <i>hack</i>. DPTSI-ITS menggunakan <i>log</i> yang tersimpan baik dari <i>SIEM</i>, perangkat jaringan maupun <i>server</i> yang terkait untuk melihat rekam aktifitas dan sumbernya, lalu diserahkan buktinya ke Hukortala-ITS untuk dilakukan pencarian dan pengintrogasian. Setelah itu pelakunya ditemukan yaitu mahasiswa dari jurusan Informatika dan diberi sanksi oleh Hukortala-ITS.</p> <p>Namun DPTSI-ITS tidak memiliki dokumentasi prosedur penanganan bukti forensik yang berisikan rangkaian pemeliharaan dan keamanan bukti, peran dan tanggung jawab karyawan yang terlibat, kompetensi yang diperlukan karyawan, dokumentasi, dan diskusi.</p> |                            |
| NC            | Untuk peran dan tanggung jawab karyawan dalam aktifitas forensik, DPTSI-ITS belum menetapkan secara khusus.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                            |
| NC            | Untuk sertifikasi dan kualifikasi karyawan dalam aktifitas forensik, DPTSI-ITS belum memilikinya pada karyawan yang bekerja.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                            |



|                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                     |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| C                                                                    | Untuk perangkat yang berkaitan dengan aktifitas forensik, DPTSI-ITS memiliki perangkat bantu seperti SIEM AlienVault berdasarkan kontrol A.12.4.1. Mencatat kejadian.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                     |
| A.17. Aspek Keamanan Informasi akan Manajemen Keberlangsungan Bisnis |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                     |
| A.17.1. Keberlangsungan keamanan informasi                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                     |
| A.17.1.1                                                             | Merencanakan keberlangsungan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Partially compliant |
|                                                                      | Apakah organisasi menentukan persyaratan <i>business continuity plan</i> atau <i>disaster recovery plan</i> untuk situasi krisis atau bencana?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                     |
| PC                                                                   | DPTSI-ITS tidak memiliki dokumentasi <i>BCP</i> ataupun <i>DRP</i> . Namun DPTSI-ITS memiliki <i>server co-location</i> di Telkom Gubeng untuk <i>backup</i> dan <i>disaster recovery center</i> . <i>Disaster recovery center</i> merupakan persyaratan didalam kontrak dengan PT. Telkom berdasarkan kontrol A.13.1.2. Keamanan layanan jaringan. <i>Server</i> tersebut berfungsi sebagai <i>server mirror</i> yang mampu melayani pengguna/ <i>client</i> jika <i>server</i> utama mengalami bencana atau gangguan. <i>Server mirror</i> tersebut melakukan <i>backup</i> data dari <i>server</i> utama setiap hari. <i>Server</i> yang baru dilakukan <i>backup</i> adalah <i>website</i> ITS ( <a href="https://www.its.ac.id">https://www.its.ac.id</a> ) dan Webmail ITS. |                     |
| NC                                                                   | Untuk menentukan persyaratan <i>BCP</i> dan <i>DRP</i> , DPTSI-ITS tidak menggunakan metode <i>business impact analysis</i> . Hal ini dikarenakan DPTSI-ITS tidak melakukan aktifitas manajemen resiko berdasarkan kontrol A.6.1.5. Manajemen proyek untuk keamanan informasi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                     |
| A.17.1.2                                                             | Menerapkan keberlangsungan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Non-compliant       |
|                                                                      | Apakah organisasi membuat, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol keamanan untuk memastikan tingkat kebutuhan keberlangsungan keamanan informasi untuk situasi krisis atau bencana?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                     |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                     |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| NC                 | DPTSI-ITS tidak memiliki dokumentasi prosedur dan penggunaan kerangka kerja apapun terkait <i>BCP</i> atau <i>DRP</i> yang berisikan penjelasan rencana, tindakan respon dan pemulihannya. Selain itu tidak ada pembuatan struktur manajemen ataupun penunjukan khusus untuk karyawan yang melakukan persiapan, pelaksanaan, penanganan dan pengujian didalam aktifitas <i>BCP</i> atau <i>DRP</i> .                                                                                                                                                                  |                     |
| A.17.1.3           | Memverifikasi, meninjau dan mengevaluasi keberlangsungan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Non-compliant       |
|                    | Apakah organisasi menguji secara berkala kontrol tentang <i>business continuity</i> ataupun <i>disaster recovery</i> yang dibangun dan diterapkan benar dan efektif ketika krisis atau bencana?                                                                                                                                                                                                                                                                                                                                                                       |                     |
| NC                 | DPTSI-ITS tidak memverifikasi, meninjau dan mengevaluasi <i>BCP</i> atau <i>DRP</i> . Hal ini juga dikarenakan DPTSI-ITS belum mendokumentasikan <i>BCP</i> atau <i>DRP</i> berdasarkan kontrol A.17.1.2. Menerapkan keberlangsungan keamanan informasi.                                                                                                                                                                                                                                                                                                              |                     |
| A.17.2. Redundansi |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                     |
| A.17.2.1           | Ketersediaan dari fasilitas pemrosesan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Partially compliant |
|                    | Apakah fasilitas pemrosesan informasi diterapkan secara berlebih (seperti <i>disaster recovery center</i> atau redundansi komponen) untuk memenuhi persyaratan ketersediaan?                                                                                                                                                                                                                                                                                                                                                                                          |                     |
| C                  | Untuk redundansi arsitektur, DPTSI-ITS menerapkan <i>disaster recovery center</i> berupa <i>server mirror</i> yang ditempatkan diluar organisasi berdasarkan kontrol A.17.1.1. Merencanakan keberlangsungan keamanan informasi. Selain itu untuk setiap <i>server</i> pendukung yang penting dibuat secara redundan sebagai alternatif jika <i>server</i> tidak bekerja. Misalnya <i>server DNS</i> yang diatur agar terdapat <i>master</i> dan <i>slave</i> , dan <i>server proxy</i> ITS yang memiliki banyak <i>server</i> baik <i>VPS</i> atau <i>dedicated</i> . |                     |
| C                  | Untuk redundansi komponen, Subdit Infrastruktur memasang komponen yang redundan pada <i>hardisk</i> (contohnya dua atau lebih <i>hardisk</i> dengan konfigurasi <i>RAID</i> ) dan <i>memory</i> (contohnya konfigurasi <i>dual/multiple-channel</i> ) untuk setiap <i>server</i> fisik yang dikelola. Hal ini dilakukan agar jika terjadi kegagalan/kerusakan pada satu komponen maka <i>server</i> masih dapat berjalan normal dan data yang tersimpan masih dapat terjaga.                                                                                          |                     |

|                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                     |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| PC                                                   | Untuk redundansi komponen dan perangkat berupa cadangan, DPTSI-ITS memilikinya baik <i>hardisk</i> , <i>access point</i> , <i>access switch</i> , <i>distribution switch</i> dan lainnya. Namun DPTSI-ITS tidak memiliki cadangannya untuk komponen yang harganya bisa cepat turun di waktu mendatang (seperti <i>processor</i> atau <i>memory</i> ) dan perangkat yang harganya mahal (seperti <i>firewall</i> atau <i>core switch</i> ). Jika perangkat atau komponen terjadi kerusakan dan sudah melewati umur garansi, maka yang dilakukan adalah melakukan pengadaan barang dan menunggu sampai barang datang.                                                                                                            |                     |
| A.18. Kepatuhan                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                     |
| A.18.1. Kepatuhan akan persyaratan hukum dan kontrak |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                     |
| A.18.1.1                                             | Identifikasi kebutuhan undang-undang dan kontrak yang dapat digunakan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Compliant           |
|                                                      | Apakah semua undang-undang/peraturan dan persyaratan kontrak diidentifikasi, didokumentasikan dan diperbaharui untuk organisasi dan setiap sistem informasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                     |
| C                                                    | DPTSI-ITS memiliki dokumentasi semua peraturan/hukum yang dipatuhi dan berlaku di DPTSI-ITS yang bernama Daftar Dokumen Eksternal didalam dokumen ISO 9000. Isi dari dokumen tersebut seperti Peraturan Presiden RI nomor 70 tahun 2012, Standar Harga dan Satuan Barang, dan lainnya. Daftar Dokumen Eksternal dapat dilihat pada <b>Gambar F.156</b> . Sedangkan untuk peraturan yang berlaku dan melekat pada sistem informasi terpadu yang dibuat oleh Subdit Pengembangan, seperti peraturan keuangan pada SIM Keuangan, peraturan kepegawaian pada SIM Kepegawaian dan lainnya. Semuanya itu diserahkan kepada pemohon/pengguna sistem dan Subdit Pengembangan hanya menterjemahkan dan mempelajari kebutuhan sistemnya. |                     |
| A.18.1.2                                             | Hak kekayaan intelektual                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Partially compliant |
|                                                      | Apakah prosedur diterapkan untuk memastikan kepatuhan terhadap undang-undang/peraturan yang berhubungan dengan hak kekayaan intelektual dan penggunaan lisensi perangkat lunak asli?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                     |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NC | DPTSI-ITS tidak memiliki dokumentasi kebijakan penggunaan material yang mengandung hak kekayaan intelektual yang berisikan bagaimana penggunaan material dengan hak kekayaan intelektual, apa saja aktifitas yang dilarang untuk dilakukan, sumber pengunduhan material yang dibolehkan, pengelolaan kondisi lisensi yang tepat, dan pembuangan atau pemindahan perangkat lunak ke pihak lain.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| NC | DPTSI-ITS tidak memiliki dokumentasi prosedur ataupun menerapkan kontrol untuk meninjau apakah semua perangkat lunak yang dipasang di komputer tidak melanggar hak kekayaan intelektual didalam ruang lingkup DPTSI-ITS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| NC | Untuk kesadaran perlindungan hak kekayaan intelektual, DPTSI-ITS tidak menyadarkan untuk melindungi hak kekayaan intelektual dan sanksi bagi pemangku kepentingan jika melanggarnya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| C  | <p>Berikut ini yang dilakukan oleh DPTSI-ITS dalam hak kekayaan intelektual:</p> <ul style="list-style-type: none"> <li>• Untuk komputer dan laptop, DPTSI-ITS menyediakan beragam perangkat lunak dan sistem operasi berlisensi <i>full version</i> seperti Windows, Office, Matlab, Mathematica, Minitab dan LabView berikut prosedurnya bagi dosen, karyawan dan mahasiswa di <i>website</i> <a href="https://unduh.its.ac.id">https://unduh.its.ac.id</a>. Hal ini dapat dilihat pada <b>Gambar F.157</b>. Produk-produk tersebut hanya bisa dipasang melalui jaringan ITS dan untuk aktivasi menggunakan model KMS yang menginjeksi kode lisensi yang mana satu institusi bisa mengaktifasi dengan satu serial number. Selain itu DPTSI-ITS juga menyediakan perangkat lunak dan sistem operasi berlisensi <i>open source</i> seperti Centos, Debian, Proxmox VE dan Ubuntu di <i>website</i> <a href="http://boyoy.its.ac.id">boyoy.its.ac.id</a>. Hal ini dapat dilihat pada <b>Gambar F.158</b>.</li> <li>• Untuk <i>server</i> yang dikelola oleh Subdit Infrastruktur tidak semua bisa dipastikan apa saja yang dipasang, karena tidak semua hak akses pada <i>server</i> dimiliki oleh Subdit Infrastruktur kecuali yang berhubungan dengan akademik, keuangan dan kepegawaian. Namun <i>server</i> tersebut diluar ruang lingkup SMKI.</li> </ul> |
| NC | Untuk daftar aset yang perlu dijaga hak kekayaan intelektualnya, DPTSI-ITS tidak mendokumentasikan daftar tersebut.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| C  | Untuk bukti kepemilikan barang dengan hak kekayaan intelektual, Subdit Pelayanan menyimpan CD/DVD asli perangkat lunak, panduan, dan lainnya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

|                                       |                                                                                                                                                                                                                                                                                                                                   |                            |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.18.1.3                              | Perlindungan untuk rekaman                                                                                                                                                                                                                                                                                                        | <i>Not applicable</i>      |
|                                       | Apakah rekaman dilindungi dari kehilangan, kerusakan, kepalsuan, akses tanpa izin, dan publikasi tanpa izin sesuai undang-undang, peraturan, dan persyaratan kontrak?                                                                                                                                                             |                            |
| NA                                    | DPTSI-ITS tidak melindungi rekaman untuk memenuhi undang-undang, peraturan, dan persyaratan kontrak didalam ruang lingkup, namun berdasarkan kebijakan organisasi. Hal ini dikarenakan undang-undang tentang ITE mengenai perlindungan rekaman masih belum dipublikasikan pemerintah dan digunakan DPTSI-ITS.                     |                            |
| A.18.1.4                              | Kerahasiaan dan perlindungan untuk informasi pribadi                                                                                                                                                                                                                                                                              | <i>Not applicable</i>      |
|                                       | Apakah kerahasiaan dan perlindungan informasi pribadi dibutuhkan untuk memenuhi undang-undang dan peraturan?                                                                                                                                                                                                                      |                            |
| NA                                    | DPTSI-ITS tidak melindungi informasi pribadi untuk memenuhi undang-undang, peraturan, dan persyaratan kontrak didalam ruang lingkup, namun berdasarkan kebijakan organisasi. Hal ini dikarenakan undang-undang tentang ITE mengenai perlindungan informasi pribadi masih belum dipublikasikan pemerintah dan digunakan DPTSI-ITS. |                            |
| A.18.1.5                              | Peraturan untuk kontrol kriptografi                                                                                                                                                                                                                                                                                               | <i>Not applicable</i>      |
|                                       | Apakah kontrol kriptografi digunakan untuk memenuhi undang-undang, peraturan, dan persyaratan kontrak?                                                                                                                                                                                                                            |                            |
| NA                                    | DPTSI-ITS tidak menggunakan kontrol kriptografi untuk memenuhi undang-undang, peraturan, dan persyaratan kontrak didalam ruang lingkup, namun berdasarkan kebijakan organisasi. Hal ini dikarenakan undang-undang tentang ITE mengenai kontrol kriptografi masih belum dipublikasikan pemerintah dan digunakan DPTSI-ITS.         |                            |
| A.18.2. Peninjauan keamanan informasi |                                                                                                                                                                                                                                                                                                                                   |                            |
| A.18.2.1                              | Peninjauan keamanan informasi secara independen                                                                                                                                                                                                                                                                                   | <i>Partially compliant</i> |
|                                       | Apakah pendekatan organisasi untuk mengelola keamanan informasi dan penerapannya ditinjau secara independen dalam jangka waktu tertentu atau ketika perubahan signifikan terjadi?                                                                                                                                                 |                            |

|                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                   |                      |                                                                                                                                                                                                             |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| PC                                                                                                                                                                                                          | <p>DPTSI-ITS berencana menggunakan standar SNI ISO/IEC 27001 dan melakukan sertifikasi oleh badan sertifikasi di tahun 2017 berdasarkan kontrol A.6.1.5. Manajemen proyek untuk keamanan informasi. Jadi ketika DPTSI-ITS menggunakan SNI ISO/IEC 27001, maka DPTSI-ITS disyaratkan melakukan audit keamanan informasi secara internal setidaknya selama setahun sekali dan secara eksternal oleh badan sertifikasi ISO/IEC 27001 selama tiga tahun sekali.</p> <p>DPTSI-ITS belum pernah melakukan audit keamanan informasi kecuali yang dilakukan oleh mahasiswa melalui penelitian di DPTSI-ITS yang berkaitan tentang keamanan informasi, seperti:</p> <ul style="list-style-type: none"> <li>• Perancangan <i>disaster recovery plan</i> menggunakan ISO/IEC 24762:2008. Penelitian menggunakan penilaian resiko untuk membuat prosedur pemulihan bencana yang ditujukan untuk aset tertentu yang kritis dan resiko yang memiliki prioritas tertinggi (Daud, 2013).</li> <li>• Evaluasi keamanan informasi pada pengelolaan jaringan menggunakan Indeks KAMI yang sesuai dengan SNI ISO/IEC 27001:2009. Evaluasi yang khusus dilakukan di Subdit infrastruktur yang menghasilkan nilai tingkat kematangan kondisi saat ini berdasarkan Indeks KAMI dan apa saja rekomendasi untuk meningkatkan nilai kematangan. Pemberian rekomendasi tidak berdasarkan resiko dengan kriteria resiko yang tidak dapat diterima atau resiko dengan nilai resiko menengah keatas (Ulinnuha, 2013).</li> </ul> <p>Selain itu DPTSI-ITS tidak memiliki dokumentasi prosedur audit keamanan informasi yang berisikan langkah-langkah dalam audit keamanan informasi secara internal.</p> |                                                   |                      |                                                                                                                                                                                                             |  |
| A.18.2.2                                                                                                                                                                                                    | <table border="1"> <tr> <td data-bbox="391 1393 1158 1451">Kepatuhan terhadap kebijakan dan standar keamanan</td><td data-bbox="1158 1393 1375 1451"><i>Non-compliant</i></td></tr> <tr> <td colspan="2" data-bbox="391 1451 1375 1606">Apakah pihak manajemen meninjau secara berkala kepatuhan karyawan terhadap kebijakan, prosedur, standar dan persyaratan keamanan lainnya saat menjalankan proses bisnis didalam area tanggung jawab mereka?</td></tr> </table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Kepatuhan terhadap kebijakan dan standar keamanan | <i>Non-compliant</i> | Apakah pihak manajemen meninjau secara berkala kepatuhan karyawan terhadap kebijakan, prosedur, standar dan persyaratan keamanan lainnya saat menjalankan proses bisnis didalam area tanggung jawab mereka? |  |
| Kepatuhan terhadap kebijakan dan standar keamanan                                                                                                                                                           | <i>Non-compliant</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                   |                      |                                                                                                                                                                                                             |  |
| Apakah pihak manajemen meninjau secara berkala kepatuhan karyawan terhadap kebijakan, prosedur, standar dan persyaratan keamanan lainnya saat menjalankan proses bisnis didalam area tanggung jawab mereka? |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                   |                      |                                                                                                                                                                                                             |  |
| NC                                                                                                                                                                                                          | <p>DPTSI-ITS tidak memiliki dokumentasi kebijakan tentang keamanan informasi yang lengkap dan masih belum mengadopsi standar keamanan informasi untuk organisasi berdasarkan kontrol A.5.1.1. Kebijakan untuk informasi dan kontrol A.18.2.1. Peninjauan keamanan informasi secara independen. Jadi proses peninjauan apakah terdapat ketidak-patuhan (<i>non-conformity</i>) yang dilakukan karyawan terhadap kebijakan, prosedur dan</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                   |                      |                                                                                                                                                                                                             |  |

|                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                    |                                   |                                                                                                                                 |  |
|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------|--|
| <p><i>NC</i><br/>(lanj.)</p>                                                                                                    | <p>persyaratan keamanan lainnya yang merupakan persyaratan dalam standar keamanan informasi tidak dilakukan. Selain itu DPTSI-ITS tidak memiliki dokumentasi prosedur tindakan perbaikan (<i>corrective action</i>) yang berisikan apa saja yang dilakukan ketika melakukan peninjauan kebijakan, prosedur, standar dan persyaratan keamanan lainnya.</p>                                                                                                                                                                                                                                                                                                                                      |                                    |                                   |                                                                                                                                 |  |
| <p>A.18.2.3</p>                                                                                                                 | <table border="1"> <tr> <td data-bbox="347 472 1121 589"> <p>Peninjauan kepatuhan teknis</p> </td><td data-bbox="1121 472 1350 589"> <p><i>Partially compliant</i></p> </td></tr> <tr> <td colspan="2" data-bbox="347 589 1350 701"> <p>Apakah sistem informasi ditinjau secara berkala agar patuh terhadap kebijakan dan standar keamanan informasi organisasi?</p> </td></tr> </table>                                                                                                                                                                                                                                                                                                       | <p>Peninjauan kepatuhan teknis</p> | <p><i>Partially compliant</i></p> | <p>Apakah sistem informasi ditinjau secara berkala agar patuh terhadap kebijakan dan standar keamanan informasi organisasi?</p> |  |
| <p>Peninjauan kepatuhan teknis</p>                                                                                              | <p><i>Partially compliant</i></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                    |                                   |                                                                                                                                 |  |
| <p>Apakah sistem informasi ditinjau secara berkala agar patuh terhadap kebijakan dan standar keamanan informasi organisasi?</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                    |                                   |                                                                                                                                 |  |
| <p><i>PC</i></p>                                                                                                                | <p>DPTSI-ITS tidak melakukan aktifitas tes penetrasi dan pemindaian kerentanan secara berkala untuk menguji keamanan sistem informasi terpadu dan infrastruktur jaringan. Adapun terdapat pemindaian kerentanan dan <i>stress test</i>, tapi tidak dilakukan secara berkala dan umumnya dilakukan ketika ada masalah saja. DPTSI-ITS tidak memasukkan aktifitas tes penetrasi dan pemindaian kerentanan saat pengujian sistem yang dikembangkan oleh Subdit Pengembangan berdasarkan kontrol A.14.2.9. Pengujian penerimaan sistem. Selain itu DPTSI-ITS tidak memiliki dokumentasi prosedur peninjauan kepatuhan teknis yang berisikan aktifitas tes penetrasi dan pemindaian kerentanan.</p> |                                    |                                   |                                                                                                                                 |  |

Tabel E.1 Klasifikasi Tingkat Kepatuhan

| Klasifikasi                | Kode      | Keterangan                                                                                                              |
|----------------------------|-----------|-------------------------------------------------------------------------------------------------------------------------|
| <i>Compliant</i>           | <i>C</i>  | DPTSI-ITS patuh secara keseluruhan dengan area tertentu pada SNI ISO/IEC 27001.                                         |
| <i>Partially compliant</i> | <i>PC</i> | DPTSI-ITS telah melakukan berbagai cara untuk patuh, namun masih memerlukan pekerjaan tambahan yang harus dijalankan.   |
| <i>Non-compliant</i>       | <i>NC</i> | DPTSI-ITS tidak memiliki beberapa kontrol keamanan ditempat untuk memenuhi beberapa persyaratan dari SNI ISO/IEC 27001. |
| <i>Not applicable</i>      | <i>NA</i> | Telah ditinjau dan diidentifikasi bahwa kontrol keamanan tidak dapat diterapkan di DPTSI-ITS.                           |

Tabel E.2 Data Analisa Kesenjangan (Sesudah)

| No<br><i>Annex</i>                                               | Pertanyaan                                                                                                                        | Tingkat<br>Kematangan      |
|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <b>A.5.1. Arahan pihak manajemen terhadap keamanan informasi</b> |                                                                                                                                   |                            |
| A.5.1.1                                                          | Kebijakan keamanan informasi                                                                                                      | <i>Partially compliant</i> |
|                                                                  | Apakah kebijakan untuk keamanan informasi dibuat dan dikomunikasikan ke karyawan dan pemangku kepentingan yang terkait?           |                            |
| <i>NC</i>                                                        | Kebijakan penggunaan perangkat <i>mobile</i> (A.6.2.1) belum didokumentasikan.                                                    |                            |
| <i>NC</i>                                                        | Kebijakan penggunaan komputer/laptop (A.6.2.2) belum didokumentasikan.                                                            |                            |
| <i>PC</i>                                                        | Kebijakan penggunaan <i>internet</i> , <i>intranet</i> , <i>email</i> dan media sosial (A.8.1.3) belum semuanya didokumentasikan. |                            |
| <i>C</i>                                                         | Kebijakan klasifikasi informasi (A.8.2.1) sudah didokumentasikan.                                                                 |                            |
| <i>PC</i>                                                        | Kebijakan kontrol akses (A.9.1.1) belum didokumentasikan, masih dalam proses perencanaan pembuatan dan format <i>draft</i> .      |                            |
| <i>NC</i>                                                        | Kebijakan penggunaan enkripsi (A.10.1.1) belum didokumentasikan.                                                                  |                            |



|         |                                                                                                                                                                                                                                                                                                                                                                                                                                             |                  |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| NC      | Kebijakan manajemen kunci enkripsi (A.10.1.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                       |                  |
| NC      | Kebijakan kontrol akses fisik (A.11.1.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                            |                  |
| C       | Kebijakan bekerja di area yang aman (A.11.1.5) sudah didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                      |                  |
| C       | Kebijakan merapihkan meja dan membersihkan layar ( <i>clear desk and screen</i> ) (A.11.2.9) sudah didokumentasikan.                                                                                                                                                                                                                                                                                                                        |                  |
| C       | Kebijakan manajemen perubahan (A.12.1.2) sudah didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                            |                  |
| NC      | Kebijakan pemindahan perangkat lunak (A.12.1.4) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                     |                  |
| C       | Kebijakan penanganan <i>malware</i> (A.12.2.1) sudah didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                      |                  |
| C       | Kebijakan <i>backup</i> informasi (A.12.3.1) sudah didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                        |                  |
| C       | Kebijakan pemasangan dan penghapusan perangkat lunak (A.12.5.1) sudah didokumentasikan.                                                                                                                                                                                                                                                                                                                                                     |                  |
| C       | Kebijakan manajemen kerentanan teknis (A.12.6.1) sudah didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                    |                  |
| C       | Kebijakan pembatasan penggunaan perangkat lunak (A.12.6.2) sudah didokumentasikan.                                                                                                                                                                                                                                                                                                                                                          |                  |
| NC      | Kebijakan pertukaran informasi (A.13.2.1) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                                                           |                  |
| PC      | Kebijakan pengembangan sistem informasi (A.14.2.1) belum didokumentasikan, masih dalam proses perencanaan pembuatan dan format <i>draft</i> .                                                                                                                                                                                                                                                                                               |                  |
| NC      | Kebijakan penggunaan material yang mengandung hak kekayaan intelektual (A.18.1.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                   |                  |
| C       | Untuk komunikasi kebijakan yang berlaku, DPTSI-ITS mengkomunikasikannya melalui rapat jika kebijakan bersifat internal, sedangkan untuk kebijakan yang berlaku untuk seluruh dosen, karyawan dan mahasiswa ITS dikomunikasikan melalui <i>website</i> <a href="https://dptsi.its.ac.id/?page_id=161">https://dptsi.its.ac.id/?page_id=161</a> dan <a href="https://dptsi.its.ac.id/?page_id=156">https://dptsi.its.ac.id/?page_id=156</a> . |                  |
| A.5.1.2 | Peninjauan kebijakan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                     | <i>Compliant</i> |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |           |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
|                            | Apakah kebijakan untuk keamanan informasi ditinjau dalam jangka waktu yang direncanakan atau jika terjadi perubahan dalam organisasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |
| C                          | DPTSI-ITS melakukan peninjauan kebijakan keamanan informasi berdasarkan penilaian resiko yang terkait secara berkala. Setiap peninjauan kebijakan keamanan informasi melibatkan dan disetujui oleh Direktur DPTSI-ITS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |
| A.6.1. Organisasi internal |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |           |
| A.6.1.1                    | Peran dan tanggung jawab keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Compliant |
|                            | Apakah semua tanggung jawab tentang keamanan informasi didefinisikan dan dialokasikan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |
| C                          | Untuk peran dan tanggung jawab dalam suatu aset atau informasi spesifik, DPTSI-ITS sudah mendefinisikan dan mendokumentasikannya berdasarkan kontrol A.8.1.2. Kepemilikan aset.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |           |
| C                          | Untuk peran dan tanggung jawab dalam aktifitas manajemen resiko, DPTSI-ITS sudah menetapkannya kepada Subdit Infrastruktur sebagai salah satu tim pengelola SMKI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |           |
| C                          | <p>Untuk peran dan tanggung jawab dalam aktifitas keamanan informasi baik secara umum dan khusus, DPTSI-ITS memiliki Subdit Infastruktur. Subdit Infastruktur bertugas untuk perumusan kebijakan, pengembangan, pengawasan, pemeliharaan, peninjauan dan pelaporan infrastruktur dan keamanan TIK. Tanggung jawab yang dimiliki Kasubdit adalah:</p> <ul style="list-style-type: none"><li>• Menyusun rencana program kerja dan mempersiapkan pelaksanaan program kerja DPTSI-ITS.</li><li>• Menentukan kebijakan internal atau eksternal DPTSI-ITS.</li><li>• Menentukan/memilih penanggung jawab operasional dalam suatu kegiatan.</li><li>• Menentukan arah perkembangan dibidang TIK dan jaringan ITS.</li><li>• Menerima tugas lain dan memberikan laporan pertanggung jawaban ke Rektor ITS.</li><li>• Memastikan dan meninjau kesesuaian penerapan dan peningkatan SMKI.</li></ul> |           |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| C<br>(lanj.)                   | <ul style="list-style-type: none"><li>• Menyediakan arahan yang jelas pada strategi SMKI organisasi dalam mengelola keamanan informasi.</li><li>• Mendukung pimpinan untuk mencapai sasaran strategis organisasi, terutama dalam keamanan informasi.</li></ul> <p>Sedangkan tanggung jawab Subdit Infrastruktur adalah:</p> <ul style="list-style-type: none"><li>• Merawat jaringan <i>backbone</i> ITS.</li><li>• Mengembangkan desain, <i>administrator</i> dan aplikasi jaringan.</li><li>• Mengembangkan dan merawat jaringan <i>INHERENT</i>.</li><li>• Membuat modul pelatihan <i>administrator</i> jaringan komputer.</li><li>• Mengkonfigurasi dan merawat perangkat keras dan perangkat jaringan.</li><li>• Pemeliharaan <i>website</i> ITS (<a href="https://its.ac.id">https://its.ac.id</a>).</li><li>• Merencanakan, mengerakkan, dan mengatur aktifitas yang berkaitan dengan SMKI.</li><li>• Mengelola aktifitas manajemen resiko dan beberapa dokumen terkait SMKI.</li></ul> <p>Selain itu peran dan tanggung jawab keamanan informasi di DPTSI-ITS dapat dilihat secara lengkap pada <b>Gambar 4.10</b> tentang struktur tim pengelola SMKI.</p> |           |
| A.7.2. Selama karyawan bekerja |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |
| A.7.2.2                        | Kesadaran, pendidikan dan pelatihan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Compliant |
|                                | Apakah semua karyawan dan kontraktor menerima program kesadaran keamanan dan pelatihan, serta pembaharuan berkala pada kebijakan dan prosedur yang terkait pekerjaanya?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |           |
| C                              | Untuk program kesadaran keamanan, DPTSI-ITS mengadakan program bagi karyawan, dosen, mahasiswa dan pemangku kepentingan lainnya melalui empat cara, yaitu pemasangan poster di beberapa tempat mading dilingkungan ITS, melakukan <i>posting</i> ke <i>website</i> DPTSI-ITS, acara seminar dan pemasangan <i>screensaver</i> pada setiap komputer/laptop dinas (khusus didalam ruang lingkup DPTSI-ITS saja). Selain itu DPTSI-ITS mengadakan program kesadaran keamanan sekaligus memberitahukan kebijakan dan prosedur tentang keamanan informasi yang terkait kepada karyawan yang baru masuk baik PNS, non-PNS ataupun magang.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |           |

|                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C<br>(lanj.)                               | DPTSI-ITS mendokumentasikan perencanaan pelatihan tentang keamanan informasi kedalam format matriks yang bernama Matriks Kebutuhan Program Kesadaran Keamanan. Isi dari matriks ini adalah peserta (internal DPTSI-ITS atau pengguna sistem), waktu, materi/topik, narasumber dan jenis program (seminar, madding ITS, publikasi <i>website</i> , atau pembaharuan <i>screensaver</i> ).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| C                                          | <p>Berikut ini adalah pelatihan kerja yang diadakan oleh DPTSI-ITS:</p> <ul style="list-style-type: none"> <li>• Untuk sosialisasi pelatihan sistem, DPTSI-ITS melakukan sosialisasi pelatihan sistem untuk sistem informasi atau layanan TIK yang digunakan didalam lingkungan ITS kepada pemangku kepentingan terkait. Hasil aktifitas sosialisasi pelatihan sistem biasanya didokumentasikan di <i>website</i> DPTSI-ITS.</li> <li>• Untuk pelatihan dan sertifikasi kerja, DPTSI-ITS memberikan pelatihan kerja kepada karyawan dan mendokumentasikan perencanaan pelatihan kerja yang akan diberikan kedalam format matriks yang bernama Matriks Kebutuhan Pelatihan SDM. Isi dari matriks ini adalah nama karyawan, pelatihan yang akan diberikan (seperti Ms. SQL Server, Linux, pemrograman <i>web</i> (<i>PHP</i> dan <i>framework</i>-nya), pemasangan dan perbaikan <i>fiber optic</i>, sertifikasi CISCO dan lainnya), dan jadwal pelatihannya.</li> </ul>                                                                                                                                                                                                        |
| C                                          | <p>Untuk menilai penyerapan ilmu pada pelatihan atau program yang dilakukan ke karyawan, DPTSI-ITS melakukan pengujian untuk pelatihan kerja, seperti terdapat daftar pertanyaan sebelum dilakukan pelatihan dan setelahnya untuk dapat memperkirakan seberapa besar ilmu yang diserap. Selain itu juga pengadaan pelatihan kerja umumnya dilakukan berdasarkan kebutuhan dalam penanganan masalah atau melakukan aktifitas tertentu. Contohnya Subdit Pengembangan mulai menggunakan <i>framework</i> Laravel dan memerlukan pelatihan kerja penggunaan <i>framework</i>. Jadi penilaian dapat dilakukan dengan meihat apakah karyawan tersebut mampu menggunakan <i>framework</i> setelah dilakukan pelatihan.</p> <p>DPTSI-ITS juga melakukan pengujian tingkat kesadaran terhadap keamanan informasi bagi semua pemangku kepentingan melalui Integra ITS setiap 6 bulan sekali sebelum mengakses Integra ITS. Pengujian berisikan pertanyaan tentang isu-isu keamanan informasi, membedakan mana yang baik dan buruk pada aktifitas penggunaan TIK, kontrol keamanan apa yang harusnya dipasang di komputer atau perangkat <i>mobile</i> yang digunakan, dan lainnya.</p> |
| <b>A.8.1. Tanggung jawab terhadap aset</b> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                  |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| A.8.1.1 | Inventaris aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <i>Compliant</i> |
|         | Apakah aset yang berhubungan dengan informasi dan fasilitas pendukungnya diidentifikasi dan daftar inventarisnya didokumentasikan dan dikelola?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                  |
| C       | <ul style="list-style-type: none"> <li>• Aset Barang Milik Negara (BMN) didokumentasikan kedalam sistem E-Aset dan <i>file</i> Daftar Inventaris Aset oleh karyawan penyusun laporan dan pengelola BMN dibawah Subdit Infrastruktur. Yang termasuk BMN adalah perangkat keras (komputer, <i>server</i>, <i>printer</i>, komponennya, dan lainnya), perangkat jaringan (<i>router</i>, <i>firewall</i>, <i>switch</i> dan lainnya), perangkat lunak (pengolah gambar, kantor dan lainnya), perangkat perlengkapan (<i>AC</i>, <i>UPS</i>, <i>diesel generator</i>, dan lainnya), dan furnitur (kursi, meja, lemari dan lainnya). Dokumen ini berisikan kode barang, nama barang, merek/tipe, jumlah total barang, jumlah barang yang dipasang dan cadangannya (khusus untuk perangkat keras/jaringan), tanggal garansi habis (khusus untuk perangkat keras/jaringan), lokasi barang dan kondisi barang.</li> <li>• Aset SIM didokumentasikan kedalam <i>file</i> Daftar Inventaris SIM oleh Subdit Pengembang. Yang didokumentasikan adalah semua sistem informasi yang dikembangkan di DPTSI-ITS, sedangkan yang dikembangkan masing-masing oleh unit atau jurusan tidak termasuk. Dokumen ini berisikan nama SIM, modul dan fitur yang dimiliki, <i>log</i> aktifitas pengembangan, alamat <i>IP address</i>, <i>server</i> yang dimiliki (<i>development</i> dan/atau <i>live</i>), yang mengelola sekarang, nama pengembang, tahun berapa dikembangkan, dana yang diperlukan (jika ada).</li> <li>• Aset data/informasi didokumentasikan kedalam Daftar Rekaman Mutu. Dokumen ini berisikan judul rekaman (contohnya arsip keuangan), masa simpan (dalam tahun), lokasi simpan (contohnya almari kas keuangan), penanggung jawab (Subdit/jabatan), metode indeks (kelompok/urut abjad/urut tanggal).</li> <li>• Aset informasi yang dibuat, dikelola atau digunakan oleh masing-masing Subdit dan karyawan DPTSI-ITS lainnya kedalam Daftar Inventaris Aset Informasi. Dokumen ini berisikan nomor aset, nama aset, jenis aset (informasi, perangkat keras, perangkat lunak, dan lainnya sesuai dengan penelitian ini), bentuk aset (fisik/nyata/<i>hardcopy</i> atau <i>logic</i>/tidak nyata/<i>softcopy</i>), lokasi aset, dan pemilik aset.</li> </ul> |                  |
| A.8.1.2 | Kepemilikan aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <i>Compliant</i> |

|                                 |                                                                                                                                                                                                                                                                                                                                                                                    |                     |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                                 | Apakah setiap aset yang dikelola pada inventaris terdapat pemilik atau pengelolanya?                                                                                                                                                                                                                                                                                               |                     |
| C                               | DPTSI-ITS memiliki dokumen pemilik aset yang berisikan siapa yang bertanggung jawab terhadap aset (pemilik aset) pada masing-masing aset secara lengkap dan jelas. Contohnya AC dan UPS pemilik asetnya adalah bapak Bustari, atau materi pelatihan dan dokumen ISO 9000 pemilik asetnya adalah ibu Widiyaningsih.                                                                 |                     |
| A.8.1.4                         | Pengembalian aset                                                                                                                                                                                                                                                                                                                                                                  | Partially compliant |
|                                 | Apakah semua karyawan dan pihak ketiga mengembalikan semua aset yang dimiliki ketika pemberhentian atau kontrak kerja karyawan?                                                                                                                                                                                                                                                    |                     |
| PC                              | Untuk pengembalian aset yang dipinjam karyawan, DPTSI-ITS mengharuskan karyawan yang keluar mengembalikan aset yang dipinjam (contohnya laptop dinas). Yang mengurus peminjaman dan pengembalian adalah karyawan penyusun laporan dan pengelola BMN. Namun DPTSI-ITS tidak memiliki dokumentasi prosedur pengembalian aset yang dipinjam karyawan yang berhenti atau mutasi kerja. |                     |
| C                               | Untuk penyerapan ilmu karyawan yang dimiliki, DPTSI-ITS menerapkan <i>knowledge management</i> untuk mendokumentasikan ilmu-ilmu yang dimiliki karyawan selama bekerja di DPTSI-ITS.                                                                                                                                                                                               |                     |
| A.8.2. Klasifikasi informasi    |                                                                                                                                                                                                                                                                                                                                                                                    |                     |
| A.8.2.1                         | Klasifikasi informasi                                                                                                                                                                                                                                                                                                                                                              | Compliant           |
|                                 | Apakah informasi diklasifikasikan berdasarkan nilai, kekritisannya, atau kerahasiaan?                                                                                                                                                                                                                                                                                              |                     |
| C                               | DPTSI-ITS memiliki dokumentasi klasifikasi kerahasiaan informasi berdasarkan tingkatan publik, internal dan rahasia untuk setiap data yang diolah sistem informasi ( <i>database</i> ), data yang dibuat sistem ( <i>log, backup, file konfigurasi, ID login</i> ), maupun data yang diolah manual baik berbentuk <i>file (worksheet, spreadsheet)</i> atau dokumen kertas.        |                     |
| A.9.2. Manajemen akses pengguna |                                                                                                                                                                                                                                                                                                                                                                                    |                     |

|           |                                                                                                                                                                                                                                                                                                                                     |                            |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| A.9.2.2   | Penyediaan akses pengguna                                                                                                                                                                                                                                                                                                           | <i>Partially compliant</i> |
|           | Apakah proses penyediaan akses pengguna secara formal diterapkan untuk memberikan dan menghapus hak akses untuk semua tipe pengguna pada semua sistem dan layanan?                                                                                                                                                                  |                            |
| <i>C</i>  | Untuk otorisasi hak akses pada perangkat, DPTSI-ITS melakukan otorisasi hak akses yang dilakukan oleh pemilik aset pada perangkat tersebut. Contohnya pemilik aset perangkat <i>firewall</i> memberikan otorisasi hak akses kepada karyawan baru yang ditunjuk sebagai salah satu pengelola <i>firewall</i> .                       |                            |
| <i>C</i>  | Untuk verifikasi dalam pemberian hak akses, DPTSI-ITS melakukan verifikasi apakah hak akses yang diberikan sesuai dengan tugas yang diemban karyawan tersebut, serta melakukan verifikasi dengan kebijakan kontrol akses.                                                                                                           |                            |
| <i>C</i>  | Untuk pembatasan hak akses yang aktif sebelum prosedur otorisasi, DPTSI-ITS melakukan pembatasan hanya hak akses yang diberikan secara prosedural saja yang aktif.                                                                                                                                                                  |                            |
| <i>C</i>  | Untuk rekaman hak akses yang diberikan, DPTSI-ITS merekam hak akses yang dimiliki oleh karyawan pada <i>server</i> , perangkat lunak, perangkat jaringan dan akses fisik.                                                                                                                                                           |                            |
| <i>PC</i> | Untuk peninjauan hak akses, DPTSI-ITS melakukannya berdasarkan kontrol A.9.2.5. Meninjau hak akses pengguna. Namun tidak semua perangkat yang dilakukan peninjauan.                                                                                                                                                                 |                            |
| <i>C</i>  | Untuk dokumentasi prosedur penyediaan hak akses pengguna, DPTSI-ITS memiliki dokumentasi prosedur untuk sistem informasi, <i>server</i> , perangkat jaringan, komputer/laptop dinas dan akses fisik yang berisikan verifikasi tingkatan hak akses sesuai tugas, pemberian persetujuan, dokumentasi hak akses pengguna, dan lainnya. |                            |
| <i>C</i>  | Untuk dokumentasi prosedur penghapusan/pencabutan hak akses pengguna, DPTSI-ITS memiliki dokumentasi prosedur untuk sistem informasi, <i>server</i> , perangkat jaringan, komputer/laptop dinas dan akses fisik yang berisikan langkah-langkah dalam penghapusan hak akses.                                                         |                            |
| A.9.2.3   | Manajemen hak akses <i>administrator</i>                                                                                                                                                                                                                                                                                            | <i>Compliant</i>           |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | Apakah alokasi dan penggunaan hak akses <i>administrator</i> dikontrol dan dibatasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| C | Untuk identifikasi hak akses apa saja yang dimiliki setiap sistem, DPTSI-ITS belum memiliki dokumentasinya baik untuk sistem operasi, <i>DBMS</i> dan aplikasi lainnya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| C | Untuk persyaratan hak akses minimum ( <i>least privilege</i> ), DPTSI-ITS mengatur semua hak akses yang diberikan berdasarkan peran karyawan. Misalnya hak akses <i>administrator</i> Webmail ITS yang dimiliki oleh Subdit Pelayanan untuk mengelola akun <i>email</i> pengguna, dan hak akses <i>administrator server</i> dimiliki oleh Subdit Infrastruktur untuk mengelola <i>server</i> . Selain itu dilakukan pembatasan dan penerapan tingkatan hak akses untuk komputer dan <i>server</i> dengan membatasi fungsi apa saja yang bisa dilakukan oleh karyawan tertentu. Misalnya hak akses dibagi menjadi tiga tingkatan yaitu pengguna biasa, <i>administrator</i> (yang dibatasi akses dan modifikasi <i>file log</i> ), dan <i>administrator</i> penuh. |
| C | Untuk rekaman hak akses yang diberikan, DPTSI-ITS merekam hak akses yang diberikan dan dimiliki karyawan termasuk hak akses <i>administrator</i> berdasarkan kontrol A.9.2.2. Penyediaan akses pengguna                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| C | Untuk kebutuhan hak akses <i>administrator</i> yang berjangka waktu ( <i>expired</i> ), DPTSI-ITS memberikan hak akses yang berjangka waktu ( <i>expired</i> ) kepada karyawan yang bukan pemilik aset jika diperlukan saja, misalnya membantu karyawan pemilik aset dalam <i>troubleshooting</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| C | Untuk pemisahan hak akses <i>administrator</i> dari penggunaan aktifitas biasa, DPTSI-ITS memisahkan penggunaan antara aktifitas biasa maupun aktifitas <i>administrator</i> . Hal ini dilakukan dengan cara memberikan dua jenis hak akses bagi <i>administrator</i> , satu untuk aktifitas <i>administrator</i> dan lainnya untuk aktifitas biasa.                                                                                                                                                                                                                                                                                                                                                                                                              |
| C | Untuk peninjauan apakah karyawan berkompetensi terhadap hak akses <i>administrator</i> yang dimiliki, DPTSI-ITS tidak melakukannya. Namun DPTSI-ITS mengadakan pelatihan kerja untuk meningkatkan kompetensi karyawan dalam melakukan pekerjaannya berdasarkan kontrol A.7.2.2. Kesadaran, pendidikan dan pelatihan keamanan informasi.                                                                                                                                                                                                                                                                                                                                                                                                                           |



|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                            |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| C       | Untuk dokumentasi prosedur pengecekan <i>password default</i> vendor, DPTSI-ITS memiliki dokumentasi prosedur yang berisikan langkah-langkah dalam pemeriksaan apakah terdapat <i>password default</i> pada perangkat yang digunakan dan belum diganti.                                                                                                                                                                                                                                                                                                                                                                                                |                            |
| C       | Untuk dokumentasi prosedur pengelolaan <i>sharing password administrator generic</i> , DPTSI-ITS memiliki dokumentasi prosedur yang berisikan langkah-langkah penggantian <i>password</i> secara berkala atau jika terdapat pengguna yang berhenti kerja, pemilihan kekuatan <i>password</i> , dan pengkomunikasian ke pengguna.                                                                                                                                                                                                                                                                                                                       |                            |
| A.9.2.4 | Manajemen informasi autentikasi rahasia dari pengguna                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <i>Partially compliant</i> |
|         | Apakah alokasi informasi <i>password</i> pengguna dikontrol melalui proses formal?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                            |
| PC      | Untuk perjanjian kerahasiaan informasi (termasuk <i>password</i> ), setiap karyawan PNS diharuskan mengucapkan sumpah/janji karyawan PNS dan Subdit Pengembangan diharuskan menandatangani perjanjian kerahasiaan sebelum diberikan akses kedalam sistem informasi yang akan dikelola berdasarkan kontrol A.13.2.4. Perjanjian kerahasiaan atau tidak menyebarkan informasi. Namun hal tersebut tidak melingkupi untuk semua karyawan.                                                                                                                                                                                                                 |                            |
| PC      | Untuk pemaksaan perubahan <i>password</i> sementara yang diberikan saat pemberian <i>password</i> pertama kali atau <i>reset password</i> , hanya <i>server</i> saja yang diatur, dan tidak mencakup Webmail ITS dan komputer/laptop dinas berdasarkan kontrol A.9.4.3. Sistem manajemen <i>password</i> .                                                                                                                                                                                                                                                                                                                                             |                            |
| C       | Untuk dokumentasi prosedur <i>reset password</i> , DPTSI-ITS memiliki: <ul style="list-style-type: none"> <li>• Prosedur Layanan <i>E-Mail: Reset Password</i> untuk melakukan <i>reset password</i> akun <i>email</i> yang dapat dilakukan dengan tiga cara yaitu mengunjungi DPTSI-ITS, mengirim surat permohonan, dan melakukan <i>reset password</i> akun <i>email</i> secara <i>online</i>.</li> <li>• Prosedur <i>reset password</i> sistem dan perangkat yang berisikan langkah-langkah dalam <i>reset password</i> untuk sistem informasi, <i>server</i>, perangkat jaringan atau komputer/laptop dinas didalam ruang lingkup SMKI.</li> </ul> |                            |

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                     |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| NC                                       | Untuk pengiriman <i>password</i> sementara secara aman, DPTSI-ITS menggunakan <i>email</i> untuk pengiriman <i>password</i> sementara ke pengguna jika pengguna tidak menspesifikasikan <i>password</i> barunya melalui surat. Bahkan surat permohonan terkadang dikirim melalui <i>email</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                     |
| PC                                       | Untuk keunikan <i>password</i> sementara yang diberikan, <i>password</i> sementara yang diberikan dengan cara datang langsung ataupun pengiriman surat permohonan tidaklah unik dan mudah ditebak (jika pengguna tidak menspesifikasikan <i>password</i> barunya). Sedangkan <i>password</i> sementara yang diberikan melalui formulir lupa <i>password</i> memiliki kombinasi <i>password</i> acak yang tidak mudah ditebak dan aman.                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                     |
| C                                        | Untuk penggantian <i>password default</i> vendor, DPTSI-ITS menggantinya disaat pemasangan perangkat keras/lunak/jaringan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                     |
| A.9.2.5                                  | Meninjau hak akses pengguna                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Compliant           |
|                                          | Apakah pemilik aset meninjau hak akses pengguna dalam jangka waktu tertentu?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                     |
| PC                                       | <ul style="list-style-type: none"> <li>• Untuk kontrol <i>logic</i> (<i>server</i>, perangkat lunak dan perangkat jaringan) dilakukan peninjauan apakah terdapat hak akses yang belum terhapus didalam sistem, dan pengecekan kesesuaian hak akses yang diberikan dengan pekerjaan yang dilakukan karyawan. DPTSI-ITS juga memiliki dokumentasi prosedur peninjauan hak akses pengguna yang dilakukan satu tahun sekali atau terdapat karyawan yang berhenti atau mutasi.</li> <li>• Untuk kontrol fisik (perangkat <i>fingerprint</i>, rekaman <i>CCTV</i>, dan kunci pintu <i>analog</i>). DPTSI-ITS tidak dilakukan peninjauan apakah terdapat data <i>fingerprint</i> yang belum terhapus dan kunci yang belum dikembalikan. Namun DPTSI-ITS melakukan peninjauan aktifitas mencurigakan pada <i>CCTV</i> untuk jangka waktu tertentu dan terdapat dokumentasi prosedurnya.</li> </ul> |                     |
| A.9.4. Kontrol akses sistem dan aplikasi |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                     |
| A.9.4.3                                  | Sistem manajemen <i>password</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Partially compliant |
|                                          | Apakah terdapat sistem manajemen <i>password</i> yang gencar dan memastikan kualitas <i>password</i> ?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                     |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PC                | <ul style="list-style-type: none"> <li>• Untuk Webmail ITS sudah diatur agar menggunakan <i>password</i> yang aman, seperti panjang <i>password</i> minimal 8 karakter, mencegah penggunaan <i>password</i> yang sama, dan tidak menampilkan <i>password</i> yang dimasukkan. Namun tidak ada keharusan kualitas kombinasi karakter, mengganti <i>password</i> baru/hasil <i>reset</i> pada saat <i>login</i> pertama kali, dan mengganti <i>password</i> secara berkala.</li> <li>• Untuk <i>server</i> sudah diatur agar menggunakan <i>password</i> yang aman, seperti panjang <i>password</i> minimal 8 karakter, penggunaan kualitas kombinasi karakter, mencegah penggunaan <i>password</i> yang sama, tidak menampilkan <i>password</i> yang dimasukkan, harus mengganti <i>password</i> saat <i>login</i> pertama kali, dan harus mengganti <i>password</i> secara berkala.</li> <li>• Untuk komputer dan laptop dinas milik DPTSI-ITS sudah diatur agar menggunakan <i>password</i> yang aman, seperti panjang <i>password</i> minimal 8 karakter, penggunaan kualitas kombinasi karakter, mencegah penggunaan <i>password</i> yang sama, tidak menampilkan <i>password</i> yang dimasukkan, harus mengganti <i>password</i> saat <i>login</i> pertama kali, dan harus mengganti <i>password</i> secara berkala.</li> </ul> |
| A.11.2. Peralatan |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| A.11.2.2          | <div>Utilitas pendukung</div> <div>Compliant</div> <div>Apakah peralatan dilindungi dari kegagalan daya dan gangguan lainnya yang disebabkan gangguan pada utilitas pendukung?</div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| C                 | <p>Untuk melindungi peralatan dan perangkat dari kegagalan daya, Subdit Infrastruktur menggunakan <i>diesel generator</i> dan <i>UPS</i>. <i>Diesel generator</i> berfungsi untuk menangani kehilangan pasokan listrik yang berjalan secara otomatis ketika terjadi mati listrik. Sedangkan <i>UPS</i> difungsikan untuk membantu jeda waktu perangkat <i>diesel generator</i> untuk aktif dalam memasok listrik, dimana perangkat ini bekerja secara terus menerus (<i>standby-online</i>). <i>Diesel generator</i> dan <i>UPS</i> yang dipasang hanya memasok aliran listrik ke semua perangkat yang ada di ruang pusat data, tidak diatur agar memasok ke semua ruangan di DPTSI-ITS. Untuk melindungi perangkat komputer dari kegagalan daya, setiap perangkat juga dipasang <i>UPS</i> dengan daya rendah yang hanya mampu digunakan beberapa menit untuk menyimpan hasil pekerjaan.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                        |

|          |                                                                                                                                                                                                                                                                                                                                                                                    |                  |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| C        | Untuk memenuhi kapasitas perkembangan bisnis, Subdit Infrastruktur melakukan pengecekan dan perencanaan secara berkala apakah kapasitas sistem baik jaringan dan <i>server</i> saat ini memenuhi perkembangan bisnis kedepannya berdasarkan kontrol A.12.1.3. Manajemen kapasitas.                                                                                                 |                  |
| C        | Untuk memastikan perangkat berjalan dengan benar, Subdit Infrastruktur juga melakukan perawatan perangkat dan peralatan yang ada agar dapat beroperasi terus menerus berdasarkan kontrol A.11.2.4. Pemeliharaan perlengkapan.                                                                                                                                                      |                  |
| C        | Untuk mendeteksi malfungsi pada perangkat, Subdit Infrastruktur menggunakan Nagios dan ITS Web Monitoring System untuk mengawasi kondisi operasional (hidup-mati atau gangguan) pada perangkat jaringan, absensi <i>fingerprint</i> dan <i>server</i> berdasarkan kontrol A.13.1.1. Kontrol jaringan.                                                                              |                  |
| C        | Untuk macam-macam rute fisik yang berganda, Subdit Infrastruktur menggunakan topologi STAR dan RING pada infrastruktur jaringannya agar memiliki beberapa titik untuk <i>me-routing</i> jika terdapat satu jalur komunikasi yang bermasalah berdasarkan kontrol A.13.1.3. Pemisahan pada jaringan.                                                                                 |                  |
| C        | Untuk sumber penerangan dan komunikasi cadangan, Subdit Infrastruktur memiliki beberapa senter dan <i>walkie-talkie</i> jika terjadi keadaan darurat.                                                                                                                                                                                                                              |                  |
| C        | Untuk tombol keadaan darurat, Subdit Infrastruktur memiliki kotak panel yang terdapat tombol keadaan darurat untuk sumber daya listrik pada ruangan pusat data berdasarkan kontrol A.11.2.3. Keamanan pemasangan kabel.                                                                                                                                                            |                  |
| C        | Untuk redundansi konektifitas jaringan, DPTSI-ITS memiliki dua layanan <i>ISP</i> yaitu PT. Telkom dan PT.X.                                                                                                                                                                                                                                                                       |                  |
| A.11.2.3 | Keamanan pemasangan kabel                                                                                                                                                                                                                                                                                                                                                          | <i>Compliant</i> |
|          | Apakah kabel listrik dan jaringan dilindungi dari gangguan dan kerusakan?                                                                                                                                                                                                                                                                                                          |                  |
| C        | Untuk perlindungan kabel didalam gedung, kabel listrik dan jaringan dilindungi oleh pipa pelindung kabel. Hal ini dapat dilihat pada <b>Gambar F.97</b> . Sedangkan untuk perlindungan kabel yang ada diluar gedung, kabel dilindungi oleh pipa pelindung kabel, dan saluran beton bertulang berbentuk penampang huruf U (U-Ditch) didalam tanah. Selain itu di setiap jalur kabel |                  |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                  |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| C<br>(lanj.) | listrik dan jaringan didalam tanah diberikan patok penanda kabel agar memudahkan karyawan proyek menemukan lokasi kabel, seperti "FO" untuk kabel <i>fiber optic</i> dan "2.0 VA" untuk kabel listrik. Hal ini dapat dilihat pada <b>Gambar F.98</b> sampai <b>Gambar F.100</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                  |
| C            | Untuk melindungi dari gangguan/interfensi elektromagnetik pada data, DPTSI-ITS memisahkan kabel listrik dengan kabel jaringan ketika pemasangan. Kabel listrik dipasang didalam lantai, sedangkan untuk kabel jaringan dipasang didalam langit-langit ruangan. Untuk perlindungan tambahan, hal ini tidak diperlukan karena penggunaan kabel <i>fiber optic</i> yang tahan akan interfensi untuk jalur koneksi tertentu.                                                                                                                                                                                                                                                                                                                                                                  |                  |
| NA           | Untuk perlindungan <i>port</i> koneksi dari akses tanpa izin secara fisik, tidak perlu dilakukan pemasangan. Hal ini dikarenakan berdasarkan kontrol A.9.1.2. Akses ke jaringan dan layanan jaringan, untuk melakukan koneksi ke jaringan di lingkungan ITS diperlukan <i>login</i> ke Integra ITS. Halaman <i>login</i> Integra ITS dapat dilihat pada <b>Gambar F.51</b> .                                                                                                                                                                                                                                                                                                                                                                                                              |                  |
| C            | Untuk perlindungan kontrol panel listrik dari akses tanpa izin secara fisik, kontrol panel diletakkan didalam ruangan pusat data. Hal ini dapat dilihat pada <b>Gambar F.95</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                  |
| C            | <p>Untuk menjaga dari kerusakan kabel, DPTSI-ITS memiliki kontrol seperti:</p> <ul style="list-style-type: none"> <li>• Dokumentasi panduan untuk menginspeksi adanya kerusakan kabel seperti secara berkala dengan nama panduan Pengujian Kabel <i>UTP</i> dan panduan Pengujian Kabel <i>Fiber Optic</i>.</li> <li>• Dokumentasi panduan pemasangan kabel dengan nama panduan Perakitan Kabel (Kabel <i>UTP</i>) dan panduan Perakitan Kabel (<i>Fiber Optic</i>).</li> <li>• Perangkat pemasangan dan pengecekan kabel <i>UTP</i> dan <i>fiber optic</i> seperti <i>tester</i>, <i>crimping tool</i>, kabel cadangan, <i>jack</i>, <i>panel</i> dan lainnya.</li> <li>• Kualifikasi/sertifikasi karyawan dalam pemasangan kabel <i>UTP</i>, <i>fiber optic</i> dan listrik.</li> </ul> |                  |
| A.11.2.4     | Pemeliharaan perlengkapan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <i>Compliant</i> |
|              | Apakah peralatan dipelihara/dirawat secara benar untuk memastikan integritas dan ketersediaanya?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                  |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C | <p>DPTSI-ITS melakukan aktifitas pemeriksaan serta perawatan perangkat secara fisik dan berkala untuk menjaga kelancaran operasional perangkat. Berikut ini adalah aktifitas pemeriksaan dan perawatan terhadap beberapa perangkat yang dilakukan:</p> <ul style="list-style-type: none"> <li>• <i>Diesel generator</i> dilakukan dengan aktifitas pemanasan mesin selama satu minggu sekali, sekaligus pengecekan air aki dan kondisi radiatornya berdasarkan prosedur dari vendor. Selain itu dilakukan juga penggantian oli mesin selama satu tahun sekali.</li> <li>• <i>UPS</i> dilakukan dengan aktifitas pengecekan tegangan maupun informasi kondisi yang ditampilkan pada indikator/panel perangkat selama dua minggu sekali berdasarkan prosedur dari vendor. Jika baterai <i>UPS</i> sudah habis atau rusak, maka dilakukan penggantian baterai. Prosedur ini didokumentasikan dengan nama Penggantian Baterai <i>UPS</i> yang dapat dilihat pada <b>Gambar F.103</b>.</li> <li>• <i>AC</i> dilakukan dengan aktifitas pembersihan komponen didalam perangkat seperti <i>filter</i> selama 3 bulan sekali. Prosedur ini didokumentasikan dengan nama Perawatan <i>AC</i> yang dapat dilihat pada <b>Gambar F.104</b>. Listrik dan perangkat pengamanannya dilakukan dengan aktifitas pemeriksaan tegangan dan arus, lalu melaporkannya ke PLN jika terdapat penyimpangan selama 6 bulan sekali. Sedangkan untuk perangkat <i>grounding</i> dilakukan dengan aktifitas pemeriksaan nilai arus pada perangkat. Prosedur tersebut didokumentasikan dengan nama Perawatan Listrik yang dapat dilihat pada <b>Gambar F.105.</b>, dan Perawatan <i>Grounding</i> yang dapat dilihat pada <b>Gambar F.106</b>.</li> <li>• <i>Switch</i> dilakukan dengan aktifitas pembersihan perangkat dari debu dan mengecek kondisi komponen apakah terdapat kerusakan fisik atau tidak selama 6 bulan sekali. Prosedur ini didokumentasikan dengan nama Perawatan <i>Switch</i> yang dapat dilihat pada <b>Gambar F.107</b>.</li> <li>• <i>Server</i> dilakukan dengan aktifitas pembersihan perangkat dari debu dan mengecek kondisi komponen apakah terdapat kerusakan fisik atau tidak selama 6 bulan sekali. Prosedur tersebut didokumentasikan dengan nama prosedur Perawatan <i>Server</i>.</li> <li>• Komputer/laptop dinas dilakukan dengan aktifitas pembersihan perangkat dari debu dan mengecek kondisi komponen apakah terdapat kerusakan fisik atau tidak selama 1 tahun sekali. Prosedur tersebut didokumentasikan dengan nama prosedur Perawatan Komputer/ Laptop Dinas.</li> </ul> |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C<br>(lanj.) | Selain itu dilakukan perekaman riwayat setiap pemeriksaan dan perawatan perangkat menggunakan <i>checklist</i> waktu, nama perangkat dan tanggal pemeriksaan/perawatan yang dapat membantu apakah perangkat sudah dirawat secara terjadwal atau tidak.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| C            | Untuk karyawan yang merawat perangkat adalah yang bertanggung jawab terhadap aset tersebut, contohnya karyawan Subdit Infrastruktur yang melakukan perawatan <i>server</i> dan <i>router</i> , bukan karyawan Subdit Pengembangan atau Subdit Pelayanan. Apabila terdapat kerusakan pada <i>server</i> , <i>router</i> , <i>switch</i> , <i>access point</i> , <i>firewall</i> , <i>printer/scanner/fax</i> , <i>diesel generator</i> , <i>UPS</i> , pendingin ruangan/ <i>AC</i> , komponen perangkat dan lainnya, DPTSI-ITS memanggil vendor untuk memperbaiki jika masih dalam masa garansi setelah diinspeksi dan diperkirakan apa yang rusak (perangkat atau komponen). Sedangkan jika perangkat tersebut sudah melewati masa garansi, maka DPTSI-ITS mengganti perangkat tersebut dengan yang baru.                                                     |
| C            | Untuk rekaman riwayat perawatan, DPTSI-ITS merekam semua riwayat perbaikan pada perangkat yang berisikan semua kesalahan sebenarnya atau yang diperkirakan, dan semua tindakan pencegahan atau perbaikannya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| C            | Untuk melindungi informasi rahasia pada perangkat ketika masa perawatan, karyawan DPTSI-ITS mendampingi petugas perbaikan dari vendor yang akan menginspeksi dan memperbaiki perangkat, terutama jika petugas perbaikan masuk kedalam area sensitif seperti ruangan pusat data berdasarkan kontrol A.11.1.1. Kontrol keluar-masuk fisik. Apabila petugas perbaikan harus membawa perangkat milik DPTSI-ITS keluar dari kantor setelah diinspeksi, maka yang dibawa hanyalah komponen tertentu didalam perangkat jika kerusakan berada pada komponen tersebut. Sedangkan untuk kerusakan yang terjadi di keseluruhan perangkat, maka perangkat tersebut akan dilepas media penyimpanannya (jika ada) dan disimpan oleh Subdit Infrastruktur (contohnya <i>server</i> yang mengalami kerusakan pada <i>memory</i> , maka yang dibawa hanya <i>memory</i> saja). |
| NA           | Untuk perawatan yang dibutuhkan oleh kebijakan asuransi, DPTSI-ITS tidak melakukannya karena tidak memiliki kebijakan tersebut.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| C            | Untuk inspeksi untuk memastikan perangkat tidak dirubah tanpa izin setelah perawatan, DPTSI-ITS melakukan pengecekan kode <i>BIOS</i> dengan yang ada di <i>website</i> resmi vendor perangkat keras atau jaringan, apakah tidak ada penyimpangan versi setelah perangkat diperbaiki atau dibeli.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                  |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| A.11.2.8 | Peralatan pengguna yang tidak diawasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <i>Compliant</i> |
|          | Apakah pengguna menjamin bahwa peralatan yang tidak diawasi telah terlindungi (misalnya menggunakan <i>screensaver</i> atau <i>logout</i> otomatis)?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                  |
| C        | <ul style="list-style-type: none"> <li>• Untuk Webmail ITS diatur agar melakukan <i>log-out</i> secara otomatis, dimana pengguna tidak dapat mengakses kembali meskipun sebelumnya pengguna tersebut tidak melakukan <i>log-out</i> setelah selesai menggunakan.</li> <li>• Untuk perangkat jaringan dan <i>server</i>, karyawan yang akan mengakses <i>control panel</i> pada perangkat jaringan seperti <i>switch</i>, <i>router</i> dan <i>firewall</i> diperlukan <i>login administrator</i> ulang secara <i>default</i>. Sistem operasi Linux yang dipasang di beberapa <i>server</i> juga memerlukan karyawan untuk <i>login</i> ulang untuk melakukan koneksi <i>remote</i>.</li> <li>• Untuk komputer dan laptop dinas milik DPTSI-ITS, DPTSI-ITS mengatur agar sistem menjalankan <i>screensaver</i> yang diberi <i>password</i> ketika tidak digunakan atau ditinggal.</li> </ul>                                                                                                                                     |                  |
| A.11.2.9 | Kebijakan merapihkan meja dan membersihkan layar                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <i>Compliant</i> |
|          | Apakah kebijakan merapihkan meja untuk kertas dan <i>flashdisk</i> , dan kebijakan membersihkan layar diterapkan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                  |
| C        | <p>DPTSI-ITS memiliki dokumentasi kebijakan <i>clear desk and screen</i> yang berisikan aturan terkait kerapihan meja kerja dari dokumen, <i>flashdisk</i> atau media penyimpanan lainnya, maupun membersihkan layar monitor dari catatan terutama informasi akun pengguna. Sebagian topik yang terdapat pada kebijakan adalah:</p> <ul style="list-style-type: none"> <li>○ Mengunci dokumen rahasia/sensitif langsung didalam lemari jika tidak diperlukan (tidak meninggalkan di meja).</li> <li>○ Tidak menaruh <i>CD/DVD</i>, <i>flashdisk</i> atau <i>hardisk</i> eksternal di meja.</li> <li>○ Tidak meninggalkan dokumen apapun di <i>printer</i> atau <i>scanner</i> terutama yang bersifat sensitif.</li> <li>○ Tidak mencatat dan menempel kertas pada layar yang berisi <i>password</i> atau informasi rahasia apapun.</li> <li>○ Tidak meninggalkan komputer dalam keadaan tidak terkunci <i>password</i> dan <i>log-off</i>.</li> <li>○ Langsung menghapus tulisan di <i>whiteboard</i> setelah rapat.</li> </ul> |                  |



| <b>A.12. Keamanan Operasional</b>                      |                                                                                                                                                                                                                                                             |                            |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| <b>A.12.1. Prosedur operasional dan tanggung jawab</b> |                                                                                                                                                                                                                                                             |                            |
| A.12.1.1                                               | Mendokumentasikan prosedur operasional                                                                                                                                                                                                                      | <i>Partially compliant</i> |
|                                                        | Apakah prosedur operasional didokumentasikan dan tersedia untuk semua pengguna yang membutuhkan?                                                                                                                                                            |                            |
| <i>C</i>                                               | DPTSI-ITS memiliki dokumen ISO 9000 yang berisi berbagai dokumen, prosedur, instruksi kerja, dan formulir untuk menjalankan aktifitas bisnis di DPTSI-ITS. Dokumen ini disimpan di Subdit Pelayanan, dimana pengguna yang ingin mengakses dapat melihatnya. |                            |
| <i>NC</i>                                              | Prosedur kontak dukungan dan eskalasi (A.6.1.3) belum didokumentasikan.                                                                                                                                                                                     |                            |
| <i>NC</i>                                              | Prosedur pengembalian aset (A.8.1.4) belum didokumentasikan.                                                                                                                                                                                                |                            |
| <i>NC</i>                                              | Prosedur pemberian <i>label</i> klasifikasi informasi (A.8.2.2) belum didokumentasikan.                                                                                                                                                                     |                            |
| <i>NC</i>                                              | Prosedur penanganan aset (A.8.2.3) belum didokumentasikan.                                                                                                                                                                                                  |                            |
| <i>NC</i>                                              | Prosedur <i>removable media</i> (A.8.3.1) belum didokumentasikan.                                                                                                                                                                                           |                            |
| <i>C</i>                                               | Prosedur pemusnahan dokumen (A.8.3.2) sudah didokumentasikan.                                                                                                                                                                                               |                            |
| <i>C</i>                                               | Prosedur pembuatan akun <i>email</i> (A.9.2.1) sudah didokumentasikan.                                                                                                                                                                                      |                            |
| <i>C</i>                                               | Prosedur penghapusan akun <i>email</i> (A.9.2.1) sudah didokumentasikan.                                                                                                                                                                                    |                            |
| <i>C</i>                                               | Prosedur penyediaan hak akses pengguna (A.9.2.2) sudah didokumentasikan.                                                                                                                                                                                    |                            |
| <i>C</i>                                               | Prosedur penghapusan/pencabutan hak akses pengguna (A.9.2.2) sudah didokumentasikan.                                                                                                                                                                        |                            |
| <i>C</i>                                               | Prosedur pengecekan <i>password default</i> vendor (A.9.2.3) sudah didokumentasikan.                                                                                                                                                                        |                            |
| <i>C</i>                                               | Prosedur pengelolaan <i>sharing password administrator generic</i> (A.9.2.3) sudah didokumentasikan.                                                                                                                                                        |                            |

|    |                                                                                          |
|----|------------------------------------------------------------------------------------------|
| C  | Prosedur <i>reset password</i> (A.9.2.4) sudah didokumentasikan.                         |
| PC | Prosedur peninjauan hak akses pengguna (A.9.2.5) belum semuanya didokumentasikan.        |
| NC | Prosedur pemberian hak penggunaan aplikasi utilitas (A.9.4.4) belum didokumentasikan.    |
| NC | Prosedur penghapusan hak penggunaan aplikasi utilitas (A.9.4.4) belum didokumentasikan.  |
| NC | Prosedur pengelolaan <i>source code</i> (A.9.4.5) belum didokumentasikan.                |
| NC | Prosedur pengelolaan akses ke pusat data (A.11.1.5) belum didokumentasikan.              |
| C  | Prosedur pemeliharaan perlengkapan (A.11.2.4) sudah didokumentasikan.                    |
| NC | Prosedur perizinan peminjaman perangkat/peralatan (A.11.2.5) belum didokumentasikan.     |
| C  | Prosedur perizinan permintaan informasi (A.11.2.5) sudah didokumentasikan.               |
| NC | Prosedur pembuangan media elektronik (A.11.2.7) belum didokumentasikan.                  |
| C  | Prosedur manajemen perubahan (A.12.1.2) sudah didokumentasikan.                          |
| C  | Prosedur pemulihan dari kegagalan perubahan (A.12.1.2) sudah didokumentasikan.           |
| C  | Prosedur penanganan <i>malware</i> (A.12.2.1) sudah didokumentasikan.                    |
| C  | Prosedur peringatan <i>malware</i> (A.12.2.1) sudah didokumentasikan.                    |
| C  | Prosedur <i>backup</i> informasi (A.12.3.1) sudah didokumentasikan.                      |
| C  | Prosedur pengawasan dan pengujian hasil <i>backup</i> (A.12.3.1) sudah didokumentasikan. |
| C  | Prosedur pemasangan perangkat lunak (A.12.5.1) belum didokumentasikan.                   |
| C  | Prosedur penghapusan perangkat lunak (A.12.5.1) belum didokumentasikan.                  |

|    |                                                                                                                    |
|----|--------------------------------------------------------------------------------------------------------------------|
| C  | Prosedur manajemen kerentanan teknis (A.12.6.1) sudah didokumentasikan.                                            |
| NC | Prosedur audit sistem informasi (A.12.7.1) belum didokumentasikan.                                                 |
| C  | Prosedur pengelolaan jaringan (A.12.1.3 dan A.13.1.1) sudah didokumentasikan.                                      |
| NC | Prosedur pertukaran informasi (A.13.2.1) belum didokumentasikan.                                                   |
| NC | Prosedur Perlindungan Informasi <i>Email</i> Sensitif berupa <i>Attachement</i> (A.13.2.1) belum didokumentasikan. |
| C  | Prosedur pengembangan sistem informasi (A.14.2.2) sudah didokumentasikan.                                          |
| C  | Prosedur modifikasi paket instalasi perangkat lunak (A.14.2.4) sudah didokumentasikan.                             |
| NC | Prosedur proses pengembangan di lingkungan pengembangan untuk sistem tertentu (A.14.2.6) belum didokumentasikan.   |
| C  | Prosedur pengujian sistem (A.14.2.9) sudah didokumentasikan.                                                       |
| NC | Prosedur peninjauan kesesuaian layanan TIK (A.15.2.1) belum didokumentasikan.                                      |
| NC | Prosedur perubahan ketentuan layanan TIK (A.15.2.2) belum didokumentasikan.                                        |
| PC | Prosedur penanganan insiden (A.16.1.1) belum semuanya didokumentasikan.                                            |
| C  | Prosedur pelaporan insiden (A.16.1.2) sudah didokumentasikan.                                                      |
| NC | Prosedur penilaian dan pengklasifikasian insiden keamanan informasi (A.16.1.4) belum didokumentasikan.             |
| C  | Prosedur pencatatan aktifitas manajemen insiden (A.16.1.5) sudah didokumentasikan.                                 |
| NC | Prosedur eskalasi dan komunikasi insiden (A.16.1.6) belum didokumentasikan.                                        |
| NC | Prosedur penanganan bukti forensik (A.16.1.7) belum didokumentasikan.                                              |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                 |                  |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| NC       | Prosedur <i>business continuity plan</i> atau <i>disaster recovery plan</i> (A.17.1.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                  |                  |
| C        | Prosedur pemasangan perangkat lunak legal (A.18.1.2) sudah didokumentasikan.                                                                                                                                                                                                                                                                                                                                    |                  |
| NC       | Prosedur pengawasan perangkat lunak legal (A.18.1.2) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                    |                  |
| NC       | Prosedur audit keamanan informasi (A.18.2.1) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                            |                  |
| NC       | Prosedur tindakan perbaikan ( <i>corrective action</i> ) dari ketidakpatuhan/ <i>non-conformity</i> (A.18.2.2) belum didokumentasikan.                                                                                                                                                                                                                                                                          |                  |
| NC       | Prosedur peninjauan kepatuhan teknis (A.18.2.3) belum didokumentasikan.                                                                                                                                                                                                                                                                                                                                         |                  |
| A.12.1.2 | Manajemen perubahan                                                                                                                                                                                                                                                                                                                                                                                             | <i>Compliant</i> |
|          | Apakah perubahan pada organisasi, proses bisnis dan sistem informasi yang mempengaruhi keamanan informasi dikontrol?                                                                                                                                                                                                                                                                                            |                  |
| C        | Untuk identifikasi perubahan, DPTSI-ITS melakukan identifikasi dan pendokumentasian setiap perubahan yang dilakukan untuk semua Subdit di DPTSI-ITS berdasarkan klasifikasi perubahan. Dokumen tersebut berisikan waktu perubahan, petugas yang terlibat dalam perubahan, apa yang dirubah, dokumen pendukung (seperti konfigurasi atau perencanaan), dan hasil perubahan.                                      |                  |
| C        | Untuk perencanaan dan pengujian perubahan, DPTSI-ITS merencanakan apa saja yang akan dilakukan untuk melaksanakan perubahan dan menguji perubahan tersebut. Contohnya saat Subdit Infrastruktur memperbaharui perangkat lunak dengan versi terbaru, maka diuji terlebih dahulu apakah versi terbaru tidak menimbulkan masalah. Jika menimbulkan masalah maka Subdit Infrastruktur tetap menggunakan versi lama. |                  |
| C        | Untuk penilaian dampak perubahan, DPTSI-ITS melakukan penilaian dampak/isu keamanan yang berpotensi jika terjadi perubahan berdasarkan klasifikasi perubahan, contohnya <i>server</i> dan perangkat jaringan yang berhubungan dengan proses bisnis tertentu.                                                                                                                                                    |                  |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C | Untuk verifikasi kebutuhan keamanan informasi, DPTSI-ITS melakukan verifikasi untuk melihat apakah perubahan sesuai dengan kebutuhan keamanan yang direncanakan. Contohnya kebutuhan agar <i>server</i> tidak bisa diakses dari luar jaringan ITS (dengan memasukkan ke domain <i>private</i> ), maka dilakukan verifikasi dengan melakukan koneksi dari luar.                                                                                                                                                                                                                                                                                                                           |
| C | Untuk persetujuan formal untuk perubahan, DPTSI-ITS memerlukan pada persetujuan formal maupun tidak memerlukan berdasarkan klasifikasi perubahan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| C | Untuk komunikasi perubahan, DPTSI-ITS selalu menginformasikan kepada dosen, karyawan, dan mahasiswa melalui <i>website</i> ataupun pelatihan TIK jika perubahan melibatkan sistem informasi dan layanan TIK yang digunakan pengguna. Contohnya ketika DPTSI-ITS bekerja sama dengan Google untuk meningkatkan fasilitas <i>email</i> -nya, dimana perubahannya dipublikasikan di <i>website</i> <a href="https://mail2.its.ac.id/infoumum.php">https://mail2.its.ac.id/infoumum.php</a> .                                                                                                                                                                                                |
| C | Untuk dokumentasi kebijakan manajemen perubahan, DPTSI-ITS memiliki dokumentasi kebijakan yang berisikan aturan dalam perubahan, klasifikasi perubahan, pengujian dan penilaian dampak pada perubahan, cara mengkomunikasikan perubahan, dan lainnya.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| C | Untuk dokumentasi prosedur pemulihan dari kegagalan perubahan, DPTSI-ITS memiliki dokumentasi prosedur yang berisikan langkah-langkah untuk mengembalikan kondisi sistem ke keadaan semula jika terjadi kegagalan dalam penerapan perubahan baru.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| C | <p>Untuk dokumentasi manajemen perubahan, DPTSI-ITS memilikinya seperti:</p> <ul style="list-style-type: none"> <li>• Prosedur Dokumentasi Konfigurasi Sistem Jaringan yang digunakan untuk membuat dan mendokumentasikan setiap perubahan konfigurasi perangkat jaringan dan <i>server</i>. Langkah prosedurnya adalah membuka lembar worksheet dan mencatat seluruh perubahan. Setelah itu menyimpan perubahan berikut kedalam format <i>PDF</i>, lalu melakukan <i>backup file</i>.</li> <li>• Prosedur perubahan sistem yang dikembangkan yang digunakan untuk mengelola perubahan sistem yang baru atau pembaharuan kontrol A.14.2.2. Prosedur kontrol perubahan sistem.</li> </ul> |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                  |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| C<br>(lanj.) | <ul style="list-style-type: none"> <li>• Prosedur manajemen perubahan yang berisikan langkah-langkah mulai dari perencanaan sampai penyelesaian perubahan untuk semua jenis perubahan (baik perangkat lunak, konfigurasi, infrastruktur, dan lainnya) yang terjadi di DPTSI-ITS.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                  |
| A.12.1.3     | Manajemen kapasitas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <i>Compliant</i> |
|              | Apakah penggunaan sumber daya diawasi, ditingkatkan dan diproyeksikan untuk kebutuhan kapasitas kedepan untuk memastikan performa sistem yang dibutuhkan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                  |
| C            | <p>Dalam identifikasi kebutuhan kapisitas pada sumber daya, DPTSI-ITS melakukan:</p> <ul style="list-style-type: none"> <li>• Untuk sumber daya pada sistem dan jaringan, Subdit Infrastruktur memiliki standar spesifikasi sistem (contohnya spesifikasi <i>processor</i>, <i>memory</i>, <i>hardisk</i>, dan lainnya yang diperlukan) dan standar konfigurasi pemasangan jaringan.</li> <li>• Untuk sumber daya pada karyawan, Direktorat SDM dan Organisasi sudah mengidentifikasi kebutuhan minimum jumlah karyawan di DPTSI-ITS dengan menggunakan metode <i>workload analysis</i>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                  |
| C            | <p>Dalam pengawasan ketersediaan kapisitas pada sumber daya, DPTSI-ITS melakukan:</p> <ul style="list-style-type: none"> <li>• Untuk sumber daya pada sistem dan jaringan, Subdit Infrastruktur menggunakan Cacti dan <i>Internet Access Management</i> berdasarkan prosedur <i>Monitoring Bandwith</i>. Langkah prosedurnya adalah menjalankan aplikasi dan memantau performa <i>bandwith</i>, jika kecepatan <i>bandwith</i> lambat maka dilakukan pengaturan alokasi <i>bandwith</i>. Cacti merupakan perangkat lunak yang memonitor protokol <i>SNMP</i> dan melaporkan kondisi sistem (seperti penggunaan <i>processor</i>, <i>memory</i>, <i>hardisk</i> untuk <i>server</i>) ataupun beban trafik pada <i>backbone</i> antar jaringan (contohnya jaringan <i>LAN</i> di ITS Sukolilo dengan jaringan <i>LAN</i> di ITS Cokroaminoto), masing-masing <i>server</i> (contohnya Webmail ITS dan Integra ITS), atau perangkat lainnya yang memiliki <i>IP address</i> yang disajikan kedalam grafik yang dikelompokkan berdasarkan waktu.</li> </ul> |                  |

|              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C<br>(lanj.) | <ul style="list-style-type: none"> <li>• Untuk sumber daya pada karyawan, Direktorat SDM dan Organisasi menggunakan perangkat absensi <i>fingerprint</i> yang tersebar diseluruh unit/jurusan dilingkungan ITS untuk mengumpulkan data karyawan yang masuk kerja secara <i>realtime</i>. Data tersebut nanti diolah menggunakan SIM Kepegawaian untuk perhitungan jumlah absensi karyawan.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| C            | <p>Dalam meningkatkan dan menjaga kapasitas pada sistem (<i>server</i>, aplikasi dan infrastruktur jaringan), atau mengurangi permintaan, DPTSI-ITS melakukan:</p> <ul style="list-style-type: none"> <li>• Untuk menjaga kapasitas <i>hardisk</i> pada <i>server</i>, dilakukan dengan pengaturan logrotate (utilitas untuk mengelola <i>log</i> aktifitas) pada <i>server</i> melakukan penghapusan <i>file log</i> yang lebih dari 3 hari. Berdasarkan kontrol A.12.4.1. Mencatat kejadian, DPTSI-ITS memindahkan <i>file log</i> tersebut secara terpusat ke <i>SIEM</i>.</li> <li>• Untuk menjaga performa <i>server</i>, dilakukan dengan menonaktifkan beberapa aplikasi atau fitur yang tidak digunakan untuk menjalankan proses bisnis yang ada.</li> <li>• Untuk meningkatkan penyelesaian sejumlah proses, DPTSI-ITS melakukan pengukuran setiap aktifitas yang didokumentasikan dalam prosedur ISO 9000 berdasarkan target yang ingin dicapai.</li> <li>• Untuk meningkatkan performa sistem informasi terpadu, dilakukan dengan mengoptimasi <i>query</i> pada <i>database</i> dan logika pemrograman yang dibangun. Aktifitas ini dilakukan ketika terjadi masalah pada sistem misalnya respon lambat, atau ketika pengajuan untuk pemutakhiran oleh pengguna.</li> <li>• Untuk meningkatkan performa jaringan, dilakukan dengan membatasi alokasi <i>bandwidth</i> untuk layanan yang boros atau tidak berhubungan dengan bidang akademik seperti media <i>streaming</i> (Youtube), media sosial (Facebook, Twitter) dan lainnya. Selain itu berdasarkan kontrol A.13.1.1. Kontrol jaringan, terdapat pembatasan protokol <i>P2P</i> untuk torrent yang banyak menghabiskan <i>bandwidth</i>.</li> </ul> |
| C            | <p>Untuk proyeksi dan perencanaan kapasitas pada sumber daya, Subdit Infrastruktur mendokumentasikan perencanaan manajemen kapasitas kedepan hanya untuk sistem kritis yang sudah ditentukan saja. Hal ini dilakukan dengan cara melihat riwayat data penggunaan sistem dan jaringan yang dikumpulkan oleh Cacti dan melakukan analisa tren penggunaannya.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                     |                  |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| C<br>(lanj.)                            | Selain itu juga Direktorat SDM dan Organisasi mendokumentasikan perencanaan manajemen kapasitas kedepan untuk karyawan di DPTSI-ITS dengan cara analisa tren pada data riwayat kebutuhan penambahan karyawan.                                                                                                                                                                       |                  |
| A.12.2 Perlindungan dari <i>malware</i> |                                                                                                                                                                                                                                                                                                                                                                                     |                  |
| A.12.2.1                                | Kontrol terhadap <i>malware</i>                                                                                                                                                                                                                                                                                                                                                     | <i>Compliant</i> |
|                                         | Apakah kontrol pendeteksi, perlindungan dan perbaikan untuk menangani <i>malware</i> diterapkan dengan kombinasi kesadaran pengguna yang tepat?                                                                                                                                                                                                                                     |                  |
| C                                       | Untuk pembatasan pemasangan perangkat lunak secara <i>administratif</i> , DPTSI-ITS memiliki dokumentasi kebijakan pembatasan penggunaan perangkat lunak berdasarkan kontrol A.12.6.2. Pembatasan pemasangan perangkat lunak.                                                                                                                                                       |                  |
| C                                       | Untuk pembatasan pemasangan perangkat lunak secara <i>technical</i> , DPTSI-ITS mengatur agar sistem mencegah pemasangan perangkat lunak tanpa izin berdasarkan kontrol A.12.5.1. Pemasangan perangkat lunak pada sistem operasi.                                                                                                                                                   |                  |
| C                                       | Untuk melindungi <i>website</i> berbahaya ataupun yang melanggar hukum, DPTSI-ITS memanfaatkan fitur dari <i>ISP</i> PT. Telkom yaitu InternetPositif berdasarkan kontrol A.13.1.2. Keamanan layanan jaringan. DPTSI-ITS juga melakukan pemblokiran <i>website</i> tersebut menggunakan perangkat <i>Internet Access Management</i> berdasarkan kontrol A.13.1.1. Kontrol jaringan. |                  |
| C                                       | Untuk mengurangi kerentanan yang dapat dieksploitasi oleh <i>malware</i> , DPTSI-ITS melaksanakan aktifitas manajemen kerentanan secara kebijakan dan prosedural berdasarkan kontrol A.12.6.1. Manajemen kerentanan teknis.                                                                                                                                                         |                  |
| C                                       | Untuk peninjauan perangkat lunak dan data pada sistem secara berkala, DPTSI-ITS memiliki jadwal untuk peninjauan apakah terdapat <i>file</i> atau penambahan tanpa izin secara formal dan berkala baik untuk sistem sudah diklasifikasikan kritis dan perlu dilakukan peninjauan.                                                                                                   |                  |
| C                                       | Untuk melindungi dari <i>malware</i> , DPTSI-ITS menggunakan Honeypot Dionaea dan fitur <i>anti-virus</i> dari layanan <i>ISP</i> untuk melindungi infrastruktur jaringan berdasarkan kontrol A.13.1.1. Kontrol jaringan dan kontrol A.13.1.2.                                                                                                                                      |                  |



|                |                                                                                                                                                                                                                                                                                                                                                                    |                     |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| C<br>(lanj.)   | Keamanan layanan jaringan. Selain itu DPTSI-ITS menggunakan perangkat lunak ClamAV untuk melindungi <i>server</i> dan Windows Defender untuk melindungi komputer dengan sistem operasi Windows.                                                                                                                                                                    |                     |
| C              | Untuk melindungi data yang dirusak <i>malware</i> , DPTSI-ITS melakukan aktifitas <i>backup</i> secara berkala untuk data didalam <i>server</i> berdasarkan kontrol A.12.3.1. <i>Backup</i> informasi. Sedangkan untuk data yang dipegang karyawan dilakukan masing-masing dengan cara <i>backup</i> secara <i>online</i> ke Google Drive, Office 365 dan lainnya. |                     |
| C              | Untuk karantina (lingkungan terpisah) untuk sistem yang terinfeksi, DPTSI-ITS melakukan karantina sistem apapun jika terdapat infeksi <i>malware</i> agar tidak menyebar ke sistem lain sebelum dibersihkan. Untuk <i>malware</i> yang tidak bisa ditangani, DPTSI-ITS menyimpannya kedalam bentuk <i>clone</i> untuk dianalisa lebih lanjut.                      |                     |
| C              | Untuk peran dan tanggung jawab dalam penanganan <i>malware</i> , DPTSI-ITS menetapkan karyawan untuk penanganan <i>malware</i> pada sistem, pelatihan penggunaan perangkat <i>anti-malware</i> , pelaporan dan pemulihan dari serangan <i>malware</i> .                                                                                                            |                     |
| C              | Untuk dokumentasi kebijakan penanganan <i>malware</i> , DPTSI-ITS memiliki dokumentasi kebijakan yang berisikan aturan dalam penanganan <i>malware</i> , klasifikasi sistem kritis yang ditinjau, dan cara mendapatkan <i>file</i> atau perangkat lunak pada <i>internet</i> atau media lainnya baik untuk pengguna maupun <i>administrator</i> .                  |                     |
| C              | Untuk dokumentasi prosedur penanganan <i>malware</i> , DPTSI-ITS memiliki dokumentasi prosedur yang berisikan langkah-langkah pelaporan, penanganan dan pemulihan dari serangan <i>malware</i> .,                                                                                                                                                                  |                     |
| C              | Untuk dokumentasi prosedur peringatan <i>malware</i> , DPTSI-ITS memiliki dokumentasi prosedur yang berisikan bagaimana pengumpulan informasi mengenai <i>malware</i> baru dari <i>internet</i> , verifikasi kebenaran informasi, dan pemberitahuan informasi kepada pengguna.                                                                                     |                     |
| A.12.3. Backup |                                                                                                                                                                                                                                                                                                                                                                    |                     |
| A.12.3.1       | Backup informasi                                                                                                                                                                                                                                                                                                                                                   | Partially compliant |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | Apakah salinan informasi, perangkat lunak dan <i>clone</i> dari <i>hardisk</i> diambil dan diuji secara teratur berdasarkan kebijakan <i>backup</i> ?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| C | Untuk dokumentasi kebijakan <i>backup</i> , DPTSI-ITS mendokumentasikan kebijakan yang berisikan aturan dalam melakukan <i>backup</i> (baik informasi, perangkat lunak dan sistem), banyaknya <i>copy</i> hasil <i>backup</i> , serta cara pengujian dan pengamanannya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| C | Untuk dokumentasi prosedur <i>backup</i> informasi, DPTSI-ITS memiliki prosedur yang bernama <i>Backup Data</i> untuk melakukan proses <i>backup</i> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| C | Untuk fasilitas <i>backup</i> , Subdit Infrastruktur memiliki dua tipe <i>server backup</i> yaitu yang digunakan untuk menyimpan data <i>server</i> secara otomatis (sinkronisasi <i>database</i> ), dan untuk <i>file</i> konfigurasi dan <i>file log</i> perangkat jaringan. Sedangkan untuk <i>file</i> pekerjaan tertentu yang dimiliki karyawan, biasanya dilakukan <i>backup</i> ke media penyimpanan <i>online</i> seperti Google Drive, Office 365 dan lainnya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| C | Untuk rekaman riwayat aktifitas <i>backup</i> , setiap <i>backup</i> yang dilakukan dicatat kedalam formulir yang bernama Form Rekap Kegiatan <i>Backup Database</i> dan Sistem SIM, yang berisikan nama sistem informasi yang di- <i>backup</i> , frekuensi <i>backup</i> yang dibedakan antara sistem dan <i>database</i> -nya, lokasi tempat penyimpanan <i>backup</i> , dan <i>checklist</i> apakah sudah dilakukan atau belum.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| C | <p>Untuk frekuensi dan jenis <i>backup</i> (sebagian/semua atau satuan/berganda), hal yang dilakukan DPTSI-ITS adalah:</p> <ul style="list-style-type: none"> <li>• Memperhatikan frekuensi dan apa saja yang di <i>backup</i> berdasarkan kebutuhan bisnisnya, seperti melakukan aktifitas <i>backup</i> untuk <i>server</i> Webmail ITS, <i>DNS</i>, <i>SIEM</i> AlienVault dan Git ITS dilakukan setiap hari pada jam 1 malam, sedangkan untuk <i>server proxy</i> ITS, Nagios, ITS Web Monitoring System, dan Open VPN tidak dilakukan <i>backup</i>. Sedangkan aktifitas <i>backup</i> untuk konfigurasi perangkat jaringan dilakukan hanya ketika terjadi perubahan saja.</li> <li>• Memperhatikan jenis <i>backup</i> berdasarkan kebutuhan bisnisnya, seperti aktifitas <i>backup</i> yang dilakukan untuk <i>SIEM</i> AlienVault, dan sistem lainnya didefinisikan untuk dilakukan secara berganda agar mencegah jika satu hasil <i>backup</i> mengalami <i>corrupt</i>.</li> </ul> |

|                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |           |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| NC                                          | Untuk penempatan hasil <i>backup</i> , DPTSI-ITS menaruh <i>server backup</i> didalam gedung dan ruangan yang sama dengan perangkat yang di- <i>backup</i> (pusat data DPTSI-ITS didalam gedung Research Center ITS). Sedangkan untuk sistem informasi lain yang dikembangkan (seperti SIM Akademik), memiliki hasil <i>backup</i> yang terpisah oleh masing-masing <i>administrator</i> baik dari unit atau Subdit Pengembangan, namun hal ini diluar ruang lingkup SMKI.                                    |           |
| C                                           | Untuk perlindungan hasil <i>backup</i> secara fisik, DPTSI-ITS menaruh <i>server backup</i> didalam ruangan pusat data yang dilindungi oleh pintu dengan kunci <i>finger print</i> , <i>CCTV</i> , dan lainnya berdasarkan kontrol A.11.1.2. Kontrol keluar-masuk fisik.                                                                                                                                                                                                                                      |           |
| C                                           | Untuk ujicoba hasil <i>backup</i> , DPTSI-ITS melakukan ujicoba <i>backup</i> secara berkala dengan melakukan restorasi data ke sistem <i>clone</i> yang disediakan untuk dilakukan pengujian. DPTSI-ITS juga memiliki dokumentasi prosedur pengawasan dan pengujian hasil <i>backup</i> yang berisikan pemeriksaan aktifitas <i>backup</i> dan kegagalan yang terjadi, pengujian hasil <i>backup</i> kedalam sistem untuk pengujian, dan penilaian hasil uji coba berdasarkan data yang berhasil dipulihkan. |           |
| NC                                          | Untuk perlindungan kriptografi pada hasil <i>backup</i> yang memerlukan kerahasiaan yang tinggi, DPTSI-ITS tidak menggunakan kriptografi pada <i>hardisk</i> didalam <i>server</i> maupun <i>server backup</i> berdasarkan kontrol A.10.1.1. Kebijakan dalam penggunaan kontrol kriptografi.                                                                                                                                                                                                                  |           |
| A.12.5. Kontrol perangkat lunak operasional |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |           |
| A.12.5.1                                    | Pemasangan perangkat lunak pada sistem operasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Compliant |
|                                             | Apakah prosedur diterapkan untuk mengontrol pemasangan perangkat lunak pada sistem operasi?                                                                                                                                                                                                                                                                                                                                                                                                                   |           |
| C                                           | Untuk peran dan tanggung jawab dalam pemasangan perangkat lunak, DPTSI-ITS menetapkan untuk <i>server</i> ( <i>server dedicated</i> atau <i>VPS</i> ) dan komputer/laptop dinas. Hanya yang ditetapkan saja yang bisa memasang, memperbaharui atau menghapus perangkat lunak pada server dan computer/laptop dinas yang digunakan. Hal ini dikarenakan penggunaan <i>least privilege</i> berdasarkan kontrol A.9.2.3. Manajemen hak akses <i>administrator</i> .                                              |           |

|    |                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NA | Untuk pembatasan <i>development code</i> atau <i>compiler</i> aplikasi yang dikembangkan berjalan di sistem operasional, DPTSI-ITS hanya mengembangkan sistem informasi berbasis <i>web</i> . Jadi kode program dapat dilihat baik didalam <i>server live</i> atau <i>server development</i> , jika pengguna memiliki hak aksesnya.                                                                                                                    |
| C  | Untuk pengujian sistem, DPTSI-ITS melakukan pengujian secara terpisah yang dilakukan di <i>server development</i> berdasarkan kontrol A.14.2.9. Pengujian penerimaan sistem. Selain itu semua perubahan sistem operasi dan aplikasi pendukung lainnya diuji terlebih dahulu sebelum dioperasikan dilingkungan yang terpisah dari lingkungan operasional berdasarkan kontrol A.14.2.3. Tinjauan teknis pada aplikasi setelah dilakukan perubahan dasar. |
| C  | Untuk sistem manajemen konfigurasi, DPTSI-ITS menggunakan sistem manajemen konfigurasi (seperti Puppet, Chef dan lainnya) untuk mengontrol semua konfigurasi <i>server</i> yang berupa <i>template</i> .                                                                                                                                                                                                                                               |
| C  | Untuk strategi pengembalian keadaan semula, DPTSI-ITS melakukan pemasangan kembali versi lama perangkat lunak jika perangkat lunak baru tidak sesuai dengan yang diharapkan atau terdapat <i>error</i> /konflik terhadap sistem lainnya.                                                                                                                                                                                                               |
| C  | Untuk rekaman riwayat pembaharuan <i>program library</i> untuk sistem yang dikembangkan, DPTSI-ITS menggunakan sistem Git ITS yang memiliki fungsi penyimpanan perubahan <i>source code</i> dan <i>file</i> pendukung lainnya berdasarkan kontrol A.9.4.5. Kontrol akses ke <i>source code</i> perangkat lunak.                                                                                                                                        |
| C  | Untuk penyimpanan perangkat lunak sebelumnya, DPTSI-ITS menyimpan perangkat lunak sebelumnya beserta catatan lengkap yang berisikan informasi perangkat lunak, prosedur, dan rincian konfigurasi.                                                                                                                                                                                                                                                      |
| C  | DPTSI-ITS memiliki dokumentasi kebijakan pemasangan dan penghapusan perangkat lunak yang berisikan peran dan tanggung jawab karyawan, aturan pemasangan perangkat lunak pada komputer dan <i>server</i> , apa yang harus disimpan dan dilakukan ketika pemasangan, dan lainnya.                                                                                                                                                                        |
| C  | DPTSI-ITS memiliki prosedur pemasangan atau penghapusan perangkat lunak yang tidak dikembangkan DPTSI-ITS yang berisikan langkah-langkah dalam pemasangan, pengujian atau penghapusan perangkat lunak pada komputer dan <i>server</i> .                                                                                                                                                                                                                |

| A.12.6. Manajemen kerentanan teknis |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                  |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| A.12.6.1                            | Manajemen kerentanan teknis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <i>Compliant</i> |
|                                     | Apakah informasi tentang kerentanan teknis pada sistem informasi didapatkan pada waktu tertentu dan dilakukan tindak lanjutnya (seperti <i>patch</i> ) untuk mengacu pada resiko yang terkait?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                  |
| C                                   | Untuk peran dan tanggung jawab dalam manajemen kerentanan teknis, DPTSI-ITS menetapkan karyawan yang melakukan manajemen kerentanan teknis untuk masalah <i>patch/update</i> dari Subdit Infrastruktur dalam mengelola <i>server</i> (sistem operasi dan perangkat lunaknya) dan perangkat jaringan, dan dari Subdit Pelayanan dalam mengelola komputer dan laptop dinas (sistem operasi dan perangkat lunaknya).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                  |
| C                                   | <p>Untuk identifikasi kerentanan, DPTSI-ITS mengklasifikasikan tingkat kepentingan dalam pemasangan <i>patch</i>, apakah tingkatan <i>high</i> seperti yang berkaitan dengan proses bisnis (contohnya Ms. SQL Server, PHP server) atau keamanan informasi (contohnya <i>anti-virus</i>), tingkatan <i>medium</i> seperti perangkat lunak pendukung (contohnya Ms. Office, Adobe Photoshop), dan tingkatan <i>low</i> seperti <i>driver</i> dan perangkat lunak lainnya.</p> <p>DPTSI-ITS mengawasi kerentanan baru berdasarkan klasifikasi melalui forum/<i>website</i> keamanan informasi (seperti NIST National Vulnerability Database di <a href="https://nvd.nist.gov/">https://nvd.nist.gov/</a>, Offensive Security's Exploit Database Archive di <a href="https://www.exploit-db.com/">https://www.exploit-db.com/</a>, atau CVE <a href="http://www.cvedetails.com/">http://www.cvedetails.com/</a>) dan mengawasi rilis terbaru <i>patch/update</i> dari <i>website</i> vendor perangkat lunak secara berkala dan terjadwal.</p> |                  |
| C                                   | Untuk identifikasi dan penanganan resiko terkait kerentanan yang ditemukan, DPTSI-ITS melakukan aktifitas identifikasi resiko dan penanganan resiko ketika kerentanan telah teridentifikasi. Selain itu memperbaharui laporan proses penilaian resiko di Lampiran I dan laporan proses penanganan resiko di Lampiran J.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                  |
| C                                   | Untuk resiko yang ada ketika memasang <i>patch</i> , DPTSI-ITS membandingkan resiko yang ada ketika memasang <i>patch</i> dengan kerentanan yang ada.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                  |

|                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                  |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| C                                   | Untuk pengujian <i>patch</i> , DPTSI-ITS melakukan ujicoba sebelum pemasangan <i>patch</i> untuk melihat apakah <i>patch</i> terbaru memiliki efek samping. Jika terdapat efek samping sampai mengganggu sistem informasi yang penting maka tetap menggunakan versi yang lama dan aktifitas harus direkam. DPTSI-ITS dapat mempertimbangkan menon-aktifkan layanan tertentu yang terkait kerentanan, mengubah konfigurasi perangkat jaringan, menambah pengawasan ketika serangan terdeteksi, atau memberikan pelatihan kepada karyawan tentang kerentanan. |                  |
| C                                   | Untuk riwayat aktifitas pemasangan <i>patch</i> , DPTSI-ITS merekam perangkat lunak apa saja yang sudah dan yang belum diberikan <i>patch</i> , serta yang bermasalah dalam pemberian <i>patch</i> (memiliki efek samping) dan penanggulangannya.                                                                                                                                                                                                                                                                                                           |                  |
| C                                   | Untuk penyamaan antara aktifitas manajemen kerentanan teknis dengan aktifitas manajemen insiden, DPTSI-ITS melakukan manajemen kerentanan teknis berdasarkan dokumen kebijakan dan prosedur untuk penambahan informasi pembantu ketika terjadi insiden.                                                                                                                                                                                                                                                                                                     |                  |
| C                                   | Untuk dokumentasi kebijakan manajemen kerentanan teknis, DPTSI-ITS memiliki dokumentasi kebijakan yang berisikan peran dan tanggung jawab karyawan, aturan pengawasan kerentanan dan pembaharuan <i>patch</i> , dan lainnya.                                                                                                                                                                                                                                                                                                                                |                  |
| C                                   | Untuk dokumentasi prosedur manajemen kerentanan teknis, DPTSI-ITS memiliki dokumentasi prosedur berisikan langkah-langkah dalam manajemen <i>patch</i> (termasuk kerentanan yang telah teridentifikasi namun belum memenuhi penanganan yang tepat).                                                                                                                                                                                                                                                                                                         |                  |
| A.12.6.2                            | Pembatasan pemasangan perangkat lunak                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <i>Compliant</i> |
|                                     | Apakah peraturan untuk mengatur pemasangan perangkat lunak oleh pengguna dibuat dan diterapkan?                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                  |
| C                                   | DPTSI-ITS memiliki dokumentasi kebijakan pembatasan penggunaan perangkat lunak yang berisikan rincian perangkat lunak apa saja yang boleh dipasang (baik yang tidak perlu perizinan ataupun yang memerlukan perizinan dahulu) dan yang tidak boleh dipasang.                                                                                                                                                                                                                                                                                                |                  |
| A.13.1. Manajemen keamanan jaringan |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                  |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                  |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| A.13.1.1 | Kontrol jaringan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Compliant</i> |
|          | Apakah jaringan diurus dan dikontrol untuk melindungi informasi didalam sistem dan aplikasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                  |
| C        | Untuk peran dan tanggung jawab dalam manajemen dan operasional infrastruktur jaringan, DPTSI-ITS menetapkan Subdit Infrastruktur secara khusus. Jumlah Subdit Infrastruktur adalah 8 orang yang terdiri dari Kasubdit Infrastruktur, karyawan pengembang jaringan dan pangkalan data (yang dibagi menjadi administrasi jaringan, administrasi sistem, dan administrasi kelistrikan), dan karyawan penyusun laporan dan pengelola BMN.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                  |
| C        | Untuk pemisahan peran dan tanggung jawab dalam operasional infrastruktur jaringan dengan operasional komputer, Subdit Infrastruktur tidak bertanggung jawab terhadap operasional komputer dan laptop yang ada, seperti pemasangan sistem dan pengaturannya. Hal ini dikarenakan yang bertanggung jawab adalah Subdit Pelayanan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                  |
| C        | <p>Untuk dokumentasi prosedur pengelolaan jaringan, Subdit infrastruktur memiliki:</p> <ul style="list-style-type: none"> <li>• Prosedur Instalasi Jaringan Baru yang digunakan untuk pemasangan jaringan baru di lingkungan ITS.</li> <li>• Prosedur <i>Monitoring</i> Jaringan yang digunakan untuk mengawasi kondisi jaringan. Aktifitas pengawasan dilakukan dengan bantuan Nagios dan ITS Web Monitoring System. Jika terdapat gangguan maka Subdit Infrastruktur akan melakukan <i>troubleshooting</i> seperti jika perangkat tidak menyala maka akan dinyalakan, jika terjadi <i>error</i> pada perangkat maka akan dilakukan <i>reset</i>, jika kabel tidak terpasang maka akan dipasang, dan jika layanan aplikasi mati maka akan dilaporkan.</li> <li>• Prosedur Pemeriksaan Jaringan Setelah Listrik Mati yang digunakan untuk memeriksa <i>server</i>, sistem informasi dan perangkat jaringan setelah terjadi pemadaman listrik.</li> <li>• Prosedur Instalasi <i>Access Point</i> yang digunakan untuk memasang <i>access point</i>/Wifi secara benar di setiap unit/jurusan.</li> <li>• Prosedur Pelebaran <i>Bandwith</i> yang digunakan untuk menambah <i>bandwith internet</i> bagi pengguna yang memerlukan <i>bandwith</i> lebih untuk acara khusus.</li> </ul> |                  |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C | <p>Untuk melindungi jaringan <i>intranet</i> dan <i>internet</i> dilingkungan ITS dari ancaman akses tanpa izin, <i>malware</i>, <i>hacking</i> dan lainnya, Subdit Infrastruktur menggunakan kontrol keamanan berlapis seperti:</p> <ul style="list-style-type: none"> <li>• CISCO ASA Firewall 5540 adalah perangkat jaringan <i>firewall</i> yang diatur agar <i>default</i>-nya membatasi semua <i>port</i> dan hanya memperbolehkan <i>port</i> tertentu saja, seperti memperbolehkan <i>port</i> yang digunakan <i>HTTP/HTTPS</i>, <i>SMTP</i>, <i>POP3</i>, <i>IMAP</i>, <i>SNMP</i>, <i>NTP</i>, dan lainnya yang digunakan. Sedangkan untuk <i>port</i> aneh dan tidak aman digunakan seperti <i>FTP</i>, <i>P2P</i> dan lainnya tidak diperbolehkan. Perangkat ini hanya berfungsi sebagai <i>firewall</i> dan <i>anti-virus</i>, meskipun terdapat fitur <i>VPN</i>, <i>anti-spam</i>, <i>IPS</i> dan <i>IDS</i> yang perlu dibeli masing-masing lisensinya. Selain itu Subdit infrastruktur juga menggunakan <i>firewall</i> berupa perangkat lunak yang berjalan pada sistem operasi Linux bernama ShoreWall, namun penggunaanya hanya untuk mengamankan SIM saja.</li> <li>• Honeypot Dionaea adalah <i>server</i> yang menangani dan mengkarantina serangan <i>malware</i> yang mengeksploitasi kerentanan pada layanan yang disediakan melalui jaringan ITS. Perangkat ini melakukan aktifitas pengawasan secara <i>realtime</i> pada setiap asal koneksi dan <i>IP address</i> yang terhubung dan penanganan secara langsung jika terjadi serangan. Honeypot merupakan kerjasama dengan KEMENKOMINFO.</li> <li>• Tsubame (<i>internet threat monitoring system</i>) adalah <i>server</i> untuk sensor CSIRT dikawasan Asia Pasifik yang berfungsi untuk pengawasan ancaman <i>internet</i> (contohnya infeksi <i>worm</i> ataupun investigasi kerentanan sistem), saling berbagi informasi dan analisisnya, dan meningkatkan kolaborasi antara CSIRT dengan menggunakan <i>platform</i> yang sama. Jika terjadi serangan <i>cyber</i> didalam infrastruktur jaringan di ITS maka akan dikirimkan informasinya melalui <i>email</i> ke Subdit Infrastruktur. CSIRT juga menyampaikan tren kondisi jaringan secara umum dikawasan Asia Pasifik, informasi untuk meningkatkan kewaspadaan, dan daftar kerentanan berikut penanganannya yang berdasarkan hasil analisa semua data dari organisasi yang bekerjasama dengan tim CSIRT. Tsubame merupakan kerjasama dengan KEMENKOMINFO.</li> <li>• Sangfor Internet Access Management (<i>IAM</i>) adalah perangkat jaringan yang digunakan untuk mengatur dan memaksimalkan penggunaan <i>bandwith</i> yang digunakan, serta melihat laporan penggunaan/kebiasaan pada trafik <i>internet</i>, seperti <i>email</i>, aplikasi <i>chat</i>, media sosial. Berdasarkan kontrol A.12.1.3. Manajemen kapasitas, Subdit Infrastruktur membatasi <i>bandwith</i> media sosial dan media <i>streaming</i> dengan perangkat ini. Selain</li> </ul> |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | <p>itu perangkat ini digunakan untuk memblokir <i>website</i> yang berbahaya ataupun yang melanggar hukum.</p> <ul style="list-style-type: none"> <li>• <i>Proxy</i> ITS adalah <i>server</i> yang berfungsi sebagai perantara jaringan ITS dengan koneksi luar, pemblokiran <i>IP address</i> tertentu, dan penyimpanan <i>cache</i> riwayat halaman <i>website</i>. Semua sistem yang ingin mendapatkan koneksi <i>internet</i> di area kampus dapat mengatur pengaturan <i>proxy</i> di <i>browser</i> dan memasukkan alamat dan <i>password email</i> ITS. <i>Proxy</i> ITS menggunakan perangkat lunak Squid yang berlisensi <i>open source</i>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| C | <p>Untuk menjaga <i>confidentiality</i> dan <i>integrity</i> dari data melalui jaringan <i>intranet</i> dan <i>internet</i> di lingkungan ITS, Subdit Infrastruktur menggunakan koneksi <i>VPN</i> dan protokol <i>TLS</i> berdasarkan kontrol A.10.1.1. Kebijakan dalam penggunaan kontrol kriptografi.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| C | <p>Untuk menjaga <i>availability</i> dari jaringan <i>intranet</i> dan <i>internet</i> di lingkungan ITS, Subdit Infrastruktur menggunakan beberapa kontrol keamanan seperti:</p> <ul style="list-style-type: none"> <li>• Nagios merupakan sistem informasi yang mengawasi kondisi operasional keseluruhan perangkat jaringan seperti <i>switch</i> dan <i>fingerprint</i> yang dipasang di setiap unit/jurusan di dalam lingkungan ITS secara <i>realtime</i>. Hasil dari laporan ditampilkan menggunakan TV LCD yang diletakkan di dalam ruangan Subdit Infrastruktur.</li> <li>• ITS Web Monitoring System merupakan sistem informasi yang digunakan untuk menampilkan kondisi <i>up</i> atau <i>down</i> perangkat <i>server</i> yang dikelola oleh DPTSI-ITS secara <i>realtime</i>. Hasil dari laporan perangkat tersebut ditampilkan menggunakan TV LCD yang diletakkan di dalam ruangan Subdit Pelayanan.</li> <li>• Cacti merupakan sistem informasi yang memonitor dan melaporkan kondisi ataupun beban trafik di dalam infrastruktur jaringan di ITS yang disajikan ke dalam grafik yang dikelompokkan berdasarkan waktu berdasarkan kontrol A.12.1.3. Manajemen kapasitas.</li> </ul> |
| C | <p>Untuk perekaman <i>log</i> dan pengawasan untuk merekam dan mendeteksi aktivitas, DPTSI-ITS menggunakan <i>SIEM</i> AlienVault yang merupakan sistem informasi yang menyimpan <i>file log</i> dari berbagai <i>server</i> secara terpusat berdasarkan kontrol A.12.4.1. Mencatat kejadian. <i>Log</i> yang disimpan tadi dianalisa dan dilaporkan secara ringkas, seperti serangan <i>cyber</i> yang terjadi, aktivitas yang dilakukan di dalam infrastruktur jaringan ITS, kerentanan sistem yang ada, jumlah <i>error</i> yang terjadi pada sistem, dan lainnya.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

|                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                  |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| C                                                       | Untuk meningkatkan layanan dan memastikan kontrol keamanan terpasang secara konsisten pada infrastruktur TIK, Subdt Infrastruktur bekerjasama dengan Subdit Pelayanan dalam masalah penerimaan keluhan pada sistem dan jaringan, dan penanganannya.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                  |
| C                                                       | Untuk mengautentikasi sistem didalam jaringan, pengguna diperlukan aktifitas autentikasi dengan <i>SSO</i> atau pengaturan <i>proxy</i> pada perangkat yang dimiliki berdasarkan kontrol A.9.1.2. Akses ke jaringan dan layanan jaringan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                  |
| C                                                       | Untuk membatasi koneksi ke jaringan ITS, Subdit Infrastruktur menggunakan CISCO ASA Firewall 5540. Pembatasannya seperti siapa yang boleh mengakses berdasarkan <i>IP address</i> , dan apa saja sistem atau perangkat yang bisa diakses berdasarkan jenis domain ( <i>DMZ</i> atau <i>private</i> ).                                                                                                                                                                                                                                                                                                                                                                                                                              |                  |
| A.14.2. Keamanan dalam proses pengembangan dan dukungan |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                  |
| A.14.2.4                                                | Pembatasan pada perubahan paket perangkat lunak                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <i>Compliant</i> |
|                                                         | Apakah modifikasi pada paket perangkat lunak diurungkan, dibatasi untuk perubahan yang diperlukan dan semua perubahan harus dikontrol secara ketat?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                  |
| C                                                       | Untuk pembatasan aktifitas modifikasi paket instalasi perangkat lunak, DPTSI-ITS tidak membatasinya melakukan modifikasi paket instalasi perangkat lunak yang dipasang kedalam sistem dengan cara tidak memasang bagian atau <i>plug-in</i> yang tidak diperlukan dengan mempertimbangkan alasan performa, persetujuan atau rekomendasi dari vendor, kemungkinan mendapatkan pembaharuan dari vendor, dampak dari perubahan, dan kompatibilitas dengan perangkat lunak lain. Selsin itu setiap aktifitas modifikasi paket instalasi perangkat lunak dilakukan perekaman riwayatnya seperti waktu modifikasi, petugas, perangkat lunak yang dimodifikasi, apa yang dimodifikasi dari perangkat lunak tersebut, dan hasil pengujian. |                  |
| C                                                       | Untuk pengujian hasil dari modifikasi paket instalasi perangkat lunak, secara formal, DPTSI-ITS menguji secara formal hasil modifikasi paket instalasi perangkat lunak yang dilakukan dan mendapatkan izin dari Kasubdit Pengembangan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                  |

|                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |           |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| C                  | Untuk dokumentasi prosedur modifikasi paket instalasi perangkat lunak, DPTSI-ITS memiliki dokumentasi prosedur modifikasi paket instalasi perangkat lunak yang berisikan langkah-langkah dalam perencanaan, pengujian dan pendokumentasian perubahan paket instalasi perangkat lunak.                                                                                                                                                                                                                                                                                                                                                                                                                           |           |
| A.14.2.5           | Prinsip keahlian teknis yang aman                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Compliant |
|                    | Apakah panduan keamanan teknis untuk pemrograman yang aman dibangun, didokumentasikan, dirawat dan diterapkan pada setiap penerapan sistem informasi?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |           |
| C                  | Untuk penggunaan standar teknis dan <i>source code</i> , DPTSI-ITS memiliki standar teknis dan <i>source code</i> untuk pemrograman yang aman untuk bahasa pemrograman <i>PHP</i> dan Ms. SQL Server. Standar teknis berisi tata cara penulisan <i>source code</i> dan struktur yang disetujui, teknik autentikasi pengguna, mengamankan <i>session</i> ataupun <i>cookies</i> , validasi data, menghilangkan <i>debug</i> pada <i>source code</i> , dan lainnya. Sedangkan standar <i>source code</i> merupakan fungsi tertentu yang sudah diuji dan diizinkan untuk dimasukkan ke perangkat lunak baru untuk memenuhi standar keamanan, seperti fungsi autentikasi, enkripsi, <i>backup</i> data dan lainnya. |           |
| C                  | Untuk pembaharuan standar teknis dan <i>source code</i> secara berkala, DPTSI-ITS meninjau standar teknis dan standar <i>source code</i> yang dimiliki secara berkala untuk memastikan agar selalu terbaharui dalam menangani potensi ancaman terbaru.                                                                                                                                                                                                                                                                                                                                                                                                                                                          |           |
| A.17.2. Redundansi |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |           |
| A.17.2.1           | Ketersediaan dari fasilitas pemrosesan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Compliant |
|                    | Apakah fasilitas pemrosesan informasi diterapkan secara berlebih (seperti <i>disaster recovery center</i> atau redundansi komponen) untuk memenuhi persyaratan ketersediaan?                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |           |
| C                  | Untuk redundansi arsitektur, DPTSI-ITS menerapkan <i>disaster recovery center</i> berupa <i>server mirror</i> yang ditempatkan diluar organisasi berdasarkan kontrol A.17.1.1. Merencanakan keberlangsungan keamanan informasi. Selain itu untuk setiap <i>server</i> pendukung yang penting (seperti <i>server DNS</i> dan <i>server proxy</i> ITS) dibuat secara redundan sebagai alternatif jika <i>server</i> tidak bekerja. Misalnya <i>server DNS</i> yang diatur agar terdapat <i>master</i> dan <i>slave</i> , dan <i>server proxy</i> ITS yang memiliki banyak <i>server</i> baik <i>VPS</i> atau <i>dedicated</i> .                                                                                   |           |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| C | <p>Untuk redundansi komponen, Subdit Infrastruktur memasang komponen yang redundan pada <i>hardisk</i> (contohnya dua atau lebih <i>hardisk</i> dengan konfigurasi <i>RAID</i>) dan <i>memory</i> (contohnya konfigurasi <i>dual/multiple-channel</i>) untuk setiap <i>server</i> fisik yang dikelola. Hal ini dilakukan agar jika terjadi kegagalan/kerusakan pada satu komponen maka <i>server</i> masih dapat berjalan normal dan data yang tersimpan masih dapat terjaga.</p>                                                                                                                                                                                                     |
| C | <p>Untuk redundansi komponen dan perangkat berupa cadangan, DPTSI-ITS memiliki cadangan komponen dan perangkat baik <i>processor</i>, <i>memory</i>, <i>hardisk</i>, <i>access point</i>, <i>access switch</i>, <i>distribution switch</i>, <i>firewall</i>, <i>core switch</i> dan lainnya.</p> <p>DPTSI-ITS mendefinisikan beberapa perangkat keras/jaringan atau komponennya yang dirasakan kritis untuk segera disediakan cadangannya dengan mempertimbangkan proses bisnis yang terlibat. DPTSI-ITS menyiapkan cadangan perangkat ataupun komponen jika suatu perangkat atau komponen didefinisikan kritis, sedang digunakan/beroperasional dan sudah melewati umur garansi.</p> |

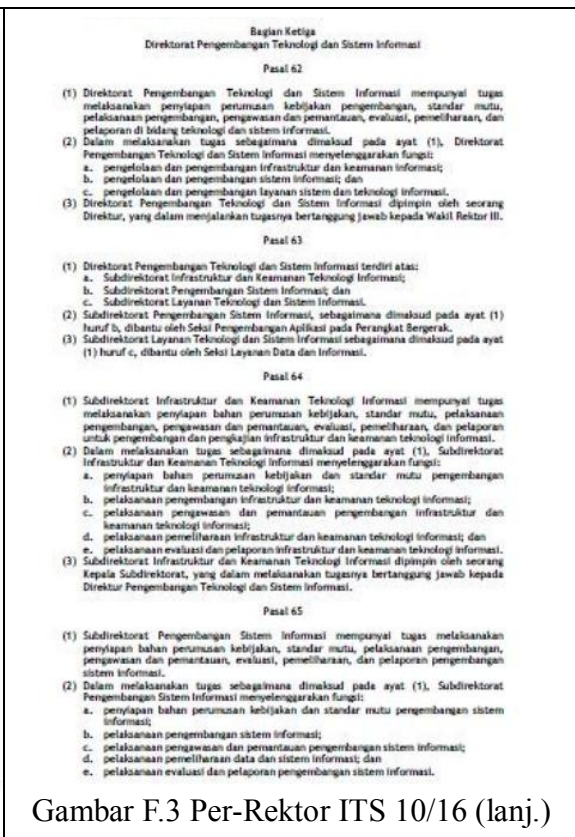
*Halaman ini sengaja dikosongkan*



Gambar F.1 Kebijakan Keamanan di Website DPTSI-ITS



Gambar F.2 Per-Rektor ITS 10/16



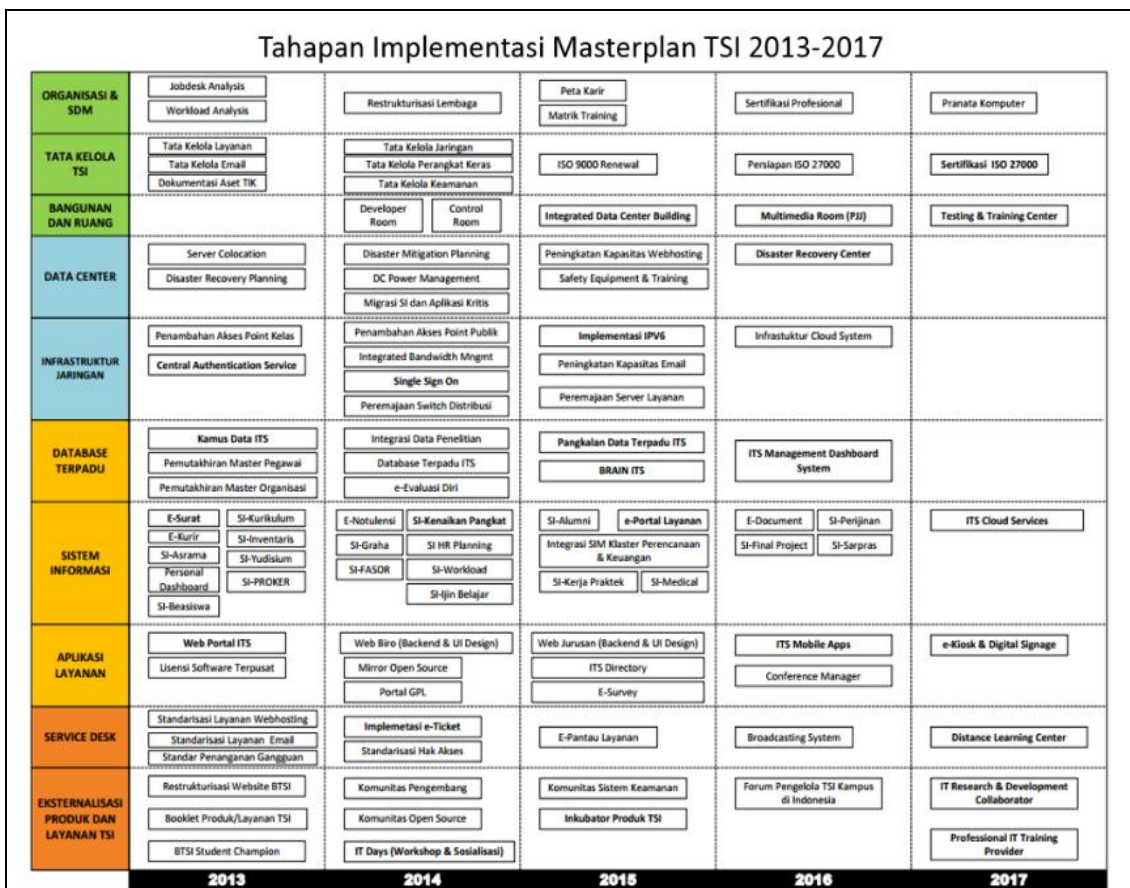
Gambar F.3 Per-Rektor ITS 10/16 (lanj.)

|  |                            | <b>URAIAN TUGAS</b><br><b>LEMBAGA PENGEMBANGAN TEKNOLOGI</b><br><b>SISTEM INFORMASI</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Tgl.Terbit : 2 Oktober 2014<br><br>Halaman : 1 dari 2                                                                                                                 |
|-----------------------------------------------------------------------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NO                                                                                | JABATAN                    | URAIAN TUGAS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | KOMPETENSI                                                                                                                                                            |
| 1                                                                                 | Ketua Lembaga              | <ul style="list-style-type: none"> <li>- Menyusun rencana program kerja dan mempersiapkan pelaksanaan program kerja LPTSI</li> <li>- Menentukan kebijakan <i>intern</i> maupun <i>extern</i> LPTSI</li> <li>- Menentukan/memilih penanggung jawab operasional dalam suatu kegiatan</li> <li>- Menentukan arah perkembangan di bidang Informasi dan Teknologi</li> <li>- Menentukan arah perkembangan jaringan ITS</li> <li>- Menerima tugas lain dan memberikan laporan pertanggung jawaban ke Rektor ITS</li> </ul>                                                                             | <ol style="list-style-type: none"> <li>1. Memiliki kemampuan manajerial yang baik</li> <li>2. Visioner</li> <li>3. Memiliki kemampuan komunikasi yang baik</li> </ol> |
| 2                                                                                 | Sekretaris Lembaga         | <ul style="list-style-type: none"> <li>- Mengkomunikasikan rencana program kerja dan membantu ketua mempersiapkan pelaksanaan program kerja LPTSI</li> <li>- Membantu ketua merealisasikan program kerja ketua lembaga</li> <li>- Menerima tugas memberikan laporan pertanggung jawaban ke ketua lembaga</li> </ul>                                                                                                                                                                                                                                                                              | <ol style="list-style-type: none"> <li>1. Memiliki kemampuan manajerial yang baik</li> <li>2. Visioner</li> <li>3. Memiliki kemampuan komunikasi yang baik</li> </ol> |
| 3                                                                                 | Koordinator Pusat          | <ul style="list-style-type: none"> <li>- Menyusun rencana program kerja dan mempersiapkan pelaksanaan program kerja LPTSI</li> <li>- Menentukan kebijakan <i>intern</i> maupun <i>extern</i> LPTSI</li> <li>- Menentukan/memilih penanggungjawab operasional dalam suatu kegiatan</li> <li>- Menentukan arah perkembangan di bidang Informasi dan Teknologi</li> <li>- Menentukan arah perkembangan jaringan ITS</li> <li>- Menerima tugas lain dan memberikan laporan pertanggung jawaban ke Rektor ITS</li> </ul>                                                                              | <ol style="list-style-type: none"> <li>1. Memiliki kemampuan manajerial yang baik</li> <li>2. Visioner</li> <li>3. Memiliki kemampuan komunikasi yang baik</li> </ol> |
| 4                                                                                 | Petugas pengelola keuangan | <ul style="list-style-type: none"> <li>- Menerima dan mengeluarkan uang dari dana PNBP</li> <li>- Mencatat penerimaan dan pengeluaran dana PNBP</li> <li>- Mengarsip bukti penerimaan dan pengeluaran dana PNBP</li> <li>- Membuat laporan keuangan per bulan</li> <li>- Membuat laporan keuangan per tahun</li> <li>- Mengajukan usulan dan pengambilan uang muka kerja</li> <li>- Mengerjakan SPJ dan melaporkannya</li> <li>- Membuat daftar gaji pegawai UPT PUSKOM yang menjadi tanggungan BAUK</li> <li>- Mendistribusikan gaji pegawai UPT PUSKOM yang menjadi tanggungan BAUK</li> </ul> | <ol style="list-style-type: none"> <li>1. Mengetahui peraturan dan perundangan dibidang keuangan</li> <li>2. Memiliki kemampuan dibidang keuangan</li> </ol>          |
| 5                                                                                 | Service Desk               | <ul style="list-style-type: none"> <li>- Menerima surat masuk</li> <li>- Memberi kartu kendali/disposisi bilamana diperlukan</li> <li>- Mencatat dibuku agenda</li> <li>- Menyampaikan ke kepala untuk mendapatkan disposisi</li> <li>- Memilah surat sesuai dengan disposisi, yang selanjutnya didistribusikan kepihak/staf yang ditunjuk.</li> <li>- Membuat konsep surat (menjawab surat masuk, bilamana diperlukan)</li> <li>- Mengarsip surat masuk dan surat keluar kedalam order yang selanjutnya disimpan kedalam almari arsip</li> <li>- Menerima telpon masuk</li> </ul>               | <ol style="list-style-type: none"> <li>1. Memiliki kemampuan kesekretariatan</li> <li>2. Memiliki kemampuan komunikasi yang baik</li> </ol>                           |
| 6                                                                                 | Analisis Sistem            | <ul style="list-style-type: none"> <li>- Menganalisa kebutuhan sistem</li> <li>- Menganalisa report data</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <ol style="list-style-type: none"> <li>1. Memiliki kemampuan analisa baik</li> <li>2. Memiliki kemampuan analisa yang baik</li> </ol>                                 |
| 7                                                                                 | Dokumentator               | <ul style="list-style-type: none"> <li>- Membuat dokumentasi program</li> <li>- Membuat user manual aplikasi</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <ol style="list-style-type: none"> <li>1. Memahami alur aplikasi dengan baik</li> <li>2. Terampil dan telaten mengolah informasi</li> </ol>                           |

Gambar F.4 Uraian Tugas

|    |                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                              |
|----|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8  | Programmer                | <ul style="list-style-type: none"> <li>- Memberikan <i>support</i> terhadap pemeliharaan <i>software</i></li> <li>- Memberikan <i>support</i> terhadap pengembangan <i>software</i></li> <li>- Mengembangkan <i>system</i> replikasi atau klasterisasi basis data</li> <li>- <i>Backup</i> rutin kode program dan berkas basis data</li> </ul>                                                                                                                                  | <ol style="list-style-type: none"> <li>1. Memiliki kemampuan dibidang <i>programmer</i> yang baik</li> <li>2. Mampu menganalisa masalah</li> <li>3. Mampu bekerja secara tim</li> </ol>                                                                                                                      |
| 9  | Admin Jaringan            | <ul style="list-style-type: none"> <li>- Merawat jaringan <i>backbone</i> ITS</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                        | <ol style="list-style-type: none"> <li>1. Memiliki kemampuan di bidang jaringan</li> </ol>                                                                                                                                                                                                                   |
|    |                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                              |
|    |                           | <ul style="list-style-type: none"> <li>- Mengembangkan <i>network design</i>, <i>administrator</i> dan aplikasi</li> <li>- Mengembangkan dan merawatan Jaringan <i>INHERENT</i> untuk wilayah Regional maupun Nasional</li> <li>- Membuat Modul Pelatihan <i>Administrator</i> Jaringan Komputer</li> <li>- Mengkonfigurasi dan merawat perangkat keras dan perangkat jaringan</li> <li>- Pemeliharaan portal ITS (<a href="http://www.its.ac.id">www.its.ac.id</a>)</li> </ul> | komputer<br><ol style="list-style-type: none"> <li>2. Mampu menangani dan me-maintain <i>server web/mail</i>, <i>switch</i>, manajemen <i>bandwidth</i></li> <li>1. Familiar dengan program-program <i>Open Source</i></li> <li>2. Mampu menganalisa masalah</li> <li>3. Mampu bekerja secara tim</li> </ol> |
| 10 | Petugas Administrasi Umum | <ul style="list-style-type: none"> <li>- Melaksanakan kebersihan dan menjaga keindahan LPTSI ITS</li> <li>- Mengirim surat</li> <li>- Membantu tugas-tugas lain yang diberikan oleh pimpinan</li> </ul>                                                                                                                                                                                                                                                                         | <ol style="list-style-type: none"> <li>1. Dapat berkomunikasi dengan baik</li> <li>2. Bertanggung jawab</li> </ol>                                                                                                                                                                                           |
|    |                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                              |

Gambar F.5 Uraian Tugas (lanj.)



**Gambar F.6 Masterplan ITS**

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div style="text-align: center;">  <p><b>PERATURAN PEMERINTAH REPUBLIK INDONESIA<br/>NOMOR 11 TAHUN 2002<br/>TENTANG</b></p> <p><b>PERUBAHAN ATAS<br/>PERATURAN PEMERINTAH NOMOR 98 TAHUN 2000<br/>TENTANG PENGADAAN PEGAWAI NEGERI SIPIL</b></p> <p><b>PRESIDEN REPUBLIK INDONESIA,</b></p> </div> <p>Menimbang :</p> <p>bahwa untuk mewujudkan Pegawai Negeri Sipil yang profesional dan bertanggung jawab dipandang perlu mengubah Peraturan Pemerintah Nomor 98 Tahun 2000 tentang Pengada Pegawai Negeri Sipil, dengan Peraturan Pemerintah;</p> <p>Mengingat :</p> <ol style="list-style-type: none"> <li>Pasal 5 ayat (2) Undang-Undang Dasar 1945;</li> <li>Undang-undang Nomor 8 Tahun 1974 tentang Pokok-pokok Kepegawaian (Lembaran Negara Tahun 1974 Nomor 55, Tambahan Lembaran Negara Nomor 3041), sebagaimana telah diubah dengan Undang-undang Nomor 43 Tahun 1999 (Lembaran Negara Tahun 1999 Nomor 11 Tambahan Lembaran Negara Nomor 3890);</li> <li>Undang-undang Nomor 22 Tahun 1999 tentang Pemerintahan Daerah (Lembaran Negara Tahun 1999 Nomor 60, Tambahan Lembaran Negara Nomor 3839);</li> <li>Undang-undang Nomor 25 Tahun 1999 tentang Perimbangan Keuangan Antara Pemerintah Pusat dan Daerah (Lembaran Negara Tahun 1999 Nomor 72, Tambahan Lembaran Negara Nomor 3848);</li> <li>Peraturan Pemerintah Nomor 25 Tahun 2000 tentang Kewenangan Pemerintah dan Kewenangan Propinsi Sebagai Daerah Otonom (Lembaran Negara Tahun 2000 Nomor 5, Tambahan Lembaran Negara Nomor 3952);</li> <li>Peraturan Pemerintah Nomor 96 Tahun 2000 tentang Wewenang Pengangkatan, Pemindahan, dan Pemberhentian Pegawai Negeri Sipil (Lembaran Negara Tahun 2000 Nomor 193, Tambahan Lembaran Negara Nomor 4014);</li> <li>Peraturan Pemerintah Nomor 97 Tahun 2000 tentang Formasi Pegawai Negeri Sipil (Lembaran Negara Tahun 2000 Nomor 194, Tambahan Lembaran Negara Nomor 4015);</li> <li>Peraturan Pemerintah Nomor 98 Tahun 2000 tentang Pengadaan Pegawai Negeri Sipil (Lembaran Negara Tahun 2000 Nomor 195, Tambahan Lembaran Negara Nomor 4016);</li> </ol> <p style="text-align: center;">MEMUTUSKAN :</p> <p>Menetapkan :</p> <p>PERATURAN PEMERINTAH TENTANG PERUBAHAN ATAS PERATURAN PEMERINTAH NOMOR TAHUN 2000 TENTANG PENGADAAN PEGAWAI NEGERI SIPIL.</p> | <p style="text-align: center;">Pasal I</p> <p>Beberapa ketentuan dalam Peraturan Pemerintah Nomor 98 Tahun 2000 tentang Pengadaan Pegawai Negeri Sipil diubah, sebagai berikut :</p> <ol style="list-style-type: none"> <li>Ketentuan Pasal 6 diubah, sehingga seluruhnya menjadi berbunyi sebagai berikut : <p style="text-align: center;">"Pasal 6</p> <p>(1) Syarat yang harus dipenuhi oleh setiap pelamar adalah :</p> <ol style="list-style-type: none"> <li>warga negara Indonesia;</li> <li>berusia serendah-rendahnya 18 (delapan belas) tahun dan setinggi-tingginya 35 (tiga puluh lima) tahun;</li> <li>tidak pernah dihukum penjara atau kurungan berdasarkan putusan pengadilan yang sudah mempunyai kekuatan hukum yang tetap, karena melakukan suatu tindak pidana kejahatan;</li> <li>tidak pernah diberhentikan dengan hormat tidak atas permintaan sendiri atau tidak dengan hormat sebagai Pegawai Negeri Sipil atau diberhentikan tidak dengan hormat sebagai pegawai swasta;</li> <li>tidak berkedudukan sebagai calon/Pegawai Negeri;</li> <li>mempunyai pendidikan, kecakapan, keahlian dan keterampilan yang diperlukan;</li> <li>berkelakuan baik;</li> <li>sehat jasmani dan rohani;</li> <li>bersedia ditempatkan di seluruh wilayah Negara Kesatuan Republik Indonesia atau negara lain yang ditentukan oleh pemerintah; dan</li> <li>syarat lain yang ditentukan dalam persyaratan jabatan.</li> </ol> <p>(2) Pengangkatan sebagai Calon Pegawai Negeri Sipil dapat dilakukan bagi mereka yang melebihi usia 35 (tiga puluh lima) tahun berdasarkan kebutuhan khusus dan dilaksanakan secara selektif."</p> </li> <li>Ketentuan Pasal 11 diubah, sehingga seluruhnya menjadi berbunyi sebagai berikut : <p style="text-align: center;">"Pasal 11</p> <p>(1) Pelamar yang dinyatakan lulus ujian penyaringan dan telah diberikan nomor identitas Pegawai Negeri Sipil diangkat sebagai Calon Pegawai Negeri Sipil.</p> <p>(2) Pengangkatan Calon Pegawai Negeri Sipil sebagaimana dimaksud dalam ayat (1) ditetapkan dengan keputusan Pejabat Pembina Kepegawaian.</p> <p>(3) Pengangkatan Calon Pegawai Negeri Sipil sebagaimana dimaksud dalam ayat (2) dilakukan dalam tahun anggaran berjalan dan penetapannya tidak boleh berlaku surut.</p> <p>(4) Golongan ruang yang ditetapkan untuk pengangkatan sebagai Calon Pegawai Negeri Sipil, adalah :</p> <ol style="list-style-type: none"> <li>Golongan ruang I/a bagi yang pada saat melamar serendah-rendahnya memiliki dan menggunakan Surat Tanda Tamat Belajar/Jazah Sekolah Dasar atau yang setingkat.</li> </ol> </li> </ol> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

**Gambar F.7 PP 11/02**

**Gambar F.8 PP 11/02 (lanj.)**





KOMPETENSI SUMBER DAYA MANUSIA

LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI

Tgl Terbit : 2 Oktober 2014

Halaman : 1 dari 4

| NO | NAMA FUNGSI KERJA                        | Minimal Jenjang Pendidikan | Bidang Keilmuan/Keahlian                           | Minimal Lama Pengalaman Kerja (tahun) | Kemampuan Pengelolaan TIK                                                                                                                                                                                                                                                                                | Pelatihan yang diperlukan                                                                                                                                                          |
|----|------------------------------------------|----------------------------|----------------------------------------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Ketua Lembaga                            | S2                         | T.elektro/T.Informatika                            | 10                                    | <ul style="list-style-type: none"> <li>• Menguasai Master Plan TIK di ITS</li> <li>• Menguasai pengelolaan infrastruktur dan sistem jaringan terkini</li> <li>• Memahami tata kelola TIK di ITS</li> <li>• Menguasai strategi implementasi TIK di ITS</li> <li>• Memahami sistem keamanan TIK</li> </ul> | <ul style="list-style-type: none"> <li>• Sistem Manajemen Mutu</li> <li>• Sistem Keamanan Jaringan</li> <li>• Disaster Recovery Management System for IT Infrastructure</li> </ul> |
| 2  | Sekretaris Lembaga                       | S2                         | T.elektro/T.Informatika                            | 10                                    | <ul style="list-style-type: none"> <li>• Menguasai bidang manajerial</li> <li>• Menguasai administrasi umum</li> <li>• Mampu mengkomunikasi program dan tujuan organisasi</li> </ul>                                                                                                                     | <ul style="list-style-type: none"> <li>• Sistem Manajemen Mutu</li> <li>• Manajerial</li> </ul>                                                                                    |
| 3  | Koord. Pusat Pengelolaan dan Layanan TIK | S2                         | Sist.Informasi/T.Industri /T.elektro/T.Informatika | 5                                     | <ul style="list-style-type: none"> <li>• Menguasai tata kelola TIK di ITS</li> <li>• Menguasai sistem dan aplikasi e-layanan ITS</li> <li>• Mampu mengelola kebutuhan pengguna terkait TIK</li> <li>• Mampu mengkomunikasikan produk TIK kepada pengguna</li> </ul>                                      | <ul style="list-style-type: none"> <li>• Sistem Manajemen Mutu</li> <li>• Sistem Helpdesk IT Terpadu</li> <li>• Audit ISO</li> </ul>                                               |
| 4  | Koord. Pusat Pengembangan SIM            | S2                         | T.elektro/T.Informatika                            | 5                                     | <ul style="list-style-type: none"> <li>• Menguasai sistem informasi manajemen di ITS</li> <li>• Mampu mengkoordinir proses pengembangan dan perawatan SIM</li> </ul>                                                                                                                                     | <ul style="list-style-type: none"> <li>• Sistem Keamanan Jaringan</li> <li>• Database System</li> </ul>                                                                            |

Gambar F.9 Kompetensi SDM



KOMPETENSI SUMBER DAYA MANUSIA

LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI

Tgl Terbit : 2 Oktober 2014

Halaman : 2 dari 4

| NO | NAMA FUNGSI KERJA                                 | Minimal Jenjang Pendidikan | Bidang Keilmuan/Keahlian                | Minimal Lama Pengalaman Kerja (tahun) | Kemampuan Pengelolaan TIK                                                                                                                                                                                                     | Pelatihan yang diperlukan                                                                                    |
|----|---------------------------------------------------|----------------------------|-----------------------------------------|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 5  | Koord. Pusat Data dan Pelaporan                   | S2                         | Sist.Informasi/T.elektro/ T.Informatika | 5                                     | <ul style="list-style-type: none"> <li>Memahami manajemen data terpadu</li> <li>Mampu mengkoordinir tim pengumpul dan pengolahan data di ITS</li> </ul>                                                                       | <ul style="list-style-type: none"> <li>Database System</li> <li>Statistical Data Analysis</li> </ul>         |
| 6  | Koord. Pusat Infrastruktur dan keamanan Informasi | S2                         | Sist.Informasi/T.elektro/ T.Informatika | 5                                     | <ul style="list-style-type: none"> <li>Memahami Infrastruktur dan keamanan Jaringan</li> <li>Mampu mengkoordinir tim</li> </ul>                                                                                               | <ul style="list-style-type: none"> <li>Network System</li> <li>Keamanan Jaringan</li> </ul>                  |
| 7  | Kasubag umum                                      | S1                         | T.elektro/T.Informatika                 | 5                                     | <ul style="list-style-type: none"> <li>Menguasai administrasi umum</li> <li>Menguasai peraturan pengadaan barang dan jasa</li> <li>Mampu mengkoordinir tim</li> </ul>                                                         | <ul style="list-style-type: none"> <li>ISO Management System</li> </ul>                                      |
| 8  | Petugas Service Desk                              | SMA/SMK                    | Umum                                    | 2                                     | <ul style="list-style-type: none"> <li>Menguasai sistem layanan TIK di ITS</li> <li>Mampu mengoperasikan NOC ITS</li> <li>Menguasai tata kelola keluhan pengguna</li> <li>Mampu mengelola dokumen terpusat di BTSI</li> </ul> | <ul style="list-style-type: none"> <li>ISO Management System</li> <li>Service Excellent</li> </ul>           |
| 9  | Analisis Sistem                                   | D3                         | Sist.Informasi/T.Informatika            | 3                                     | <ul style="list-style-type: none"> <li>Mampu menerjemahkan kebutuhan pengguna menjadi dokumen kebutuhan pengguna</li> <li>Menguasai software pembuat flowchart</li> </ul>                                                     | <ul style="list-style-type: none"> <li>Process Business Reengineering</li> <li>Dokumentasi Sistem</li> </ul> |
| 10 | Dokumentator                                      | D3                         | Sist.Informasi/T.elektro/ T.Informatika | 3                                     | <ul style="list-style-type: none"> <li>Mampu mendokumentasikan proses bisnis dan historis pengembangan SIM</li> </ul>                                                                                                         | <ul style="list-style-type: none"> <li>Dokumentasi Sistem</li> </ul>                                         |

Gambar F.10 Kompetensi SDM (lanj.)

|  |                   | <b>KOMPETENSI SUMBER DAYA MANUSIA</b><br><b>LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI</b> |                                                                      |                                       | Tgl Terbit : 2 Oktober 2014                                                                                                                                                                  |                                                                           |
|-----------------------------------------------------------------------------------|-------------------|-------------------------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
|                                                                                   |                   |                                                                                                 |                                                                      |                                       | Halaman : 3 dari 4                                                                                                                                                                           |                                                                           |
| NO                                                                                | NAMA FUNGSI KERJA | Minimal Jenjang Pendidikan                                                                      | Bidang Keilmuan/Keahlian                                             | Minimal Lama Pengalaman Kerja (tahun) | Kemampuan Pengelolaan TIK                                                                                                                                                                    | Pelatihan yang diperlukan                                                 |
|                                                                                   |                   |                                                                                                 |                                                                      |                                       | atau aplikasi atau sistem di BTSI<br>• Menguasai software dokumentasi                                                                                                                        |                                                                           |
| 11                                                                                | Analisis Data     | S1                                                                                              | Sist.Informasi/T.elektro/<br>T.Informatika/Statistika/<br>T.Industri | 3                                     | • Mampu mengolah data mentah menjadi informasi<br>• Menguasai teknik-teknik statistik<br>• Menguasai software pengolahan data atau software statistik                                        | • Statistical analysis for business                                       |
| 12                                                                                | Pengumpul Data    | D3                                                                                              | Sist.Informasi/T.elektro/<br>T.Informatika                           | 3                                     | • Menguasai teknik survey dan pengumpulan data<br>• Menguasai software dokumentasi data                                                                                                      | • Teknik Survey                                                           |
| 13                                                                                | Pengembang SIM    | S1/D4                                                                                           | T.elektro/T.Informatika                                              | 3                                     | • Mengetahui arsitektur SIM di ITS<br>• Mampu melakukan pengembangan SIM sesuai dengan standar software dan database yang ditetapkan BTSI<br>• Memahami konsep integrasi SIM                 | • Advanced programming technique<br>• Advanced MS SQL<br>• VB.Net Package |
| 14                                                                                | Perawat SIM       | S1/D4                                                                                           | T.elektro/T.Informatika                                              | 3                                     | • Mampu melakukan pelacakan kesalahan atau identifikasi kebutuhan pengguna dalam SIM<br>• Mampu melakukan perawatan SIM<br>• Mampu melakukan proses backup sistem dan database dalam sistem. | • Advanced programming technique                                          |
| 15                                                                                | Admin Jaringan    | D3                                                                                              | T.elektro/T.Informatika                                              | 3                                     | • Menguasai arsitektur jaringan dan server                                                                                                                                                   | •                                                                         |

Gambar F.11 Kompetensi SDM (lanj.)

|  |                            | <b>KOMPETENSI SUMBER DAYA MANUSIA</b><br><b>LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI</b> |                          |                                       | Tgl Terbit : 2 Oktober 2014                                                                                          |                                                                                                                      |
|-------------------------------------------------------------------------------------|----------------------------|-------------------------------------------------------------------------------------------------|--------------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
|                                                                                     |                            |                                                                                                 |                          |                                       | Halaman : 4 dari 4                                                                                                   |                                                                                                                      |
| NO                                                                                  | NAMA FUNGSI KERJA          | Minimal Jenjang Pendidikan                                                                      | Bidang Keilmuan/Keahlian | Minimal Lama Pengalaman Kerja (tahun) | Kemampuan Pengelolaan TIK                                                                                            | Pelatihan yang diperlukan                                                                                            |
|                                                                                     |                            |                                                                                                 |                          |                                       | di ITS<br>• Menguasai sistem jaringan dan server di ITS<br>• Menguasai standar layanan jaringan                      | inux Network Advanced<br>• atabase MS SQL Server Fundamental<br>• erver Administration<br>• CCNA<br>• CISCO Training |
| 16                                                                                  | Teknisi Jaringan           | SMA/SMK                                                                                         | T.elektro/T.Informatika  | 2                                     | • Menguasai teknik jaringan<br>• Memahami struktur dan standar layanan jaringan                                      | • inux System Administration<br>• ISCO Training                                                                      |
| 17                                                                                  | Petugas Pengelola Keuangan | SMA/SMK                                                                                         | Akuntansi/administrasi   | 2                                     | • Memahami standard, prosedur, dan regulasi sistem keuangan di ITS<br>• Menguasai SIM keuangan                       | • Manajemen Akuntansi                                                                                                |
| 18                                                                                  | Petugas Administrasi Umum  | SMA/SMK                                                                                         | Administrasi umum        | 2                                     | • Memahami prosedur dan standar layanan BSTI<br>• Mampu menerapkan manajemen administrasi yang rapi dan terstruktur. | • Good Houskeeping fo IT                                                                                             |

Gambar F.12 Kompetensi SDM (lanj.)

## CATEGORY ARCHIVES: SEMINAR

### Ikuti Seminar Keamanan Informasi (15 Sept) di Auditorium Pasca!

01/09/2016 AGENDA TERDEKAT, SEMINAR 3 Comments

Institut Teknologi Sepuluh Nopember melalui LPTSI dan Laboratorium Infrastruktur Keamanan Teknologi Informasi, Jurusan Sistem Informasi bekerja sama dengan Lembaga Sandi Negara (LEMSANEG) akan menyelenggarakan forum diskusi keamanan informasi.

Oleh karenanya, kami mengundang dosen, karyawan dan mahasiswa untuk bergabung dalam acara tersebut yang akan diselenggarakan pada:

Hari/Tanggal: Kamis/ 15 September 2016

Waktu: 08:00 – 12:30 WIB

Lokasi: Ruang Auditorium Pasca Sarjana ITS

Tema: "Apa itu *informasi privacy* dan bagaimana melindunginya?"

Pembicara pada acara ini yakni:

Sekretaris Utama Lembaga Sandi Negara (Bpk. Syahrul Mubarak, S.IP., M.M) dengan materi "Peran Persandian dalam Melindungi Informasi Privasi"  
Pemateri dari Komunitas ICT Watch (Bpk. Donny B.U.) dengan materi "Apa itu Informasi Privasi dan Bagaimana Melindunginya?"  
Koordinator Pusat Infrastruktur dan Keamanan Informasi, LPTSI (Bpk. Royyana Muslim Ijtihadie, S.Kom., M.Kom., Ph.D) dengan materi "Ancaman dan Serangan terhadap Informasi Privasi"

Bagaimana join acara ini?

Acara ini FREE. Untuk berpartisipasi, silahkan registrasi melalui [link di bawah ini](#).

Fasilitas: goodie bag dari Lemsaneg, snack, lunch, sertifikat

CP (Whatsapp Only):

Rima Jurusan Sistem Informasi (08813507624)

### Gambar F.13 Program Kesadaran Keamanan di Website DPTSI-ITS

Badan Teknologi dan Sistem Informasi ITS

## DOWNLOAD

[Materi Pelatihan](#)

[New-2017]

- Tutorial Setting Up Email Pimpinan di Outlook. [Download di sini](#).
- Tutorial Setting Up Email Pimpinan di Macbook. [Download di sini](#)
- Tutorial Setting Up Email Pimpinan di HP Android. [Download di sini](#)
- Tutorial Akses Email Pimpinan via e-Perkantoran. [Download di sini](#)
- Panduan Cara Menggunakan Server VPS ITS. [Download di sini](#)

[Materi Seminar/Workshop](#)

Forum Diskusi Keamanan Informasi (15 September 2016)

User Guide

- Materi pak Donny BU tentang "Data Pribadi dan Privasi". [Download di sini](#).
- Materi pak Royyana tentang "Ancaman dan Serangan terhadap Privasi Informasi". [Download di sini](#).
- Hasil survey tentang privasi dari pak Donny BU. [Download di sini](#).

Office

User Guide Office 365 bagi Dosen, Karyawan, Mahasiswa ITS. [Download di sini](#)

User Guide Office 365 bagi IT Admin. [Download di sini](#)

Office 365 Troubleshooting Guideline. [Download di sini](#)

Aktivasi Office. [Download di sini](#)

Aktivasi Office 2016. [Download di sini](#)

### Gambar F.14 Program Kesadaran Keamanan di Website DPTSI-ITS (lanj.)

Badan Teknologi dan Sistem Informasi ITS

and Google Student Ambassador ITS

presents:

### PELATIHAN ONENOTE, ONENOTE CLASS DAN OFFICE MIX BAGI DOSEN

22/11/2016 BERITA No comments

Pelatihan OneNote, OneNote Class dan Office Mix bagi dosen dilaksanakan pada tanggal 21 s.d. 22 November 2016 di Ruang Sidang Rektorat lantai 1, yang meliputi :

1. Pelatihan day 1 : pelatihan OneNote dan OneNote Class untuk optimalisasi pembelajaran, dilaksanakan pada tanggal 21 November 2016, waktu : 08.00 – 15.00 WIB
2. Pelatihan day 2 : pelatihan Office Mix untuk optimasi pembelajaran dan Microsoft for Education, dilaksanakan pada tanggal 22 November 2016, waktu 08.00 – 15.00 WIB



### Gambar F.15 Sosialisasi Pelatihan Sistem di Website DPTSI-ITS

Badan Teknologi dan Sistem Informasi ITS

and Google Student Ambassador ITS

presents:

LAUNCHING GMAIL@ITS AND SEMINAR

Agenda

Migrating to **Gmail@ITS** Accounts  
by: BTSI ITS

Google Apps: Makes Your Campus Life More Fun  
by: Denira Gunawan (Google)

More Info

click: <http://goo.gl/o7ov7>

Registration:



### Gambar F.16 Sosialisasi Pelatihan Sistem (lanj.)



MATRIK KEBUTUHAN PELATIHAN SDM

LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI

Halaman

: 1 dari 2

| N O | NAMA FUNGSI KERJA         | Pelaksana 2012-2016 | Pelatihan yang diperlukan           | Status | Rencana Jadwal Pelatihan |      |      |      |  |
|-----|---------------------------|---------------------|-------------------------------------|--------|--------------------------|------|------|------|--|
|     |                           |                     |                                     | 2014   | 2013                     | 2014 | 2015 | 2016 |  |
| 1   | Ketua Lembaga             | Ach. Affandi        | Sistem Manajemen Mutu               | Sudah  |                          |      |      |      |  |
|     |                           |                     | Integrated Data Centre Management   | Sudah  |                          |      |      |      |  |
|     |                           |                     | Disaster Recovery Management System | Sudah  |                          |      |      |      |  |
| 2   | Koord. Pusyan             | Arief R             | Sistem Manajemen Mutu               | Belum  |                          |      |      |      |  |
|     |                           |                     | Sistem Helpdesk IT Terpadu          | Belum  |                          |      |      |      |  |
|     |                           |                     | Audit ISO                           | Sudah  |                          |      |      |      |  |
| 3   | Koord. Pengembangan SIM   | Yuhana              | Sistem Keamanan Jaringan            | Belum  |                          |      |      |      |  |
|     |                           |                     | Database System                     | Belum  |                          |      |      |      |  |
| 4   | Koord. Data dan Pelaporan | Diana P             | Database System                     | Belum  |                          |      |      |      |  |
|     |                           |                     | Statistical Data Analysis           | Belum  |                          |      |      |      |  |
| 5   | Kasubag Umum              | Ardian N            | Audit Keuangan                      | Belum  |                          |      |      |      |  |
| 6   | Petugas Service Desk      | Mudjiatin           | ISO Management System               | Sudah  |                          |      |      |      |  |
|     |                           |                     | Service Excellent                   | Belum  |                          |      |      |      |  |
|     |                           | Jainul A            | ISO Management System               | Belum  |                          |      |      |      |  |
|     |                           |                     | Service Excellent                   | Belum  |                          |      |      |      |  |
| 7   | Analisis Sistem           | Widya               | Process Business Reengineering      | Belum  |                          |      |      |      |  |
|     |                           |                     | Dokumentasi Sistem                  | Belum  |                          |      |      |      |  |
| 8   | Dokumentator              | Wiwini              | Dokumentasi Sistem                  | Belum  |                          |      |      |      |  |
|     |                           |                     | Knowledge Management                | Belum  |                          |      |      |      |  |
| 9   | Analisis Data             | Arief P             | Big Data Management System          | Belum  |                          |      |      |      |  |
|     |                           |                     | Statistical analysis for business   | Belum  |                          |      |      |      |  |
| 10  | Pengumpul Data            | Inayati             | Teknik Survey Efektif               | Belum  |                          |      |      |      |  |
|     |                           |                     | Pengolahan Data Statistik Lanjut    |        |                          |      |      |      |  |

Gambar F.17 Matrik Kebutuhan Pelatihan SDM

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p>PRESIDEN<br/>REPUBLIK INDONESIA</p> <p>PERATURAN PEMERINTAH REPUBLIK INDONESIA<br/>NOMOR 53 TAHUN 2010<br/>TENTANG<br/>DISIPLIN PEGAWAI NEGERI SIPIL</p> <p>DENGAN RAHMAT TUHAN YANG MAHA ESA<br/>PRESIDEN REPUBLIK INDONESIA,</p> <p>Menimbang : a. bahwa Peraturan Pemerintah Nomor 30 Tahun 1980 tentang Peraturan Disiplin Pegawai Negeri Sipil sudah tidak sesuai dengan kebutuhan dan perkembangan keadaan;</p> <p>b. bahwa dalam rangka melaksanakan ketentuan Pasal 30 Undang-Undang Nomor 43 Tahun 1999 tentang Perubahan atas Undang-Undang Nomor 8 Tahun 1974 tentang Pokok-Pokok Kepegawaian, perlu mengganti Peraturan Pemerintah Nomor 30 Tahun 1980 tentang Peraturan Disiplin Pegawai Negeri Sipil;</p> <p>c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Pemerintah tentang Disiplin Pegawai Negeri Sipil;</p> <p>Mengingat : 1. Pasal 5 ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;</p> <p>2. Undang-Undang Nomor 8 Tahun 1974 tentang Pokok-Pokok Kepegawaian (Lembaran Negara Republik Indonesia Tahun 1974 Nomor 55, Tambahan Lembaran Negara Republik Indonesia Nomor 3041) sebagaimana telah diubah dengan Undang-Undang Nomor 43 Tahun 1999 (Lembaran Negara Republik</p> | <p>Bagian Kesatu<br/>Kewajiban</p> <p>Pasal 3</p> <p>Setiap PNS wajib:</p> <ol style="list-style-type: none"> <li>1. mengucapkan sumpah/janji PNS;</li> <li>2. mengucapkan sumpah/janji jabatan;</li> <li>3. setia . . .</li> </ol> <hr/>  <p>PRESIDEN<br/>REPUBLIK INDONESIA</p> <p>- 4 -</p> <ol style="list-style-type: none"> <li>3. setia dan taat sepenuhnya kepada Pancasila, Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Negara Kesatuan Republik Indonesia, dan Pemerintah;</li> <li>4. menaati segala ketentuan peraturan perundang-undangan;</li> <li>5. melaksanakan tugas kedinasan yang dipercayakan kepada PNS dengan penuh pengabdian, kesadaran, dan tanggung jawab;</li> <li>6. menjunjung tinggi kehormatan negara, Pemerintah, dan martabat PNS;</li> <li>7. mengutamakan kepentingan negara daripada kepentingan sendiri, seseorang, dan/atau golongan;</li> <li>8. memegang rahasia jabatan yang menurut sifatnya atau menurut perintah harus dirahasiakan;</li> </ol> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Gambar F.18 PP 53/10

Gambar F.19 PP 53/10 (lanj.)

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>10. melaporkan dengan segera kepada atasannya apabila mengetahui ada hal yang dapat membahayakan atau merugikan negara atau Pemerintah terutama di bidang keamanan, keuangan, dan materiil;</p> <p>11. masuk kerja dan menaati ketentuan jam kerja;</p> <p>12. mencapai sasaran kerja pegawai yang ditetapkan;</p> <p>13. menggunakan dan memelihara barang-barang milik negara dengan sebaik-baiknya;</p> <p>14. memberikan pelayanan sebaik-baiknya kepada masyarakat;</p> <p>15. membimbing bawahan dalam melaksanakan tugas;</p> <p>16. memberikan kesempatan kepada bawahan untuk mengembangkan karier; dan</p> <p>17. menaati peraturan kedisiplinan yang ditetapkan oleh pejabat yang berwenang.</p> <p>Bagian Kedua . . .</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | <p>2. menjadi perantara untuk mendapatkan keuntungan pribadi dan/atau orang lain dengan menggunakan kewenangan orang lain;</p> <p>3. tanpa izin Pemerintah menjadi pegawai atau bekerja untuk negara lain dan/atau lembaga atau organisasi internasional;</p> <p>4. bekerja pada perusahaan asing, konsultan asing, atau lembaga swadaya masyarakat asing;</p> <p>5. memiliki, menjual, membeli, menggadaikan, menyewakan, atau meminjamkan barang-barang baik bergerak atau tidak bergerak, dokumen atau surat berharga milik negara secara tidak sah;</p> <p>6. melakukan kegiatan bersama dengan atasan, teman sejawat, bawahan, atau orang lain di dalam maupun di luar lingkungan kerjanya dengan tujuan untuk keuntungan pribadi, golongan, atau pihak lain, yang secara langsung atau tidak langsung merugikan negara;</p> <p>7. memberi atau menyanggupi akan memberi sesuatu kepada siapapun baik secara langsung atau tidak langsung dan dengan dalih apapun untuk diangkat dalam jabatan;</p> <p>8. menerima hadiah atau suatu pemberian apa saja dari siapapun juga yang berhubungan dengan jabatan dan/atau pekerjaannya;</p> <p>9. bertindak sewenang-wenang terhadap bawahannya;</p> |
| <div data-bbox="435 723 517 806"></div> <p>PRESIDEN<br/>REPUBLIK INDONESIA</p> <p>- 5 -</p> <p>Bagian Kedua<br/>Larangan<br/>Pasal 4</p> <p>Setiap PNS dilarang:</p> <p>1. menyalahgunakan wewenang;</p> <p>Gambar F.20 PP 53/10 (lanj.)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <p>Gambar F.21 PP 53/10 (lanj.)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <p>Pasal 6</p> <p>Dengan tidak mengesampingkan ketentuan dalam peraturan perundang-undangan pidana, PNS yang melakukan pelanggaran disiplin dijatuhi hukuman disiplin.</p> <p>Bagian Kedua<br/>Tingkat dan Jenis Hukuman Disiplin</p> <p>Pasal 7</p> <p>(1) Tingkat hukuman disiplin terdiri dari:</p> <ol style="list-style-type: none"> <li>hukuman disiplin ringan;</li> <li>hukuman disiplin sedang; dan</li> <li>hukuman disiplin berat.</li> </ol> <p>(2) Jenis hukuman disiplin ringan sebagaimana dimaksud pada ayat (1) huruf a terdiri dari:</p> <ol style="list-style-type: none"> <li>teguran lisan;</li> <li>teguran tertulis; dan</li> <li>pernyataan tidak puas secara tertulis.</li> </ol> <p>(3) Jenis hukuman disiplin sedang sebagaimana dimaksud pada ayat (1) huruf b terdiri dari:</p> <ol style="list-style-type: none"> <li>penundaan kenaikan gaji berkala selama 1 (satu) tahun;</li> <li>penundaan kenaikan pangkat selama 1 (satu) tahun; dan</li> <li>penurunan pangkat setingkat lebih rendah selama 1 (satu) tahun.</li> </ol> <p>(4) Jenis hukuman disiplin berat sebagaimana dimaksud pada ayat (1) huruf c terdiri dari:</p> <ol style="list-style-type: none"> <li>penurunan pangkat setingkat lebih rendah selama 3 (tiga) tahun;</li> <li>pemindahan dalam rangka penurunan jabatan setingkat lebih rendah;</li> <li>pembebasan . . .</li> </ol> <p>Gambar F.22 PP 53/10 (lanj.)</p> | <ol style="list-style-type: none"> <li>pembebasan dari jabatan;</li> <li>pemberhentian dengan hormat tidak atas permintaan sendiri sebagai PNS; dan</li> <li>pemberhentian tidak dengan hormat sebagai PNS.</li> </ol> <p>Bagian Ketiga<br/>Pelanggaran dan Jenis Hukuman</p> <p>Paragraf 1<br/>Pelanggaran Terhadap Kewajiban</p> <p>Pasal 8</p> <p>Hukuman disiplin ringan sebagaimana dimaksud dalam Pasal 7 ayat (2) dijatuhkan bagi pelanggaran terhadap kewajiban:</p> <ol style="list-style-type: none"> <li>setia dan taat sepenuhnya kepada Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Negara Kesatuan Republik Indonesia, dan Pemerintah sebagaimana dimaksud dalam Pasal 3 angka 3, apabila pelanggaran berdampak negatif pada unit kerja;</li> <li>menaati segala peraturan perundang-undangan sebagaimana dimaksud dalam Pasal 3 angka 4, apabila pelanggaran berdampak negatif pada unit kerja;</li> <li>melaksanakan tugas kedinasan yang dipercayakan kepada PNS dengan penuh pengabdian, kesadaran, dan tanggung jawab sebagaimana dimaksud dalam Pasal 3 angka 5, apabila pelanggaran berdampak</li> </ol> <p>Gambar F.23 PP 53/10 (lanj.)</p>       |



## Ketentuan Layanan

Seluruh pengguna harus bersedia diperlakukan SAMA tanpa memandang status dan kedudukan. Selain itu, pengguna email ITS TIDAK diperkenankan:

1. Menggunakan/memanfaatkan email ITS untuk tujuan yang bertentangan dengan hukum di Indonesia ataupun Internasional
2. Menggunakan email ITS untuk mengirimkan pesan-pesan yang berbau SARA, pornografi, menakut-nakuti, mengancam seseorang, membantu penyebaran virus atau email yang berisikan rutin program yang dapat merusak komputer orang lain.
3. Menjual kembali email ITS ke pihak ketiga.
4. Menyerahkan Kata Sandinya ke pihak ketiga.
5. Menggunakan email ITS untuk SPAMMING.

Bagi ITS :

1. ITS menjamin dan menghormati kerahasiaan data pribadi setiap anggota dan berhak memberikan informasi kepada pihak ketiga berdasarkan persetujuan pengguna.
2. Kapasitas Email yang disediakan ITS adalah 20 MegaBytes, besar kapasitas email dapat berubah sewaktu-waktu.
3. ITS TIDAK bertanggung jawab atas hilangnya data/email yang disimpan pada server ITS.
4. ITS TIDAK bertanggung jawab atas kerusakan perangkat keras dan lunak pelanggan yang diakibatkan atas penggunaan fasilitas ITS.
5. ITS BERHAK menghapus keanggotaan email JIKA tidak aktif selama 3 bulan.
6. ITS BERHAK mematikan server mail untuk perawatan server mail sewaktu-waktu tanpa memberitahukan terlebih dahulu ke pengguna email ITS.
7. ITS BERHAK untuk menghentikan layanan email gratis ini sewaktu-waktu tanpa memberitahukan terlebih dahulu kepada pengguna email ITS.
8. ITS DAPAT menambah kesepakatan tanpa merubah inti kesepakatan.
9. ITS BERHAK untuk menghapus keanggotaan mail di ITS apabila pengguna tidak mematuhi kesepakatan yang tersebut diatas.
10. ITS BERHAK memberikan data pada pihak yang berwajib jika pada suatu saat menurut ketentuan hukum yang berlaku dianggap perlu.
11. ITS BERHAK memberikan informasi dari pihak ketiga kepada para pengguna email ITS tanpa pemberitahuan terlebih dahulu.

Penggunaan Mail Client

Layanan Lain

Web ITS

Web LPTSI

Portal Google Apps For Edu

Portal Software Lisensi ITS

Portal Software GPL ITS

Mirror ITS

Direktori ITS

Gambar F.24 Ketentuan Layanan *Email*

PERATURAN PEMERINTAH REPUBLIK INDONESIA

NOMOR 32 TAHUN 1979

TENTANG

PEMBERHENTIAN PEGAWAI NEGERI SIPIL

PRESIDEN REPUBLIK INDONESIA,

Menimbang : bahwa ketentuan-ketentuan mengenai pemberhentian Pegawai Negeri Sipil yang sekarang berlaku, dipandang tidak sesuai lagi dengan keadaan dewasa ini, oleh sebab itu perlu ditinjau kembali dan disempurnakan;

Mengingat : 1. Pasal 5 ayat (2) Undang-Undang Dasar 1945;

2. Undang-undang Nomor 8 Tahun 1974 tentang Pokok-pokok Kepegawaian (Lembaran Negara Tahun 1974 Nomor 55, Tambahan Lembaran Negara Nomor 3041);

MEMUTUSKAN :

Menetapkan : PERATURAN PEMERINTAH TENTANG PEMBERHENTIAN PEGAWAI NEGERI SIPIL .

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Pemerintah ini yang dimaksud dengan :

- a. pemberhentian sebagai Pegawai Negeri Sipil adalah pemberhentian yang mengakibatkan yang bersangkutan kehilangan statusnya sebagai Pegawai Negeri Sipil;
- b. pemberhentian dari jabatan negeri adalah pemberhentian yang mengakibatkan yang bersangkutan tidak bekerja lagi pada suatu satuan organisasi Negara, tetapi masih tetap masih berstatus

Gambar F.25 PP 32/79

Pemberhentian Karena Melakukan

Pelanggaran/Tindak Pidana/Penyelewengan

Pasal 8

Pegawai Negeri Sipil dapat diberhentikan tidak dengan hormat sebagai Pegawai Negeri Sipil karena :

- a. melanggar Sumpah/Janji Pegawai Negeri Sipil, Sumpah/Janji Jabatan Negeri atau Peraturan Disiplin Pegawai Negeri Sipil; atau
- b. dihukum penjara, berdasarkan keputusan Pengadilan yang sudah mempunyai kekuatan hukum yang tetap, karena dengan sengaja melakukan suatu tindakan pidana kejahatan yang diancam dengan pidana penjara setinggi-tingginya 4 (empat) tahun, atau diancam dengan pidana yang lebih berat.

Pasal 9

Pegawai Negeri Sipil diberhentikan tidak dengan hormat sebagai Pegawai Negeri Sipil apabila dipidana penjara atau kurungan berdasarkan keputusan Pengadilan yang telah mempunyai kekuatan hukum yang tetap, karena :

- a. melakukan suatu tindak pidana kejahatan jabatan atau tindak pidana kejahatan yang ada hubungannya dengan jabatan; atau
- b. melakukan suatu tindak pidana kejahatan sebagaimana dimaksud dalam pasal 104 sampai dengan Pasal 161 Kitab Undang-undang Hukum Pidana.

Pasal 10

Pegawai Negeri Sipil diberhentikan tidak dengan hormat sebagai Pegawai Negeri Sipil apabila ternyata melakukan usaha atau kegiatan yang bertujuan mengubah Pancasila dan atau Undang-Undang Dasar 1945 atau terlibat dalam gerakan atau melakukan kegiatan yang menentang Negara dan atau Pemerintah.

Bagian Kelima

Pemberhentian Karena Tidak Cakap Jasmani atau Rohani

Gambar F.26 PP 32/79 (lanj.)

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p style="text-align: center;"> <br/> PRESIDEN<br/>REPUBLIK INDONESIA </p> <p style="text-align: center;"> <b>PERATURAN PEMERINTAH REPUBLIK INDONESIA</b><br/> <b>NOMOR 65 TAHUN 2008</b><br/> <b>TENTANG</b><br/> <b>PERUBAHAN KEDUA ATAS</b><br/> <b>PERATURAN PEMERINTAH NOMOR 32 TAHUN 1979</b><br/> <b>TENTANG PEMBERHENTIAN PEGAWAI NEGERI SIPIL</b> </p> <p style="text-align: center;"> DENGAN RAHMAT TUHAN YANG MAHA ESA<br/> PRESIDEN REPUBLIK INDONESIA, </p> <p> Menimbang : a. bahwa dalam rangka menjamin kelangsungan tugas tertentu, diperlukan perpanjangan batas usia pensiun bagi jabatan eselon I tertentu; </p> <p> b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Pemerintah tentang Perubahan Kedua Atas Peraturan Pemerintah Nomor 32 Tahun 1979 tentang Pemberhentian Pegawai Negeri Sipil; </p> <p> Mengingat : 1. Pasal 5 ayat (2) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945; </p> <p> 2. Undang-Undang Nomor 8 Tahun 1974 tentang Pokok-Pokok Kepegawatan (Lembaran Negara Republik Indonesia Tahun 1974 Nomor 55, Tambahan Lembaran Negara Republik Indonesia Nomor 3041) sebagaimana telah diubah dengan Undang-Undang Nomor 43 Tahun 1999 tentang Perubahan Atas Undang-Undang Nomor 8 Tahun 1974 tentang Pokok-Pokok Kepegawatan (Lembaran Negara Republik Indonesia Tahun </p> | <p style="text-align: center;"> <br/> PRESIDEN<br/>REPUBLIK INDONESIA </p> <p style="text-align: center;">- 3 -</p> <p style="text-align: center;">*Pasal 4</p> <p> (1) Batas usia pensiun sebagaimana dimaksud dalam Pasal 3, dapat diperpanjang bagi Pegawai Negeri Sipil yang memegang jabatan tertentu. </p> <p> (2) Perpanjangan batas usia pensiun sebagaimana dimaksud pada ayat (1) sampai dengan: </p> <p> a. 65 (enam puluh lima) tahun bagi Pegawai Negeri Sipil yang memegang: </p> <ol style="list-style-type: none"> <li>jabatan Peneliti Madya dan Peneliti Utama yang ditugaskan secara penuh di bidang penelitian; atau</li> <li>jabatan lain yang ditentukan oleh Presiden;</li> </ol> <p> b. 60 (enam puluh) tahun bagi Pegawai Negeri Sipil yang memegang: </p> <ol style="list-style-type: none"> <li>jabatan struktural Eselon I;</li> <li>jabatan struktural Eselon II;</li> <li>jabatan Dokter yang ditugaskan secara penuh pada unit pelayanan kesehatan negeri;</li> <li>jabatan Pengawas Sekolah Menengah Atas, Sekolah Menengah Pertama, Sekolah Dasar, Taman Kanak-Kanak atau jabatan lain yang sederajat; atau</li> <li>jabatan lain yang ditentukan oleh Presiden;</li> </ol> <p> c. 58 (lima puluh delapan) tahun bagi Pegawai Negeri Sipil yang memegang: </p> <ol style="list-style-type: none"> <li>jabatan Hakim pada Mahkamah Pelayaran; atau</li> </ol> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Gambar F.27 PP 65/08

Gambar F.28 PP 65/08 (lanj.)

| No  | Nama Lokasi                                     | Kode Barang | Nup | Nama Barang       | merk_type                               | Kondisi |    |    |    |
|-----|-------------------------------------------------|-------------|-----|-------------------|-----------------------------------------|---------|----|----|----|
|     |                                                 |             |     |                   |                                         | B       | RR | RB | TD |
| 459 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 12  | Server            | HPPROLIANT DL 145 R G3,AMD OPTERON2.2   | v       |    |    |    |
| 460 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 13  | Server            | HPPROLIANT DL 145 R G3,AMD OPTERON2.2   | v       |    |    |    |
| 461 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 14  | Server            | HPPROLIANT DL 145 R G3,AMD OPTERON2.2   | v       |    |    |    |
| 462 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 10  | Server            | Intel Xeon 6C ProcesorX5670             | v       |    |    |    |
| 463 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 1   | Server            | Server Merk Altos                       |         |    | v  |    |
| 464 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 20  | Server            | Server seleksi & Alokasi                | v       |    |    |    |
| 465 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 15  | Server            | Server Web & Download                   | v       |    |    |    |
| 466 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 16  | Server            | Server Web & Download                   | v       |    |    |    |
| 467 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 17  | Server            | Server Web & Download                   | v       |    |    |    |
| 468 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 18  | Server            | Server Web & Download                   | v       |    |    |    |
| 469 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 19  | Server            | Server Web & Download                   | v       |    |    |    |
| 470 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 21  | Server            | UPS ICA RN 3200C                        | v       |    |    |    |
| 471 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 22  | Server            | UPS ICA RN 3200C                        | v       |    |    |    |
| 472 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 23  | Server            | UPS ICA RN 3200C                        | v       |    |    |    |
| 473 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3100204001  | 4   | Server            | Xeon                                    | v       |    |    |    |
| 474 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3050201005  | 1   | Sice              | Kursi tamu                              | v       |    |    |    |
| 475 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3050201005  | 2   | Sice              | Sofa                                    | v       |    |    |    |
| 476 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 3080703004  | 1   | Software DAAS MOD | Software Pengemb. Sistem Infor Manj (CM | v       |    |    |    |
| 477 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 8010101001  | 32  | Software Komputer | ADOBE                                   | v       |    |    |    |
| 478 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 8010101001  | 33  | Software Komputer | ADOBE                                   | v       |    |    |    |
| 479 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 8010101001  | 34  | Software Komputer | Adobe                                   | v       |    |    |    |
| 480 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 8010101001  | 13  | Software Komputer | Adobe Creative Suite 5 Master           | v       |    |    |    |
| 481 | LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI | 8010101001  | 14  | Software Komputer | Adobe Creative Suite 5 Master           | v       |    |    |    |

Gambar F.29 Daftar Inventaris Aset

DEPARTEMEN PENDIDIKAN NASIONAL  
DITJEN PENDIDIKAN TINGGI  
ITS

DAFTAR INVENTARIS RUANGAN ( DIR )

NAMA UPB : UPT PUSAT KOMPUTER  
KODE UPB : 023.04.05.414964.048

NAMA RUANGAN : R. PROS  
KODE RUANGAN :

| No | NUP | Nama Barang       | Identitas Barang        |            |         | Jumlah<br>Barang | Penguasaan | Keterangan |
|----|-----|-------------------|-------------------------|------------|---------|------------------|------------|------------|
|    |     |                   | Merk/Type               | Kd Brg     | Th Prlh |                  |            |            |
| 1  | 2   | 3                 | 4                       | 5          | 6       | 7                | 8          |            |
| 1  |     | Kursi Besi/Metal  |                         | 2050103007 |         | 5                | PUSKOM     |            |
| 2  |     | Scanner           | OpSCAN5                 |            |         | 1                | PUSKOM     |            |
| 3  |     | Printer           | Epson/LQ2180            |            |         | 2                | PUSKOM     |            |
| 4  |     | Filing Cabinet    | Bostinco/4 laci         | 2050104005 |         | 1                | PUSKOM     |            |
| 5  |     | Lemari Besi       | Bostinco                | 2050104001 |         | 1                | PUSKOM     |            |
| 6  |     | Lemari Besi       | Asahi                   | 2050104001 |         | 1                | PUSKOM     |            |
| 7  |     | Rak Besi          |                         |            |         | 1                | PUSKOM     |            |
| 8  |     | Meja Komputer     | Coklat                  | 2050201009 |         | 7                | PUSKOM     |            |
| 9  |     | Meja Komputer     | CD90                    | 2050201008 |         | 2                | PUSKOM     |            |
| 10 |     | Meja Print        | Besi                    |            |         | 1                | PUSKOM     |            |
| 11 |     | Personal Komputer | HP/idx7800              | 2050204006 |         | 4                | PUSKOM     |            |
| 12 |     | Personal Komputer | Sim-X/PIV               | 2120102001 |         | 1                | PUSKOM     |            |
| 13 |     | UPS               | ICA                     | 2050206017 |         | 1                | PUSKOM     |            |
| 14 |     | AC Split          | Nasional                | 2050204004 |         | 1                | PUSKOM     |            |
| 15 |     | AC Split          | Panasonic/<br>CS-PC9GKJ | 2050204004 |         | 1                | PUSKOM     |            |

Surabaya, 1 Nopember 2011

Penanggungjawab Ruangan,

Kasubbag TU,

*Handwritten signature*

*Handwritten signature*

Gambar F.30 Daftar Inventaris Ruangan

| TAHUN 2014 |                                    |           |                                                                              |             |            |
|------------|------------------------------------|-----------|------------------------------------------------------------------------------|-------------|------------|
| NO         | NAMA SISTEM INFORMASI              | PUSAT PIC | NAMA KEGIATAN                                                                | DOKUMENTASI | MODUL PENG |
| 1          | SIM TUGAS AKHIR                    | PUSBANG   | Pengembangan modul Tugas Akhir (SIM Akademis dan Kemahasiswaan)              | v           | v          |
| 2          | SIM AKADEMIK DAN SIM INVENTARISASI | PUSBANG   | Implementasi modul Yudisium, DO, Wisuda dan SI Manajemen                     | v           | v          |
| 3          | SIM KEPEGAWAIAN                    | PUSBANG   | SIM (SIM Akademis dan Kemahasiswaan [Integra.ITS], dan tridharma PT terpadu) | v           | v          |
| 4          | SIM KEPEGAWAIAN                    | PUSBANG   | Pengembangan modul tugas belajar, ijin belajar, mutasi dan peng              | v           | v          |
| 5          | MODUL QUESIONER                    | PUSDATA   | Pengembangan Sistem Monitoring Kinerja Pegawai                               | v           | v          |
| 6          | DASHBOARD DATA                     | PUSDATA   | Pembuatan Jasa Sistem Pengolahan Data Kuesioner Survei                       | v           | v          |
| 7          | SIM KEPEGAWAIAN                    | PUSDATA   | Kepuasan secara Online                                                       | v           | v          |
| 8          | SIM KEARSIPAN                      | PUSDATA   | Pembuatan Dashboard Data Akademik, Data Dosen, dan Data PNS                  | v           | v          |
| 9          | SIM KERJA PRAKTEK                  | PUSYAN    | Pembuatan Situs Profil Peneliti dan Relasinya                                | v           | v          |
| 10         | WEBSITE                            | PUSYAN    | Pengembangan SIM Kearsipan                                                   | v           | v          |
| 11         | WEBSITE                            | PUSYAN    | Pembangunan SIM Kerja Praktek ITS                                            | v           | v          |
| 12         | SIM MEDICAL CENTRE                 | PUSYAN    | Pembangunan Master Website Jurusan                                           | v           | v          |
| 13         | SIM E-TICKET                       | PUSYAN    | Pengembangan Master Website Unit Kerja Pusat                                 | v           | v          |
| 14         | APLIKASI PANAROMA                  | PUSYAN    | Pembangunan SIM Medical Centre Terpadu                                       | v           | v          |
|            |                                    |           | Pengembangan e-Ticket untuk Layanan ITS                                      | v           | v          |
|            |                                    |           | Pengembangan Aplikasi Panorama ITS                                           | v           | v          |

Gambar F.31 Daftar Inventaris SIM



| DAFTAR REKAMAN MUTU       |                                |             |                              |                             |              |
|---------------------------|--------------------------------|-------------|------------------------------|-----------------------------|--------------|
| No.                       | JUDUL REKAMAN                  | MASA SIMPAN | LOKASI SIMPAN                | PENANGGUNG JAWAB            | METODE INDEK |
| 1                         | Arsip Kepegawaian              | 5 Tahun     | Almari Ka.Subbag. & Hardisk  | Ka. Subbag                  | urut abjad   |
| 2                         | Arsip SK                       | 5 Tahun     | Almari Ka.Subbag. & Hardisk  | Ka. Subbag                  | urut abjad   |
| 3                         | Arsip Inventaris               | 5 Tahun     | Almari Inventaris            | Bag. Inventaris             | Urut Ruang   |
| 4                         | Arsip Surat Masuk              | 2 Tahun     | Almari Sekretariat           | Sekretariat                 | Tanggal      |
| 5                         | Arsip Surat Keluar             | 2 Tahun     | Almari Sekretariat           | Sekretariat                 | Tanggal      |
| 6                         | Arsip Kehadiran Pegawai        | 2 Tahun     | Almari Sekretariat           | Sekretariat                 | bulan        |
| 7                         | Arsip Keuangan                 | 10 tahun    | UPT Kearsipan ITS            | Pemegang Uang Muka          | kelompok     |
| 8                         | Arsip Data Jaringan            | 5 Tahun     | noc.its.ac.id                | Admin Jaringan              | kelompok     |
| 9                         | Arsip Data Email               | 5 Tahun     | mail.its.ac.id               | Admin Jaringan              | urut abjad   |
| 10                        | Arsip Stock Barang             | 2 Tahun     | Ruang Administrasi           | Pelaksana Gudang            | urut laporan |
| 11                        | Arsip Notulen Rapat            | 1 Tahun     | server                       | Admin                       | -            |
| 12                        | Buku Kas Harian                | 5 tahun     | Lemari arsip Bagian keuangan | Pemegang Uang Muka          | kelompok     |
| 13                        | Buku Tabelaris                 | 5 Tahun     | Lemari arsip Bagian keuangan | Pemegang Uang Muka          | kelompok     |
| 14                        | Buku Bank                      | 5 tahun     | Lemari arsip Bagian keuangan | Pemegang Uang Muka          | kelompok     |
| 15                        | Buku Pajak                     | 5 Tahun     | Lemari arsip Bagian keuangan | Pemegang Uang Muka          | kelompok     |
| 16                        | Dokumentasi Kunjungan Instansi | 5 Tahun     | Almari Sekretariat           | Sekretariat                 | urut tanggal |
| 17                        | Arsip Pengaduan Pelanggan      | 5 Tahun     | noc.its.ac.id                | Admin Jaringan              | kelompok     |
| 18                        | Penilaian Rekanan              | 5 Tahun     | Lemari Ka. Subbag. TU        | Ka. Subbag. TU              | kelompok     |
| 19                        | Arsip Pelatihan                | 5 Tahun     | Almari Sekretariat           | Sekretariat                 | urut tanggal |
| Diketahui oleh :          |                                |             |                              | TANGGAL : 2 Oktober 2014    |              |
| Diana Ekawati,ST.         |                                |             |                              | Dibuat Oleh :               |              |
| MANAGEMENT REPRESENTATIVE |                                |             |                              | Dr. Ir. Achmad Affandi,DEA. |              |
|                           |                                |             |                              | KETUA LPTSI ITS             |              |

Gambar F.32 Daftar Rekaman Mutu

|                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p style="text-align: center;"><b>INSTRUKSI KERJA<br/>SCANNER</b></p> <ul style="list-style-type: none"> <li>• Nyalakan komputer yang terhubung dengan scanner</li> <li>• Nyalakan scanner dengan menekan tombol on</li> <li>• Buka program scanner</li> <li>• Scanner siap digunakan</li> <li>• Untuk mematikan scanner, tekan tombol off</li> </ul> <p>Gambar F.33 Instruksi Kerja Penggunaan<br/><i>Scanner</i></p> | <p style="text-align: center;"><b>INSTRUKSI KERJA<br/>SERVER</b></p> <ul style="list-style-type: none"> <li>○ Server dinyalakan dengan menekan tombol power</li> <li>○ Apabila terjadi trouble lakukan analisa</li> <li>○ Lakukan Perbaikan.</li> </ul> <p>Gambar F.34 Instruksi Kerja Penggunaan<br/><i>Server</i></p> |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p style="text-align: center;"><b>INSTRUKSI KERJA<br/>ROUTER</b></p> <ul style="list-style-type: none"> <li>○ Router dinyalakan dengan menekan tombol power</li> <li>○ Apabila terjadi trouble lakukan analisa</li> <li>○ Lakukan Perbaikan.</li> </ul> <p>Gambar F.35 Instruksi Kerja Penggunaan<br/><i>Router</i></p> | <p style="text-align: center;"><b>INSTRUKSI KERJA<br/>SWITCH/HUB</b></p> <ul style="list-style-type: none"> <li>○ Switch / HUB dinyalakan dengan menekan tombol power</li> <li>○ Apabila terjadi trouble lakukan analisa</li> <li>○ Lakukan Perbaikan.</li> </ul> <p>Gambar F.36 Instruksi Kerja Penggunaan<br/><i>Switch/Hub</i></p>                                                                                                                                                                                                         |
| <p style="text-align: center;"><b>INSTRUKSI KERJA<br/>HT</b></p> <ul style="list-style-type: none"> <li>○ Tekan Tombol 'on' untuk menyalakan.</li> <li>○ Telan tombol 'talk' untuk berbicara.</li> </ul> <p>Gambar F.37 Instruksi Kerja Penggunaan<br/><i>HT</i></p>                                                    | <p style="text-align: center;"><b>INSTRUKSI KERJA<br/>APAR</b></p> <ul style="list-style-type: none"> <li>• Lepaskan segel pada APAR</li> <li>• Lepaskan kunci pengaman (ring silver) pada pegangan</li> <li>• Buka tutup ujung selang</li> <li>• Arahkan selang dengan jarak 2 meter dari sumber api</li> <li>• Pada waktu melakukan penyemprotan pegang selang supaya fokus ke sumber api</li> <li>• Tekan handle hingga gas keluar untuk digunakan memadamkan api</li> </ul> <p>Gambar F.38 Instruksi Kerja Penggunaan<br/><b>APAR</b></p> |

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**  
**BADAN TEKNOLOGI DAN SISTEM INFORMASI**

|                                 |                                 |
|---------------------------------|---------------------------------|
| POB-TSI-05                      | Revisi : 00                     |
| PROSEDUR OPERASIONAL BAKU (POB) | Tanggal terbit : 7 Januari 2013 |
| PEMUSNAHAN DOKUMEN              | Halaman : 1 dari 3              |

|                          |                              |
|--------------------------|------------------------------|
| Dibuat :                 | Disetujui :                  |
| Suroso                   | Dr. Ir. Achmad Affandi, DEA. |
| Staf BTSi                | Kepala BTSi                  |
| Tanggal : 7 Januari 2013 | Tanggal : 7 Januari 2013     |

Catatan :

- Prosedur Sistem ini diterbitkan untuk digunakan internal dibawah kewenangan BTSi
- Siapaapun dilarang mengandakan prosedur sistem ini tanpa izin tertulis dari BTSi ITS

- Tujuan**  
Tertib administrasi
- Ruang Lingkup**  
Pelanggan, Bagian Arsip
- Definisi**  
Pelanggan adalah orang/lembaga/instansi yang menggunakan jasa UPT PUSKOM  
Bagian Arsip adalah petugas UPT PUSKOM yang bertanggungjawab terhadap pengarsipan dokumen Pelanggan
- Dokumen terkait**  
Berita Acara Pemusnahan Dokumen Pelanggan
- Rincian Prosedur**

| NO | PENANGGUNG JAWAB    | AKTIVITAS                                                                                                                                                                                                 |
|----|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | <u>Pelanggan</u>    | <ul style="list-style-type: none"> <li>Mengambil dokumen pelanggan atau memberikan kewenangan untuk memusnahkan dokumen kepada UPT PUSKOM</li> </ul>                                                      |
| 2  | <u>Bagian Arsip</u> | <ul style="list-style-type: none"> <li>Mengirim surat pemberitahuan kepada pelanggan bahwa dokumen miliknya sudah habis masa simpan</li> <li>Membuat Berita Acara Pemusnahan Dokumen Pelanggan</li> </ul> |

Gambar F.39 Prosedur Pemusnahan Dokumen

## Akses Internet di Kampus ITS

ITS akan secara bertahap menerapkan sistem single sign-on (SSO) dimana civitas akan menggunakan 1 akun yakni akun integra sebagai pintu ke semua sistem dan layanan TIK yang ada di ITS. Termasuk diantara layanan TIK tersebut adalah layanan internet, yang dapat diakses dengan akun integra. Untuk akses internet dengan akun integra ini, tidak memerlukan proxy.

Namun demikian, civitas akademika masih tetap dapat menggunakan internet dengan proxy. **Bagaimana cara men-setting Proxy?**

Bagaimana langkah untuk dapat mengakses internet?

Pastikan Anda terhubung dengan jaringan kampus

Akses Internet @ ITS

Akses Internet @ ITS

Anda akan diredirect ke halaman ini. Pilih "Lanjutkan"

Lanjutkan Logout

Gambar F.40 Panduan Konfigurasi Proxy di Website DPTSI-ITS

## Cara Setting Proxy (Enabled dan Disabled) di Chrome, Mozilla Firefox, IE

05/10/2016 ARTIKEL TIK No comments

Bagi dosen, karyawan dan mahasiswa yang ingin mengakses internet dengan menggunakan proxy, maka harus melakukan setting proxy di browsernya. Nah, bagaimana caranya set up proxy di browser? Berikut adalah langkah-langkah untuk mengaktifkan dan me-nonaktifkan setting proxy di tiga browser yakni Chrome, Mozilla, Firefox.

### Setting Proxy di Chrome

Langkah-langkah untuk setting proxy (Enable dan Disable) di Chrome sebagai berikut:

Gambar F.41 Panduan Konfigurasi Proxy di Website DPTSI-ITS (lanj.)

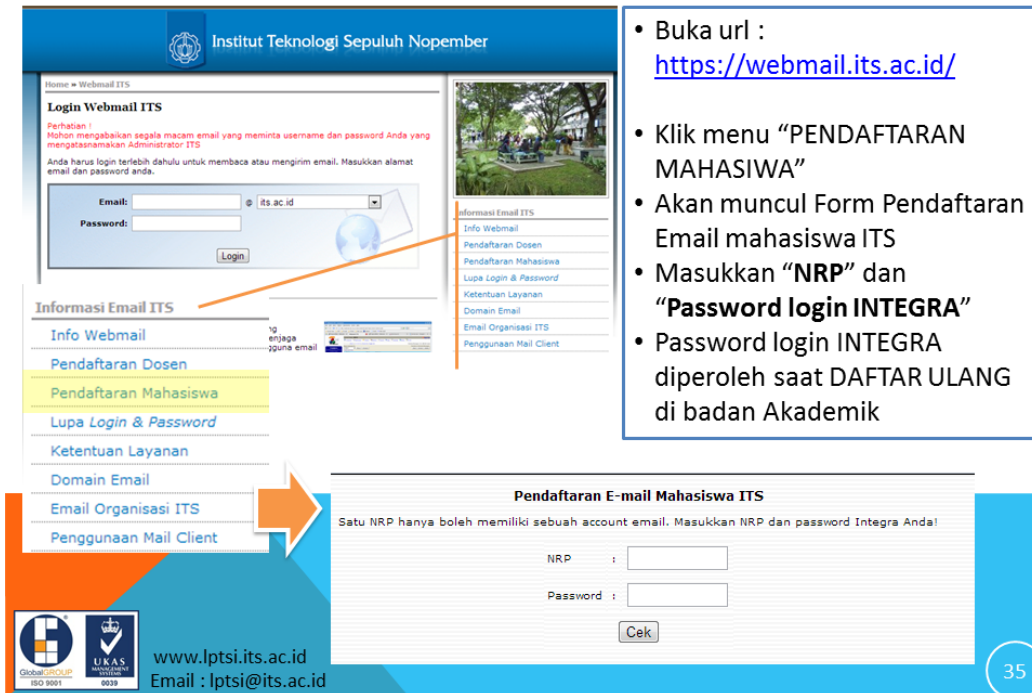
```

10.199.13.48 - PuTTY
login as: rizki
rizki@10.199.13.48's password:

```

Gambar F.42 Login ke Server Menggunakan Putty

## Langkah I :Masuk ke halaman Pendaftaran



• Buka url :  
<https://webmail.its.ac.id/>

• Klik menu “PENDAFTARAN MAHASIWA”

• Akan muncul Form Pendaftaran Email mahasiswa ITS

• Masukkan “NRP” dan “Password login INTEGRA”

• Password login INTEGRA diperoleh saat DAFTAR ULANG di badan Akademik

**Pendaftaran E-mail Mahasiswa ITS**

Satu NRP hanya boleh memiliki sebuah account email. Masukkan NRP dan password Integra Anda!

NRP :

Password :

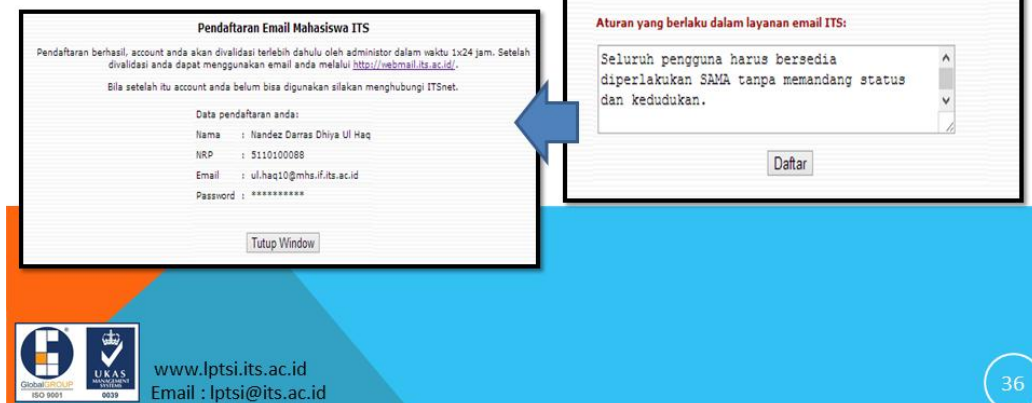
www.lptsi.its.ac.id  
Email : lptsi@its.ac.id

35

Gambar F.43 Pendaftaran Akun *Email* secara Online

## Langkah II : Pemilihan Username dan Pembuatan Password

- Pilih alternatif nama email yang disediakan
- Masukkan password minimal 8 karakter
- Password kombinasi Huruf dan Angka
- Jangan gunakan kombinasi tanggal lahir
- Kemudian klik DAFTAR dan jika berhasil akan tampil halaman validasi dan sukses



**Pendaftaran E-mail Mahasiswa ITS**

NRP : 5110100088

Nama : Nandez Darras Dhiya Ul Haq

Username :  10@mhs.if.its.ac.id

Password :

Password (lagi) :

**Aturan yang berlaku dalam layanan email ITS:**

Seluruh pengguna harus bersedia diperlakukan SAMA tanpa memandang status dan kedudukan.

**Pendaftaran Email Mahasiswa ITS**

Pendaftaran berhasil, account anda akan divalidasi terlebih dahulu oleh administrator dalam waktu 1x24 jam. Setelah divalidasi anda dapat menggunakan email anda melalui <https://webmail.its.ac.id/>.

Bila setelah itu account anda belum bisa digunakan silakan menghubungi ITSnet.

Data pendaftaran anda:

Nama : Nandez Darras Dhiya Ul Haq

NRP : 5110100088

Email : ul.haq10@mhs.if.its.ac.id

Password : \*\*\*\*\*

www.lptsi.its.ac.id  
Email : lptsi@its.ac.id

36

Gambar F.44 Pendaftaran Akun *Email* secara Online (lanj.)

|                                                                                   |                                 |                                 |
|-----------------------------------------------------------------------------------|---------------------------------|---------------------------------|
|  | POB-TSI.YAN-04                  | Revisi : 01                     |
|                                                                                   | PROSEDUR OPERASIONAL BAKU (POB) | Tanggal terbit : 2 Oktober 2014 |
|                                                                                   | LAYANAN E-MAIL: PEMBUATAN AKUN  | Halaman : 2 dari 14             |

#### 1. Tujuan

Membuat akun *email* yang diminta oleh pengguna layanan (*user*) LPTSI.

#### 2. Ruang Lingkup

Mengatur proses pembuatan *email* ITS yang diminta oleh pengguna layanan (*user*) LPTSI, yaitu:

- Tenaga pendidik (Dosen ITS).
- Tenaga kependidikan (Karyawan ITS).
- Pejabat di lingkungan ITS.
- Unit kerja yang terdapat di lingkungan ITS.
- Mahasiswa ITS.

#### 3. Definisi

- *Email* ITS merupakan akun surat elektronik yang disediakan oleh LPTSI yang dapat digunakan oleh pihak-pihak tertentu di lingkungan ITS. Selain sebagai sarana komunikasi, *email* tersebut juga digunakan untuk proses *autentifikasi* penggunaan fasilitas IT seperti Wi-Fi dan internet.
- Tenaga pendidik ialah PNS kementerian di bidang pendidikan nasional yang ditempatkan di ITS, dan non PNS yang diangkat Rektor sesuai dengan peraturan perundang-undangan.
- Tenaga kependidikan ialah mereka yang bekerja di ITS baik yang berstatus PNS maupun non PNS
- Pejabat adalah para pemegang jabatan struktural di ITS.
- Unit kerja merupakan unsur pelaksana administrasi, pelaksana akademik, pengembang dan pelaksana tugas strategis, dan unsur penunjang yang berada di ITS.
- Mahasiswa adalah mereka yang terdaftar sebagai peserta didik pendidikan akademik, vokasi, dan profesi di ITS.

#### 4. Dokumen Terkait

- Manual cara pendaftaran.
- Standardisasi penamaan *email*.
- Ketentuan layanan pembuatan *email*.
- Ketentuan penggunaan *email*.
- Surat permohonan pembuatan *email* ITS.

#### 5. Rincian Prosedur

- Melalui **website** ([webmail.its.ac.id](http://webmail.its.ac.id) atau [gmail.its.ac.id](http://gmail.its.ac.id)), khusus untuk Mahasiswa dan Tenaga Pendidik:

| NO | ENTITAS        | AKTIVITAS                                                                                                                                                                             |
|----|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | User           | - Mengentrikan NRP/NIP dan <i>password</i> Integra.<br>- Memilih alamat <i>email</i> dan memasukkan <i>password</i> yang diinginkan.<br>- Menunggu validasi, maksimal 1x24 jam kerja. |
| 2. | Operator LPTSI | Melakukan validasi.                                                                                                                                                                   |
| 3. | User           | - <i>Login</i> ke <i>webmail</i> . Jika gagal, <i>user</i> diarahkan untuk mengikuti prosedur <i>reset password</i> atau <i>manual reset password email</i> ITS.                      |

Gambar F.45 Prosedur Layanan *Email*: Pembuatan Akun

|                                                                                     |                                 |                                 |
|-------------------------------------------------------------------------------------|---------------------------------|---------------------------------|
|  | POB-TSI.YAN-04                  | Revisi : 01                     |
|                                                                                     | PROSEDUR OPERASIONAL BAKU (POB) | Tanggal terbit : 2 Oktober 2014 |
|                                                                                     | LAYANAN E-MAIL: PEMBUATAN AKUN  | Halaman : 3 dari 14             |

- Melalui surat resmi, khusus untuk Pejabat dan Unit yang ada di lingkungan ITS.

| NO | ENTITAS        | AKTIVITAS                                                                                                                                                                                                                                                                                                                                     |
|----|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | User           | - Membuat dan mengirimkan surat resmi ke <i>Office</i> LPTSI dengan menyebutkan nama, NIP, jabatan, alamat <i>email</i> yang diminta, dan <i>password</i> sementara.<br>- Selain terdapat tanda tangan <i>user</i> , surat resmi harus disetujui oleh Pejabat Struktural terdekat.<br>- Menunggu proses pendaftaran, maksimal 1x24 jam kerja. |
| 2. | Operator LPTSI | - Melakukan validasi data <i>user</i> .<br>- Membuat akun <i>email</i> berdasarkan permintaan <i>user</i> , dengan memasukkan data nama, NIP, jabatan, alamat <i>email</i> yang diminta, dan <i>password</i> sementara.                                                                                                                       |
| 3. | User           | - <i>Login</i> ke <i>webmail</i> . Jika gagal, <i>user</i> diarahkan untuk mengikuti prosedur <i>reset password</i> atau <i>manual reset password email</i> ITS.                                                                                                                                                                              |

- Bagi Tenaga Kependidikan:

| NO | ENTITAS        | AKTIVITAS                                                                                                                                                                                                |
|----|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | User           | - Menghubungi <i>Office</i> LPTSI dengan menyebutkan nama, NIP, alamat e-mail yang diminta, dan <i>password</i> sementara.<br>- Menunggu proses pendaftaran, maksimal 1x24 jam kerja.                    |
| 2. | Operator LPTSI | - Melakukan validasi data <i>user</i> .<br>- Membuat akun <i>email</i> berdasarkan permintaan <i>user</i> , dengan memasukkan data nama, NIP, alamat e-mail yang diminta, dan <i>password</i> sementara. |
| 3. | User           | - <i>Login</i> ke <i>webmail</i> . Jika gagal, <i>user</i> diarahkan untuk mengikuti prosedur <i>reset password</i> atau <i>manual reset password email</i> ITS.                                         |

#### 6. Diagram Alir

Terlampir

#### 7. Record/Catatan Mutu

*Form* pelayanan pembuatan *email*.

#### 8. Indikator Keberhasilan

Waktu tunggu pembuatan *email*.

#### 9. Perubahan Dokumen

Belum ada.

Gambar F.46 Prosedur Layanan *Email*: Pembuatan Akun (lanj.)



|                                 |                                 |
|---------------------------------|---------------------------------|
| POP-TSI.YAN-04                  | Revisi : 01                     |
| PROSEDUR OPERASIONAL BAKU (POB) | Tanggal terbit : 2 Oktober 2014 |
| LAYANAN EMAIL: PENGHAPUSAN AKUN | Halaman : 12 dari 14            |

#### 1. Tujuan

Menghapus akun *email* yang tidak diperlukan lagi oleh pengguna layanan (*user*) LPTSI.

#### 2. Ruang Lingkup

Mengatur proses penghapusan akun E-mail ITS yang tidak diperlukan lagi oleh pengguna layanan (*user*) LPTSI.

#### 3. Definisi

- *Email* ITS merupakan akun surat elektronik yang disediakan oleh LPTSI yang dapat digunakan oleh pihak-pihak tertentu di lingkungan ITS. Selain sebagai sarana komunikasi, *email* ini juga digunakan untuk proses autentikasi penggunaan fasilitas IT seperti Wi-Fi dan internet.
- Tenaga pendidik PNS kementerian di bidang pendidikan nasional yang ditempatkan di ITS, dan non PNS yang diangkat Rektor sesuai dengan peraturan perundang-undangan.
- Tenaga kependidikan ialah mereka yang bekerja di ITS baik yang berstatus PNS maupun non PNS.
- Pejabat adalah para pemegang jabatan struktural di ITS.
- Unit kerja merupakan unsur pelaksana administrasi, pelaksana akademik, pengembang dan pelaksana tugas strategis, dan unsur penunjang yang berada di ITS.
- Mahasiswa adalah mereka terdaftar sebagai peserta didik pendidikan akademik, vokasi, dan profesi yang belajar di ITS.
- Alumni adalah mahasiswa yang telah lulus dari pendidikan akademik, vokasi, maupun profesi di ITS.

#### 4. Dokumen Terkait

- Surat permohonan penghapusan akun email.

#### 5. Rincian Prosedur

| NO | ENTITAS        | AKTIVITAS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | User           | <ul style="list-style-type: none"> <li>- Membuat dan mengirimkan surat resmi ke Office LPTSI dengan menyebutkan nama, NIP, jabatan, alamat, dan <i>password email</i> yang akan dihapus, serta rentang waktu migrasi.</li> <li>- Selain terdapat tanda tangan <i>user</i>, surat resmi harus disetujui oleh Pejabat Struktural terdekat.</li> <li>- Menunggu proses penghapusan, maksimal 1x24 jam kerja.</li> <li>- Menerima pemberitahuan tanggal terhapusnya akun <i>email</i> untuk melakukan migrasi data dari <i>email</i> yang akan dihapus (jika perlu).</li> </ul> |
| 2. | Operator LPTSI | <ul style="list-style-type: none"> <li>- Mencari akun <i>email user</i> pada database.</li> <li>- Melakukan validasi data <i>user</i>.</li> <li>- Menghapus akun <i>email</i> yang diminta <i>user</i> setelah rentang waktu yang diminta <i>user</i> migrasi habis.</li> </ul>                                                                                                                                                                                                                                                                                             |

#### 6. Diagram Alir

Terlampir.

Gambar F.47 Prosedur Layanan *Email*: Penghapusan Akun



|                                 |                                 |
|---------------------------------|---------------------------------|
| POB-TSI.YAN.04                  | Revisi : 01                     |
| PROSEDUR OPERASIONAL BAKU (POB) | Tanggal terbit : 2 Oktober 2014 |
| LAYANAN E-MAIL: RESET PASSWORD  | Halaman : 7 dari 14             |

#### 1. Tujuan

Untuk mengatur ulang *password* akun *email* ITS yang diminta pengguna layanan (*user*).

#### 2. Ruang Lingkup

Mengatur proses atur ulang (*reset*) *password* akun *email* ITS yang dilakukan secara langsung, yakni tanpa melalui sistem yang terdapat pada Portal Mail ITS (webmail.its.ac.id dan gmail.its.ac.id).

#### 3. Definisi

- *Email* ITS merupakan akun surat elektronik yang disediakan oleh LPTSI yang dapat digunakan oleh pihak-pihak tertentu di lingkungan ITS. Selain sebagai sarana komunikasi, e-mail ini juga digunakan untuk proses autentikasi penggunaan fasilitas IT seperti Wi-Fi dan internet.
- Tenaga pendidik ialah PNS kementerian di bidang pendidikan nasional yang ditempatkan di ITS, dan non PNS yang diangkat Rektor sesuai dengan peraturan perundang-undangan.
- Tenaga kependidikan ialah mereka yang bekerja di ITS baik yang berstatus PNS maupun non PNS.
- Pejabat adalah para pemegang jabatan struktural di ITS.
- Unit kerja merupakan unsur pelaksana administrasi, pelaksana akademik, pengembang dan pelaksana tugas strategis, dan unsur penunjang yang berada di ITS.
- Mahasiswa adalah mereka terdaftar sebagai peserta didik pendidikan akademik, vokasi, dan profesi yang belajar di ITS.

#### 4. Dokumen Terkait

- Manual *reset password* akun e-mail ITS melalui sistem.
- Manual operasi *email* ITS.
- Surat permohonan *reset password email* ITS.

#### 5. Rincian Prosedur

- Bagi Mahasiswa, Tenaga Pendidik, dan Tenaga Kependidikan:

| NO | ENTITAS        | AKTIVITAS                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | User           | <ul style="list-style-type: none"> <li>- Menghubungi Office LPTSI untuk me-reset <i>password</i>, dengan menyertakan nama, NRP/NIP, dan alamat <i>email</i>, serta tanggal lahir <i>user</i>.</li> </ul>                                                                                                                                                                                                                                                     |
| 2. | Operator LPTSI | <ul style="list-style-type: none"> <li>- Mencari akun <i>email user</i> pada database.</li> <li>- Melakukan validasi data <i>user</i> (NIP/NRP dan tanggal lahir).</li> <li>- Me-reset <i>password</i> akun <i>email user</i>.</li> <li>- Memberikan <i>password</i> sementara kepada <i>user</i>.</li> <li>- Menyarankan <i>user</i> menggunakan fasilitas sistem <i>reset password</i> yang telah ada pada portal Mail ITS (webmail.its.ac.id).</li> </ul> |
| 3. | User           | <ul style="list-style-type: none"> <li>- Login ke webmail. Jika gagal, <i>user</i> diarahkan untuk mengikuti prosedur <i>reset password</i> atau manual <i>reset password email</i> ITS.</li> </ul>                                                                                                                                                                                                                                                          |

Gambar F.48 Prosedur Layanan *E-Mail*: Reset Password



|                                       |                                 |
|---------------------------------------|---------------------------------|
| POB-TSI.YAN.04                        | Revisi : 01                     |
| PROSEDUR OPERASIONAL BAKU (POB)       | Tanggal terbit : 2 Oktober 2014 |
| LAYANAN E-MAIL: <i>RESET PASSWORD</i> | Halaman : 8 dari 14             |

— Bagi Pejabat dan Unit:

| NO | ENTITAS        | AKTIVITAS                                                                                                                                                                                                                                                                                                                                                               |
|----|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | <i>User</i>    | <ul style="list-style-type: none"><li>- Membuat dan mengirimkan surat resmi ke <i>Office</i> LPTSI dengan menyebutkan nama, NIP, jabatan, alamat e-mail, dan <i>password</i> baru.</li><li>- Selain terdapat tanda tangan <i>user</i>, surat resmi harus disetujui oleh Pejabat Struktural terdekat</li><li>- Menunggu proses reset, maksimal 1x24 jam kerja.</li></ul> |
| 2. | Operator LPTSI | <ul style="list-style-type: none"><li>- Mencari akun <i>email user</i> pada database</li><li>- Melakukan validasi data <i>user</i></li><li>- Me-reset <i>password</i> akun e-mail <i>user</i> dengan yang baru.</li></ul>                                                                                                                                               |
| 3. | <i>User</i>    | <ul style="list-style-type: none"><li>- Login ke webmail. Jika gagal, <i>user</i> diarahkan untuk mengikuti prosedur <i>reset password</i> atau <i>manual reset password email ITS</i>.</li></ul>                                                                                                                                                                       |

**6. Diagram Alir**

Terlampir.

**7. Record/Catatan Mutu**

Formulir waktu pelayanan.

**8. Indikator Keberhasilan**

Waktu tunggu untuk me-reset *password*.

**9. Perubahan Dokumen**

Belum ada.

Gambar F.49 Prosedur Layanan *Email: Reset Password* (lanj.)



## Login Webmail ITS

### Perhatian !

Mohon mengabaikan segala macam email yang meminta username dan password Anda yang mengatasnamakan Administrator ITS

Anda harus login terlebih dahulu untuk membaca atau mengirim email. Masukkan alamat email dan password anda.

|           |                          |   |           |                                      |
|-----------|--------------------------|---|-----------|--------------------------------------|
| Email:    | <input type="text"/>     | @ | its.ac.id | <input type="button" value="Login"/> |
| Password: | <input type="password"/> |   |           |                                      |

## Lupa Password

Masukkan alamat email anda pada form di bawah ini. Bila anda telah mengisi daftar pertanyaan yang harus anda jawab, pertanyaan tersebut akan muncul di bawah. Jawablah seluruh pertanyaan tersebut dengan tepat untuk me-reset password anda.

Alamat email:

## Khusus Mahasiswa Aktif

Jika anda lupa login dan password e-mail gunakan fasilitas di bawah ini:

NRP   
Password Integra

Gambar F.50 Reset Password secara Online



Sistem Informasi Terintegrasi

Jika mengalami kesulitan login silakan hubungi TU jurusan atau email ke [sim@its.ac.id](mailto:sim@its.ac.id)

Selasa, 25 April 2017

|                                      |                          |
|--------------------------------------|--------------------------|
| Username                             | <input type="text"/>     |
| Password                             | <input type="password"/> |
| <input type="button" value="Login"/> |                          |

[Lupa password?](#)

### Jangan lupa mengubah password

Untuk menjaga keamanan data anda, ubah password anda secara berkala. Gunakan password minimal 8 karakter yang terdiri dari huruf kapital, huruf kecil, dan bilangan. Lebih baik jangan menggunakan tanggal lahir atau hal-hal umum lainnya sebagai password.

### Tampilan terbaik menggunakan Mozilla Firefox

Gambar F.51 Saran Penggunaan Password yang Aman di Integra ITS



### Informasi Email ITS

[Info Webmail](#)

[Pendaftaran Mahasiswa](#)

[Lupa Login & Password](#)

[Ketentuan Layanan](#)

[Domain Email](#)

[Penggunaan Mail Client](#)

### Layanan Lain

[Web ITS](#)

[Web LPTSI](#)

[Portal Google Apps P](#)

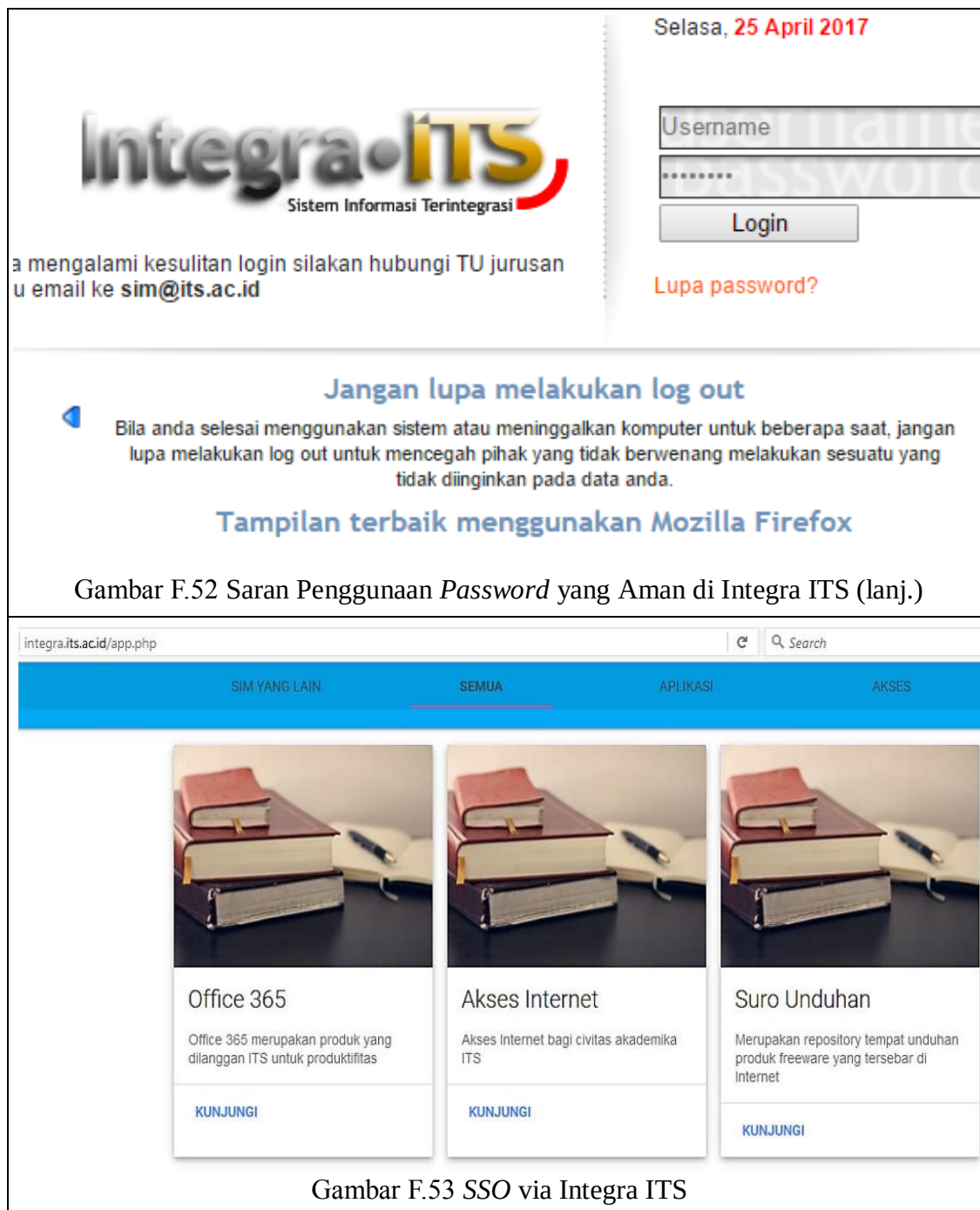
[Portal Software Lisensi](#)

[Portal Software GPL I](#)

[Mirror ITS](#)

[Direktori ITS](#)





# Akses Internet @ ITS

Akses internet ini akan tercatat atas nama pengguna  
9114205324  
FURQON MAULADANI  
9114205324-FURQONMAULADANI

Keterangan  
Diakses dari 10.199.6.68  
Waktu akses : 28-04-2017 07:58:57

Lanjutkan

Logout

Gambar F.54 SSO via Integra ITS untuk Sukses *Login*

## ITS-Net Administration Center

Administration center for ITS-Net Network Provider

Enter your username and password below

| Operator Login                       |          |
|--------------------------------------|----------|
| Username                             | admin    |
| Password                             | ●●●●●●●● |
| <input type="button" value="Login"/> |          |

.. Copyright©2003-ITS-Net Crew ..

Gambar F.55 Halaman *Login Administrator* Webmail ITS

Operator : **sofi sofi**

[ [Jml users](#) ] - [ [Option](#) ] - [ [Help](#) ] - [ [SignOut](#) ]

Last login : Thursday, 27 Apr 2017 | 03:05:46

### Control Panel

[ [User List](#) ] - [ [Block List](#) ] - [ [Alias List](#) ] - [ [Add User](#) ]

Paging

20 ▼

Go

goto page :

Go

|< <

Page 1/11

> >|

### Search Tool

Category :

Login ▼

Search string :

Search

| No. | NRP        | Nama                                | Login                                | Quota |
|-----|------------|-------------------------------------|--------------------------------------|-------|
| 1.  | 2202100060 | <a href="#">Muhammad Abdillah</a>   | abdillah@elect-eng.its.ac.id         | 200 M |
| 2.  | 2211105053 | <a href="#">Abdul Halim</a>         | abdul.halim11@mhs.ee.its.ac.id       | 20 M  |
| 3.  | 5108100180 | <a href="#">Muhammad Iqbal A</a>    | abdullah@cs.its.ac.id                | 200 M |
| 4.  | 0          | <a href="#">Annisa Rahmawati</a>    | acha86@its.ac.id                     | 200 M |
| 5.  | 910004001  | <a href="#">Achmad Ustadziwasis</a> | achmad_u@its.ac.id                   | 200 M |
| 6.  | 3312201018 | <a href="#">Adam Rus Nugroho</a>    | adam12@mhs.enviro.its.ac.id          | 20 M  |
| 7.  | 2213201003 | <a href="#">Mei Adetya Praja</a>    | adetya13@mhs.ee.its.ac.id            | 20 M  |
| 8.  | 3308100115 | <a href="#">Adi Trisnawati</a>      | adhie@enviro.its.ac.id               | 200 M |
| 9.  | 2209100112 | <a href="#">Adib Nur Ikhwan</a>     | adib09@mhs.ee.its.ac.id              | 20 M  |
| 10. | 3512100076 | <a href="#">Bekti Wahyu Aditya</a>  | aditya.wahyu12@mhs.geodesy.its.ac.id | 20 M  |

Record 1 - 10 from 216

Paging

20 ▼

Go

goto page :

Go

|< <

Page 1/11

> >|

Gambar F.56 Halaman Daftar Pengguna Webmail ITS

Operator : **sofi sofi** [ [Jml users](#) ] - [ [Option](#) ] - [ [Help](#) ] - [ [SignOut](#) ]  
 Last login : Thursday, 27 Apr 2017 | 03:02:24

**Control Panel** [ [User List](#) ] - [ [Block List](#) ] - [ [Alias List](#) ] - [ [Add User](#) ]

Paging   goto page :   |< < Page 1/62336 > >|

**Search Tool** Category :  Search string :

| No. | NRP        | Nama             | Login                                      | Domain            |
|-----|------------|------------------|--------------------------------------------|-------------------|
| 1.  | 9114205324 | Furqon Mauladani | <a href="#">furqon14@mhs.mmt.its.ac.id</a> | mhs.mmt.its.ac.id |

Found 1 record from 1

Paging   goto page :   |< < Page 1/62336 > >|

.. Copyright©2003-2015 PusNet Crew ..

Gambar F.57 Halaman Pencarian Pengguna Webmail ITS

Operator : **sofi sofi** [ [Jml users](#) ] - [ [Option](#) ] - [ [Help](#) ] - [ [SignOut](#) ]  
 Last login : Thursday, 27 Apr 2017 | 03:03:36

**Control Panel** [ [User List](#) ] - [ [Block List](#) ] - [ [Alias List](#) ] - [ [Add User](#) ]

**Search Tool** Category :  Search string :

**User : Furqon Mauladani**

|                 |                                              |
|-----------------|----------------------------------------------|
| Username        | : <a href="#">furqon14@mhs.mmt.its.ac.id</a> |
| Domain          | : mhs.mmt.its.ac.id                          |
| Nama            | : Furqon Mauladani                           |
| Quota           | : 20971520                                   |
| Tgl Pendaftaran | : 2014-10-01 19:38:10                        |
| NRP/NIP         | : 9114205324                                 |
| Alamat          | :                                            |
| No. Telepon     | :                                            |
| Jenis Pengguna  | : Mahasiswa                                  |
| Lokasi Mailbox  | : Non ITS                                    |
| Akun Aktif      | : Aktif                                      |

.. Copyright©2003-2015 PusNet Crew ..

Gambar F.58 Halaman Lihat Pengguna Webmail ITS

Operator : **sofi sofi** [ [Jml users](#) ] - [ [Option](#) ] - [ [Help](#) ] - [ [SignOut](#) ]  
 Last login : Thursday, 27 Apr 2017 | 03:06:45

**Control Panel** [ [User List](#) ] - [ [Block List](#) ] - [ [Alias List](#) ] - [ [Add User](#) ]

**Search Tool** Category : **Login** Search string :

**User :**

|                |   |                                                                                                                                                         |                                                |
|----------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
| Password       | : | <input type="text"/>                                                                                                                                    | <input type="button" value="Change Password"/> |
| Username       | : | furqon14@mhs.mmt.its.ac.id                                                                                                                              |                                                |
| Domain         | : | mhs.mmt.its.ac.id                                                                                                                                       |                                                |
| Quota          | : | 20 MB <input type="checkbox"/> Unlimited                                                                                                                |                                                |
| Nama           | : | <input type="text" value="Furqon Mauladani"/>                                                                                                           |                                                |
| NRP/NIP        | : | <input type="text" value="9114205324"/>                                                                                                                 |                                                |
| Alamat         | : | <input type="text"/>                                                                                                                                    |                                                |
| No. Telepon    | : | <input type="text"/>                                                                                                                                    |                                                |
| Akun Aktif     | : | Aktif <input type="button" value="v"/>                                                                                                                  |                                                |
| Jenis Pengguna | : | Mahasiswa <input type="button" value="v"/>                                                                                                              |                                                |
| Lokasi Mailbox | : | <input type="button" value="Google"/> <input type="button" value="ITS"/> <input type="button" value="Google"/> <input type="button" value="Office365"/> |                                                |

.. Copyright©2003-2015 PusNet Crew ..

Gambar F.59 Halaman Rubah Data Pengguna Webmail ITS

Operator : **sofi sofi** [ [Jml users](#) ] - [ [Option](#) ] - [ [Help](#) ] - [ [SignOut](#) ]  
 Last login : Thursday, 27 Apr 2017 | 03:05:13

**Control Panel** [ [User List](#) ] - [ [Block List](#) ] - [ [Alias List](#) ] - [ [Add User](#) ]

**Search Tool** Category : **Login** Search string :

**Add New User**

|                  |   |                                               |
|------------------|---|-----------------------------------------------|
| Username         | : | <input type="text"/>                          |
| Password         | : | <input type="text"/>                          |
| NRP/NIP          | : | <input type="text"/>                          |
| Grup             | : | Karyawan <input type="button" value="v"/>     |
| Domain           | : | al.its.ac.id <input type="button" value="v"/> |
| Quota            | : | 50 MB <input type="checkbox"/> Unlimited      |
| Nama             | : | <input type="text"/>                          |
| Alamat           | : | <input type="text"/>                          |
| Tanggal Berakhir | : | <input type="text"/>                          |
| No. Telepon      | : | <input type="text"/>                          |

.. Copyright©2003-2015 PusNet Crew ..

Gambar F.60 Halaman Pendaftaran Pengguna Webmail ITS Baru



### ERROR

Unknown user or password incorrect.

[Go to the login page](#)

Gambar F.61 Notifikasi *Login* Gagal Layanan *Email* Mandiri

## Institut Teknologi Sepuluh Nopember

Sign in with your organizational account

Incorrect user ID or password. Type the correct user ID and password, and try again.

furqon14@mhs.mmt.its.ac.id

.....

Sign in

Gambar F.62 Notifikasi *Login* Gagal Layanan *Email* Microsoft

**Error**  
You could not be logged in! Either the username and password do not match or you have not validated your membership!  
[\[Please try again\]](#)

Gambar F.63 Notifikasi *Login* Gagal *Administrator* Webmail ITS

Compose Addresses Folders Options Search Help Calendar Notes To Do

**Lupa Sandi** - [redacted]

Anda harus memasukkan data berupa pasangan pertanyaan dan jawaban. Anda akan diminta untuk menjawab pertanyaan yang anda masukkan apabila anda menggunakan fasilitas "Lupa Password".

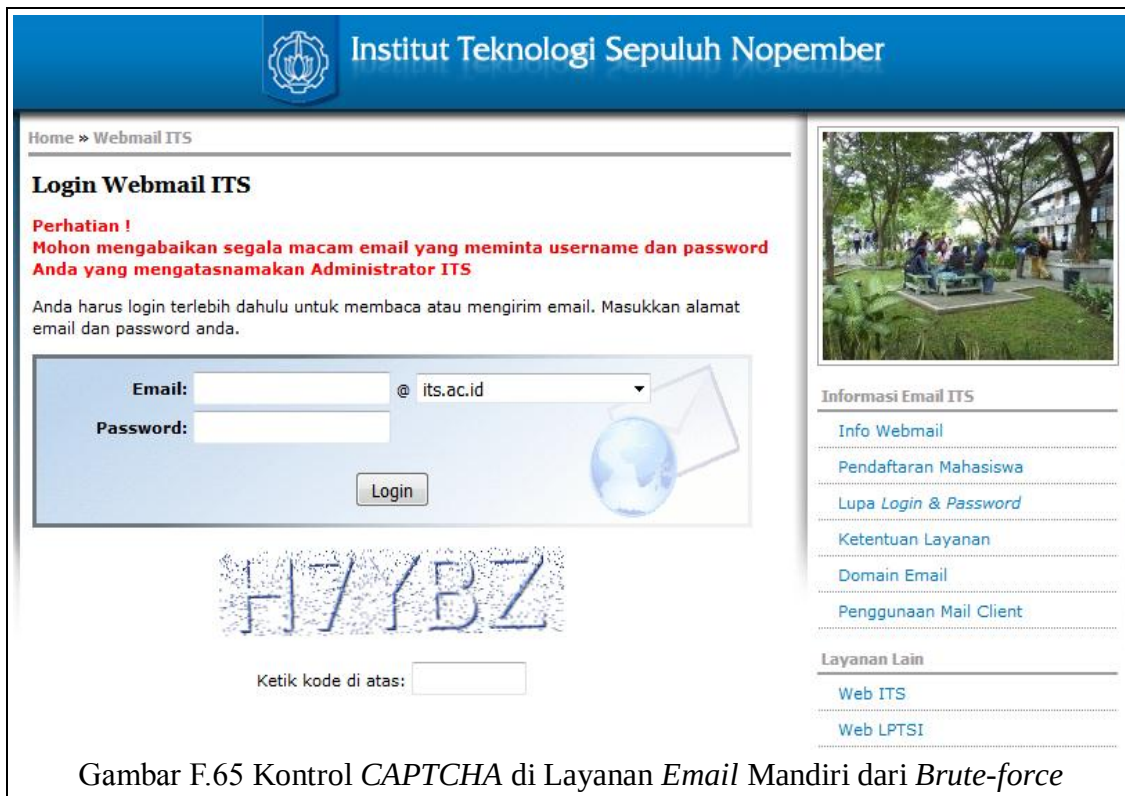
Ingat, **SEMUA ORANG** dapat membaca pertanyaan yang anda masukkan di sini. Pastikan bahwa **HANYA ANDA SAJA** yang mengetahui jawabannya. Siapa pun yang dapat menjawab pertanyaan yang anda masukkan dapat mengganti kata sandi email anda.

Daftar pertanyaan telah tersimpan

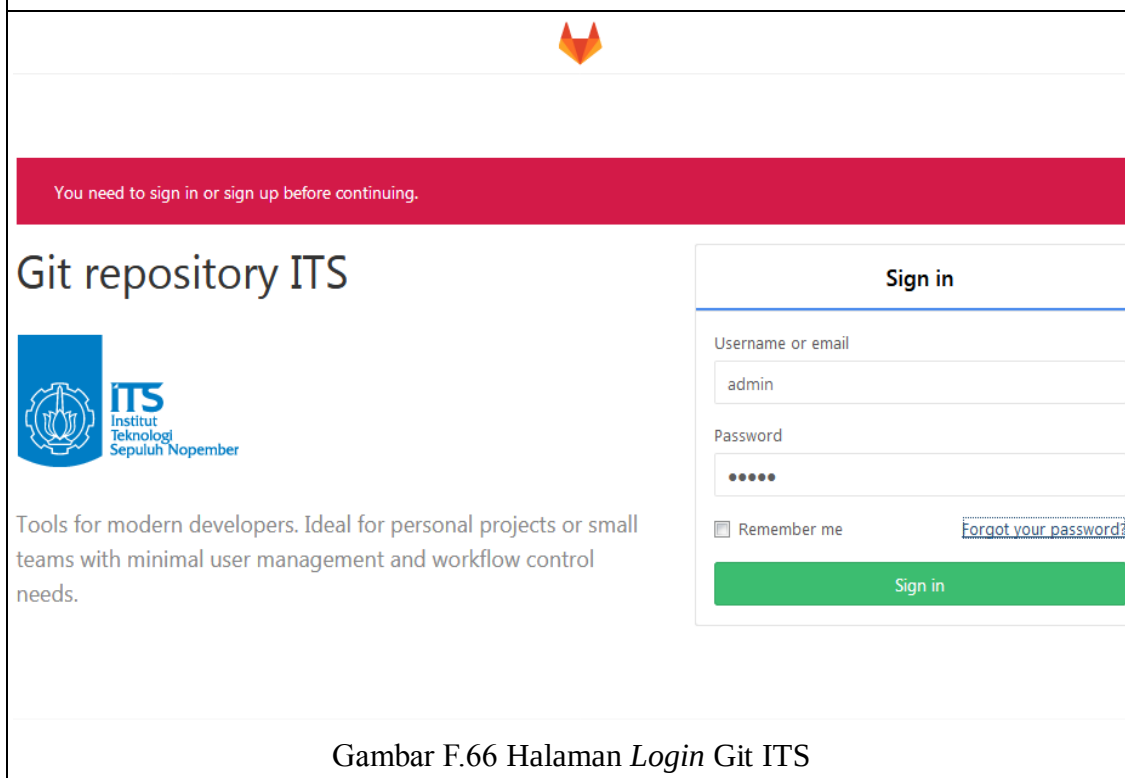
| No | Pertanyaan       | Jawaban |
|----|------------------|---------|
| 1  | satu tambah satu | dua     |
| 2  | tiga tambah tiga | ya enam |
| 3  |                  |         |
| 4  |                  |         |
| 5  |                  |         |
| 6  |                  |         |

Simpan

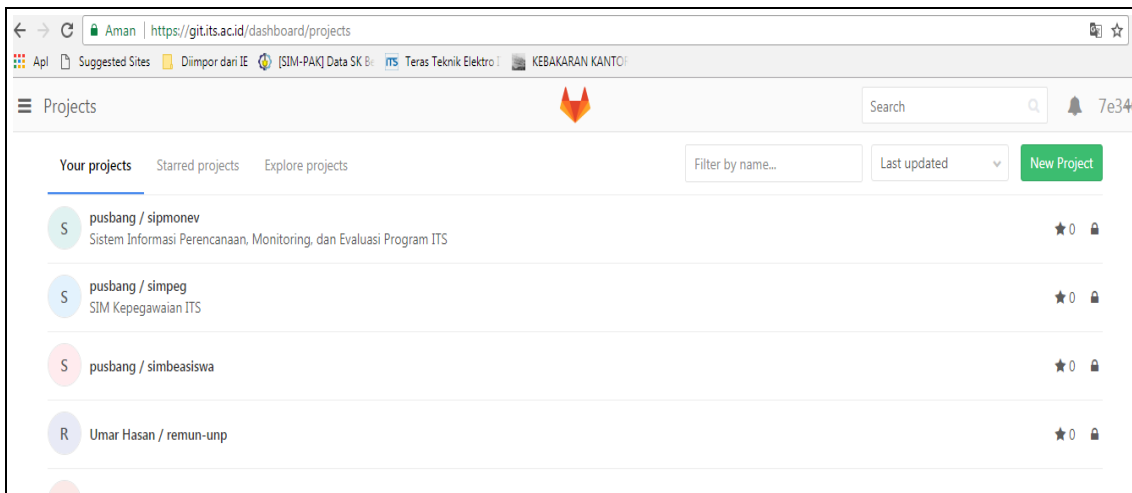
Gambar F.64 Pengisian Bantuan *Lupa Password* di Layanan *Email* Mandiri



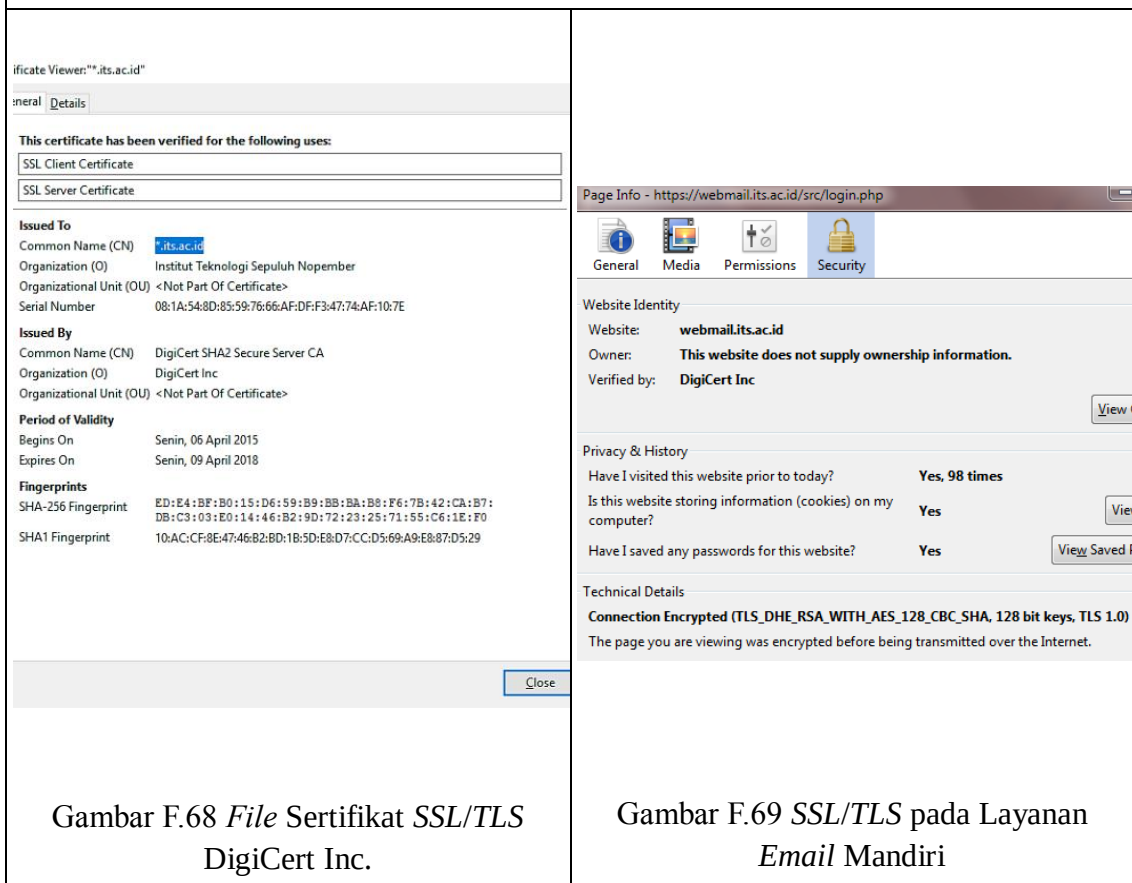
Gambar F.65 Kontrol *CAPTCHA* di Layanan *Email* Mandiri dari *Brute-force*



Gambar F.66 Halaman *Login* Git ITS



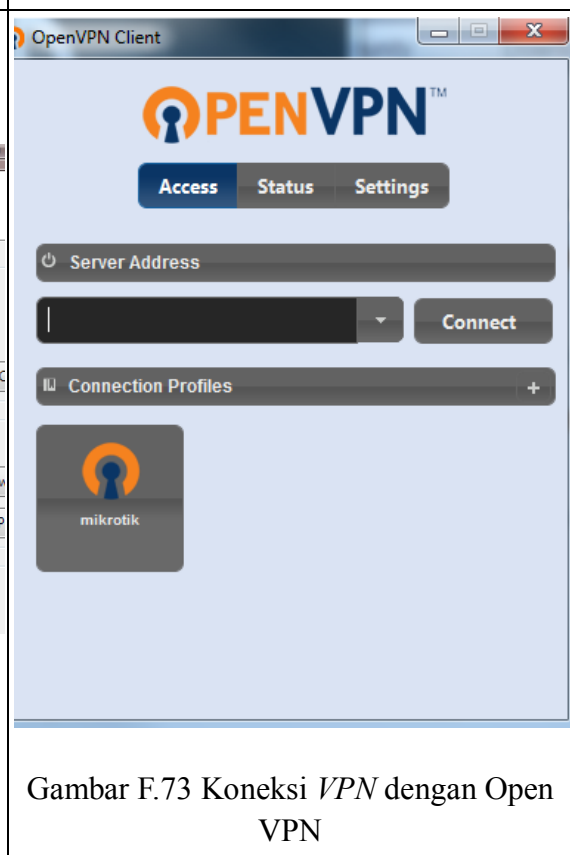
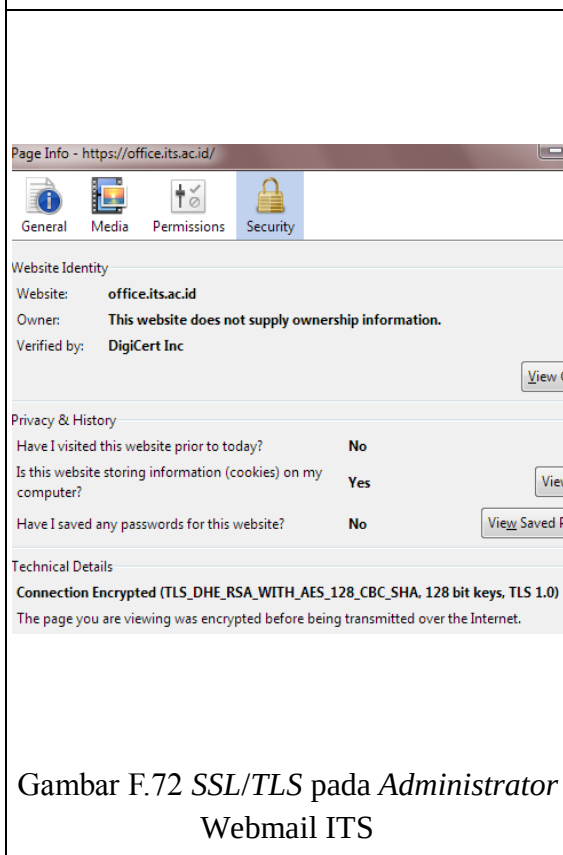
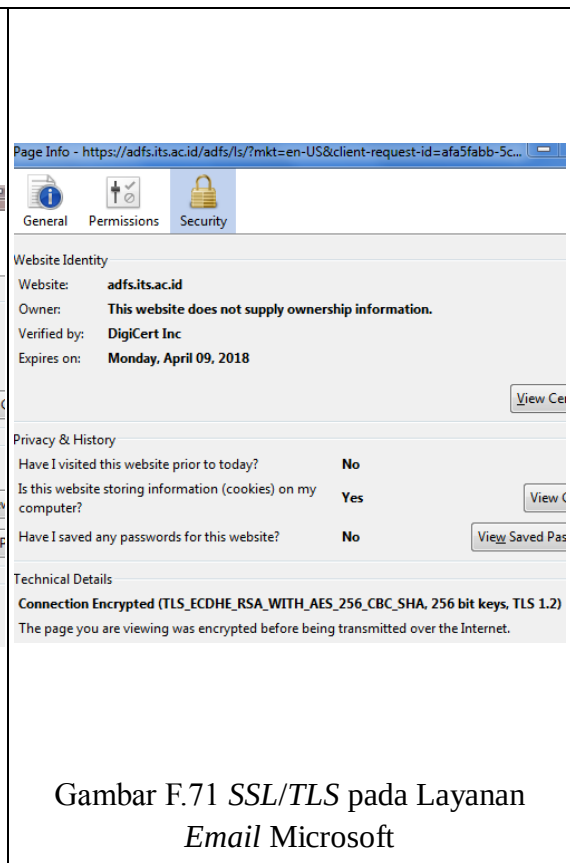
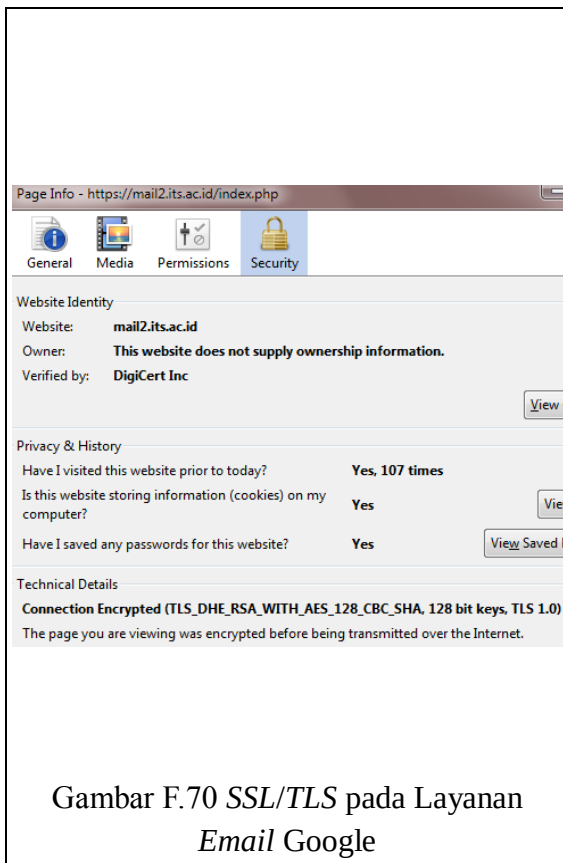
Gambar F.67 Halaman Awal Git ITS



Gambar F.68 File Sertifikat SSL/TLS  
DigiCert Inc.

Gambar F.69 SSL/TLS pada Layanan  
Email Mandiri





| postfix.mailbox: 61.775 rows total, 36.715 rows match to filter                                                                                                                                                                                                                                                                                                                                                |                                        |                               |                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-------------------------------|------------------------------------------------------|
| Recent filters: 'username' LIKE '%mhs%' OR 'password' LIKE '%mhs%' OR 'name' LIKE '%mhs%' OR 'maildir' LIKE '%mhs%'...                                                                                                                                                                                                                                                                                         |                                        |                               |                                                      |
| 'username' LIKE '%mhs%' OR 'password' LIKE '%mhs%' OR 'name' LIKE '%mhs%' OR 'maildir' LIKE '%mhs%' OR 'quota' LIKE '%mhs%' OR 'domain' LIKE '%mhs%' OR 'created' LIKE '%mhs%' OR 'modified' LIKE '%mhs%' OR 'expired' LIKE '%mhs%' OR 'active' LIKE '%mhs%' OR 'mbx' LIKE '%mhs%' OR 'migrated' LIKE '%mhs%' OR 'nnnnn' LIKE '%mhs%' OR 'slasht' LIKE '%mhs%' OR 'teln' LIKE '%mhs%' OR 'grouse' LIKE '%mhs%' |                                        |                               |                                                      |
| username                                                                                                                                                                                                                                                                                                                                                                                                       | password                               | name                          | maildir                                              |
| rausyan.fikri13@mhs.prodes.its.ac.id                                                                                                                                                                                                                                                                                                                                                                           | \$1\$Agl.C/hA\$9PgPH2Y5cd7ndfiaMBzd/   | Rausyan Fikri                 | mhs.prodes.its.ac.id/r/rausyan.fikri13/Maildir/      |
| rahmadini.khoirunnisa16@mhs.ie.its.ac.id                                                                                                                                                                                                                                                                                                                                                                       | \$1\$1jhtzLjO\$4dPIxj/gcXnlOPxCqB7bM1  | Rahmadini Khoirunnisa         | mhs.ie.its.ac.id/r/rahmadini.khoirunnisa16/Maildir/  |
| eko15@mhs.ce.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                         | \$1\$Wp.dO2sG\$OVSBLeypa1FkH2fw0fc31   | Eko Nur Hapsoro               | mhs.ce.its.ac.id/e/eko15/Maildir/                    |
| prayogo15@mhs.chem-eng.its.ac.id                                                                                                                                                                                                                                                                                                                                                                               | \$1\$c/GMmkQf\$0/FohAzWjKto/14IAI0M1   | Prayogo Kuntoro               | mhs.chem-eng.its.ac.id/p/prayogo15/Maildir/          |
| muhammad.luqman.hakim15@mhs.chem-eng.i...                                                                                                                                                                                                                                                                                                                                                                      | \$1\$16bOJAos\$Fv3hDBCNxEB6sGUzbn1JT/  | Muhammad Luqman Hakim         | mhs.chem-eng.its.ac.id/m/muhammad.luqman.hakim15/... |
| freddy16@mhs.ie.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                      | \$1\$zGXNcDy4\$Ptt1e8OP.8VreBCOAW01r/  | Freddy David Chlongola        | mhs.ie.its.ac.id/f/freddy16/Maildir/                 |
| rafif15@mhs.ce.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                       | \$1\$CFZpWbqW\$RkReeyfSkxJ/yNUq10XP/   | Rafif Hayyu Pradana           | mhs.ce.its.ac.id/r/rafif15/Maildir/                  |
| firda15@mhs.ie.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                       | \$1\$PRLXcce1\$PuuJwBR.e.uyiOFgZmswCE. | Firda Nur Rizkiani            | mhs.ie.its.ac.id/f/firda15/Maildir/                  |
| salimah16@mhs.geofisika.its.ac.id                                                                                                                                                                                                                                                                                                                                                                              | \$1\$24Kc7H4s\$9HJhVb/fBkWGtUCYxuj1z1  | Mar'atus Salimah              | mhs.geofisika.its.ac.id/s/salimah16/Maildir/         |
| abdul.rosyid16@mhs.ne.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                | \$1\$dbakJola\$tbVvYDZnQNV/oZff1P7n1   | Abdul Rosyid                  | mhs.ne.its.ac.id/a/abdul.rosyid16/Maildir/           |
| atiqa16@mhs.chem-eng.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                 | \$1\$ALekPau6\$bauglkdnd42lvZYsz0pV.   | Atiqa Rahmawati               | mhs.chem-eng.its.ac.id/a/atiqa16/Maildir/            |
| irene16@mhs.geodesy.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                  | \$1\$RKEJNE9\$QO9/PC9kPFwT3R5.xkad01   | Irene Rwabudandi              | mhs.geodesy.its.ac.id/i/irene16/Maildir/             |
| luhur15@mhs.me.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                       | \$1\$xSR.e2Ybf\$5eWjCTkOEtf9bNgBqPB0   | Luhur Setiabudi               | mhs.me.its.ac.id/l/luhur15/Maildir/                  |
| farai.william16@mhs.me.its.ac.id                                                                                                                                                                                                                                                                                                                                                                               | \$1\$gOpKul8\$K4RfFq4mXOEMQxQkSwb1J1   | Farai William Saungweme       | mhs.me.its.ac.id/f/farai.william16/Maildir/          |
| donald16@mhs.mb.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                      | \$1\$ow7S1PgB\$Hq6p11wCSkLJYc4BMKuR41  | Donald Ralph Allan Sai'i      | mhs.mb.its.ac.id/d/donald16/Maildir/                 |
| razafiarison16@mhs.arch.its.ac.id                                                                                                                                                                                                                                                                                                                                                                              | \$1\$X4cExAWp\$Q8Jr1k87jst/V/twfp/La.  | Razafiarison Serge Landry     | mhs.arch.its.ac.id/r/razafiarison16/Maildir/         |
| mohammed.khatib16@mhs.is.its.ac.id                                                                                                                                                                                                                                                                                                                                                                             | \$1\$hdT7mtYg\$R8LOU2HaY9OGnyUwnVf/    | Mohammed Khatib Juma          | mhs.is.its.ac.id/m/mohammed.khatib16/Maildir/        |
| muhamad16@mhs.me.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                     | \$1\$XkWSZ0uM\$Prhrm1sSbJE1emieYoXIA.  | Muhamad Faisol                | mhs.me.its.ac.id/m/muhamad16/Maildir/                |
| shofiyah.nadhifah16@mhs.bio.its.ac.id                                                                                                                                                                                                                                                                                                                                                                          | \$1\$T44Jvxyt\$ZdYI/dITr5Ymt0dyGGS0    | Shofiyah Nadhifah Pramitasari | mhs.bio.its.ac.id/s/shofiyah.nadhifah16/Maildir/     |
| nadhira16@mhs.urplan.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                 | \$1\$HFgR.OcMG\$8mfjYYVpJDMPULoOma4IT1 | Nadhira Putri Rizkia          | mhs.urplan.its.ac.id/n/nadhira16/Maildir/            |
| alfia.rahma15@mhs.bio.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                | \$1\$wiDkM6FL\$ydo5sdrduEx1dodtX2t.G/  | Alfia Rahma Kurniawati        | mhs.bio.its.ac.id/a/alfia.rahma15/Maildir/           |
| yustisia.vicky16@mhs.ce.its.ac.id                                                                                                                                                                                                                                                                                                                                                                              | \$1\$C2840TSX\$Nk.OJ9mp25imPvL17B1aU.  | Vicky Wildan Yustisia         | mhs.ce.its.ac.id/y/yustisia.vicky16/Maildir/         |
| ainul16@mhs.matematika.its.ac.id                                                                                                                                                                                                                                                                                                                                                                               | \$1\$FTjZfAtu\$DSz/S/W3uJ6jX/cRaGduD1  | Ainul Imam                    | mhs.matematika.its.ac.id/a/ainul16/Maildir/          |
| rifqi.soedjono16@mhs.urplan.its.ac.id                                                                                                                                                                                                                                                                                                                                                                          | \$1\$trgoTg6y\$3GscUolQuTYI.enbXhuV1   | Muhammad Rifqi Soedjono       | mhs.urplan.its.ac.id/r/rifqi.soedjono16/Maildir/     |
| taufan.majid16@mhs.ce.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                | \$1\$P0L6XoN\$ZyXUq1ZISndtO9.n12K0.    | Taufan Fairus Majid           | mhs.ce.its.ac.id/t/taufan.majid16/Maildir/           |
| raulia.reno16@mhs.geofisika.its.ac.id                                                                                                                                                                                                                                                                                                                                                                          | \$1\$RZaxMBEK\$3p.G94.jOfmNJWje3rEw1   | Raulia Reno Cahyaningtyas     | mhs.geofisika.its.ac.id/r/raulia.reno16/Maildir/     |
| rifqi.fauzan16@mhs.na.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                | \$1\$gGUazUnS\$AGxvsBT6gFmpQntC77d2/   | Rifqi Fauzan Soepardjo        | mhs.na.its.ac.id/r/rifqi.fauzan16/Maildir/           |
| cintantya.budi15@mhs.ce.its.ac.id                                                                                                                                                                                                                                                                                                                                                                              | \$1\$wf/k01nr\$X0HEXbWxd5svXINEQB0C0C/ | Cintantya Budi Casita         | mhs.ce.its.ac.id/c/cintantya.budi15/Maildir/         |
| wijaya16@mhs.enviro.its.ac.id                                                                                                                                                                                                                                                                                                                                                                                  | \$1\$ox7.yk1P\$AVmAz97nMIUgChD/0z.Lz0  | I Made Wahyu Wijaya           | mhs.enviro.its.ac.id/w/wijaya16/Maildir/             |

Gambar F.74 Enkripsi Field Password didalam Database



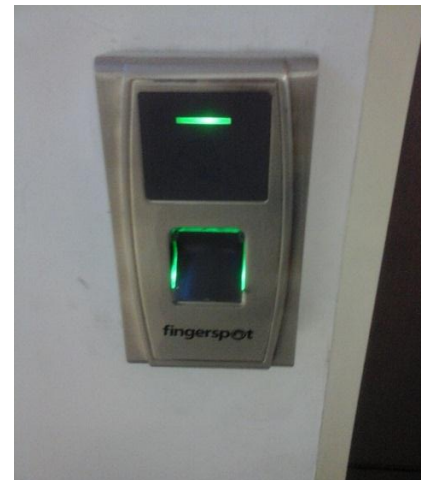
Gambar F.75 *Receptionist Area* (Diluar)



Gambar F.76 *Receptionist Area* (Didalam)



Gambar F.77 *Receptionist Area* (Didalam) (lanj.)



Gambar F.78 Pintu dengan Kunci *Fingerprint*





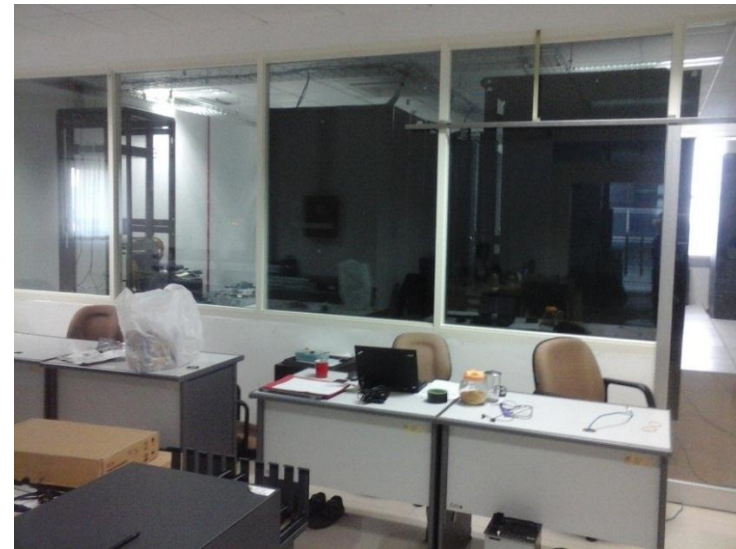
Gambar F.79 Pintu Kebakaran



Gambar F.80 CCTV



Gambar F.81 Ruangan Subdit Infrastruktur (Diluar)



Gambar F.82 Ruangan Subdit Infrastruktur (Didalam)



Gambar F.83 Ruangn Pusat Data



Gambar F.84 Nomor pada Ruangan



Gambar F.85 Hydrant



Gambar F.86 Perangkat Pemadam Otomatis



Gambar F.87 Perangkat Pendeteksi Asap



Gambar F.88 Perangkat APAR





Gambar F.89 Lemari



Gambar F.90 Lemari (lanj.)



Gambar F.91 Pintu Masuk Gedung Research Center ITS



Gambar F.92 AC



Gambar F.93 Remote AC dengan Pengatur Suhu dan Kelembaban



Gambar F.94 Perangkat *Grounding*





Gambar F.95 Kotak Panel Listrik dengan Fungsi *Circuit Breaker*



Gambar F.96 Stop Kontak dengan Fungsi *Circuit Breaker*



Gambar F.97 Pemasangan Pipa Pelindung Kabel



Gambar F.98 Patok Penanda Kabel Listrik



Gambar F.99 Patok Penanda Kabel *Fiber Optic*



Gambar F.100 Patok Penanda Kabel *Fiber Optic* (Kondisi Rusak)

### INSTRUKSI KERJA

#### Cable Tester

- Masukkan kedua ujung UTP kedalam Cable Tester.
- Nyalakan power kabel tester.
- Amati urutan lampu yang menyala

Gambar F.101 Instruksi Kerja *Cable Tester*

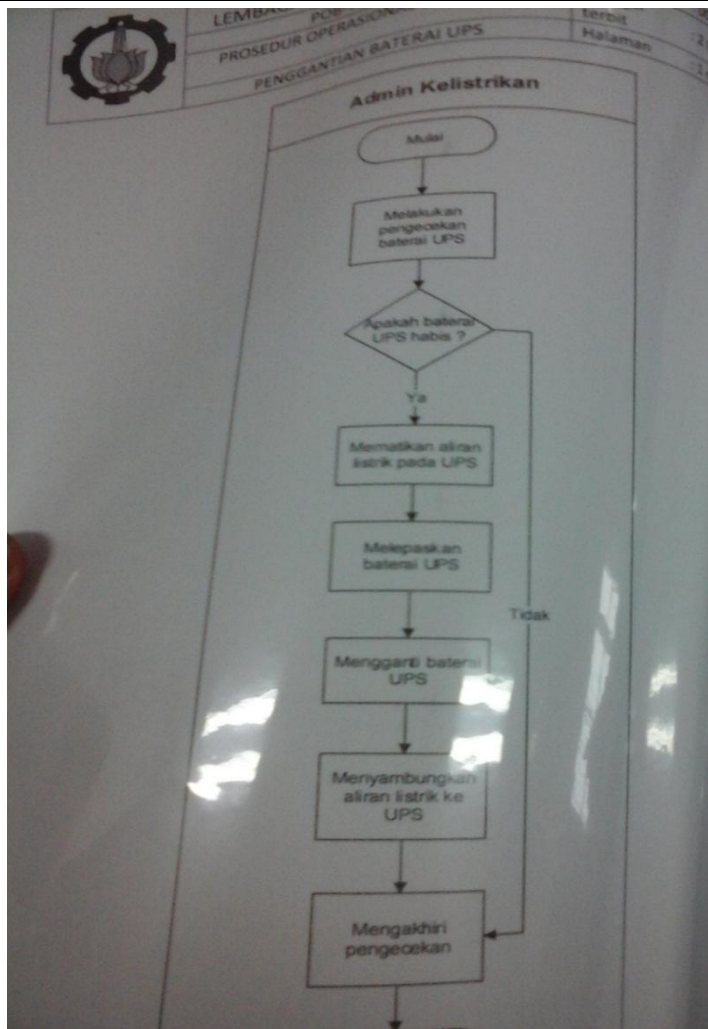
### INSTRUKSI KERJA

#### Crimping Tools

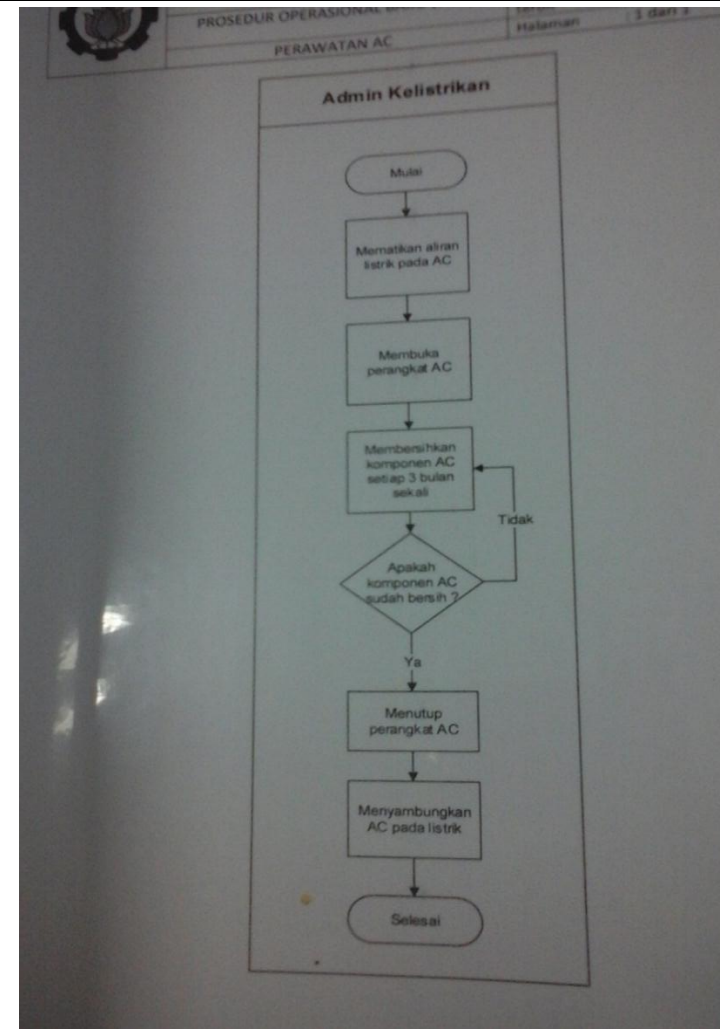
- Kupas kabel UTP sesuai urutan.
- Masukkan kabel UTP kedalam Connector.
- Masukkan kedalam Crimping Tools
- Tekan tuas Crimping Tools.

Gambar F.102 Instruksi Kerja *Crimping Tools*

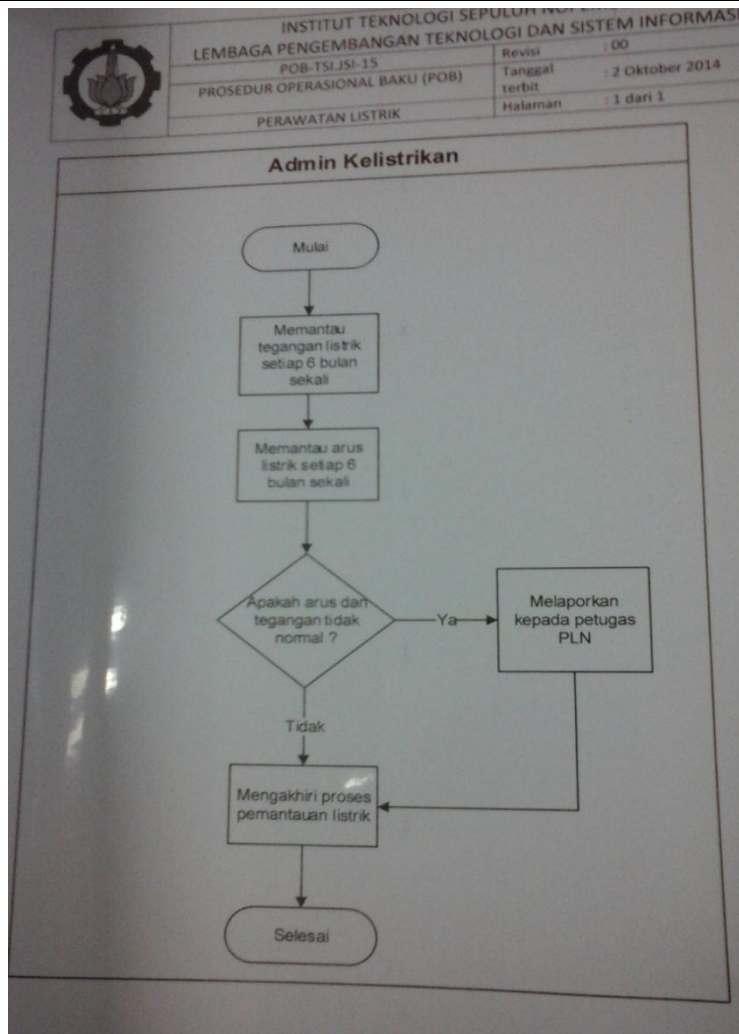




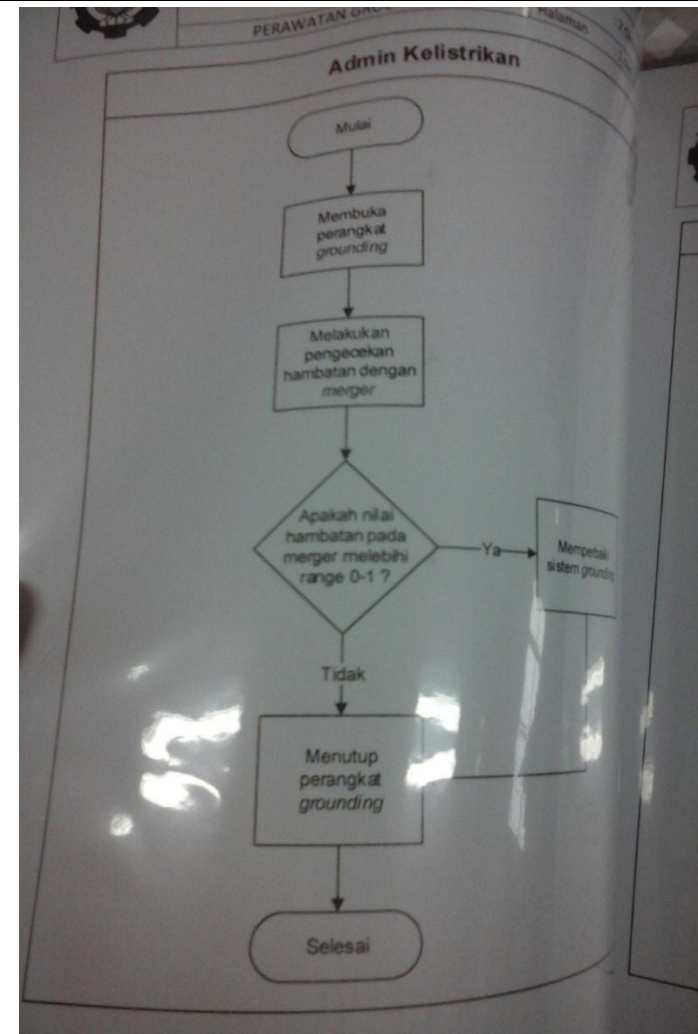
Gambar F.103 Prosedur Penggantian Baterai *UPS*



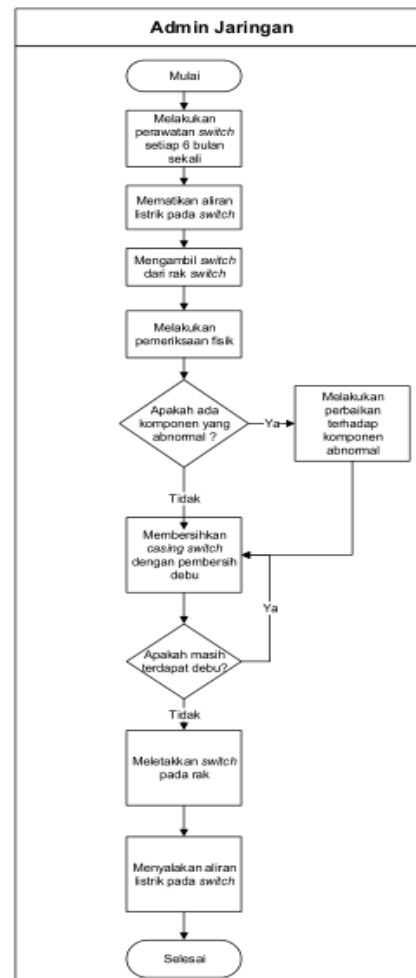
Gambar F.104 Prosedur Perawatan *AC*



Gambar F.105 Prosedur Perawatan Listrik



Gambar F.106 Prosedur Perawatan *Grounding*



Gambar F.107 Prosedur Perawatan Switch



#### 1. Tujuan

- Melayani permintaan data ITS baik dari dalam ITS maupun luar ITS
- Memenuhi kebutuhan informasi baik akademik maupun non akademik, sehingga dapat dipergunakan sebagai mana mestinya sesuai kebutuhan pengguna data.

#### 2. Ruang Lingkup

Pelayanan permintaan data baik dari Unit-Unit di ITS, perseorangan sivitas akademika ITS, maupun instansi dan perseorangan dari luar ITS adalah salah satu bentuk kewajiban yang harus dipenuhi di Pusat Data dan Pelaporan LPTSi ITS. Data yang dapat diberikan adalah data akademik dan non akademik, yaitu data:

- Akademik (jumlah mahasiswa, jumlah jurusan/prodi, jumlah peminat, jumlah lulusan, data IPK, TOEFL, produktivitas)
- Non akademik (jumlah dosen dan staf, dana, fasilitas, serta data informasi lainnya yang terjadi di lingkungan ITS).

#### 3. Definisi

- Mahasiswa ITS adalah seluruh mahasiswa ITS dari seluruh jenjang pendidikan
- Staf Akademik atau tenaga pendidik adalah jumlah dosen tetap (PNS & CPNS) yang telah memiliki Nomor Induk Pegawai (NIP) termasuk yang sedang studi lanjut dan non PNS
- Staf non atau tenaga kependidikan akademik adalah jumlah staf administrasi (CPNS & PNS) yang meliputi: tenaga administrasi, teknisi, laboran, pustakawan, dan umum

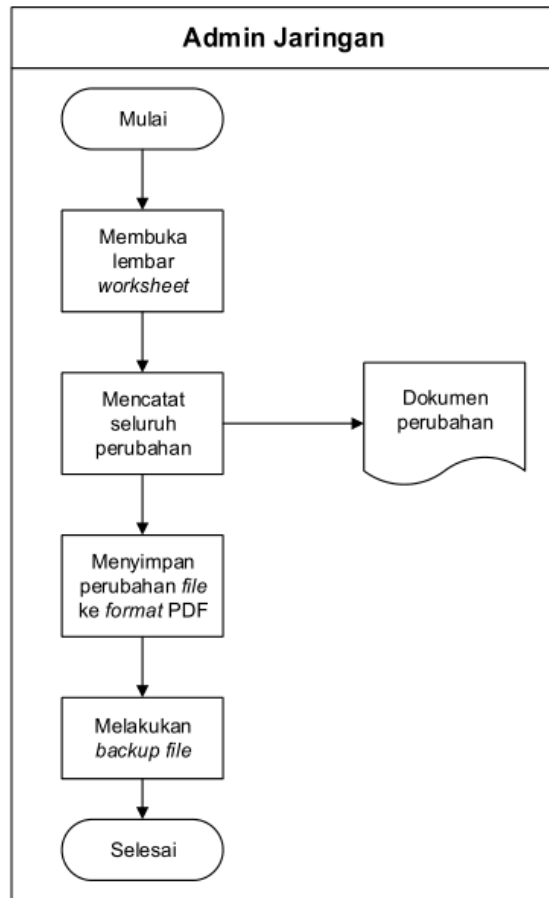
#### 4. Dokumen / sumber data Terkait

- Laporan Tahunan Rektor dalam rangka Dies Natalis
- Informasi pada laman ITS di [www.its.ac.id](http://www.its.ac.id)
- Sistem Informasi Akademik, Sistem Informasi Kepegawaian, dll baik yang sudah terintegrasi di integra dan yang belum terintegrasi.

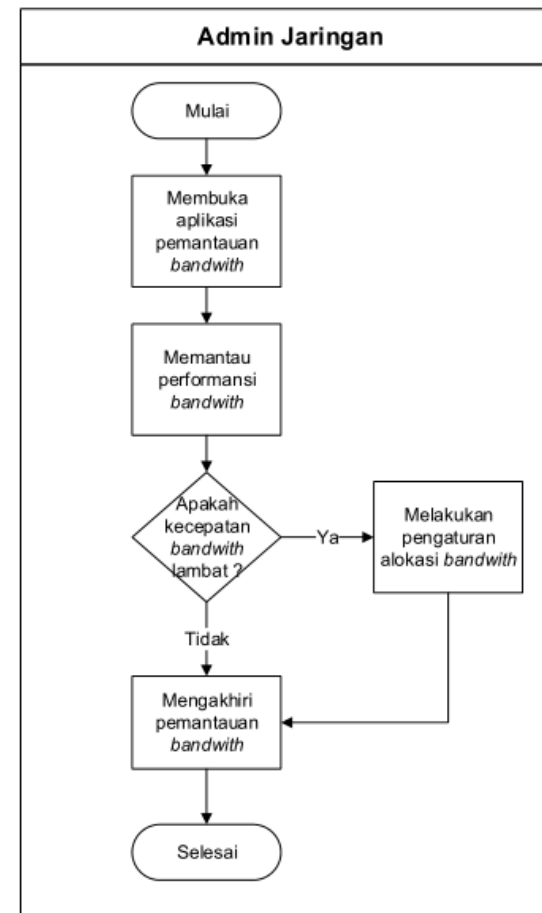
#### 5. Rincian Prosedur

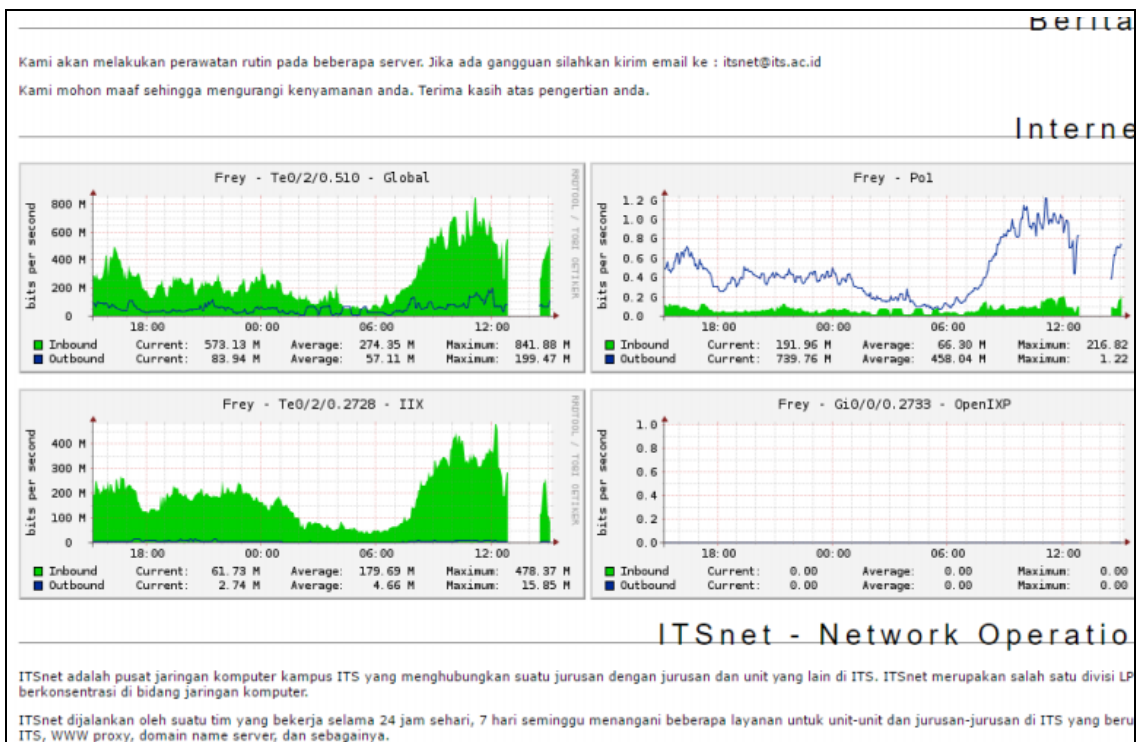
| No | Penanggung jawab       | Aktivitas                                                                                                                                                                                                                                                                                                                                                                    |
|----|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Help desk LPTS         | <ul style="list-style-type: none"> <li>- Menerima permintaan data melalui email atau surat</li> <li>- Meneruskan email/surat permintaan data kepada Koordinator Pusat data dan pelaporan</li> </ul>                                                                                                                                                                          |
| 2. | Koordinator Pusat Data | <ul style="list-style-type: none"> <li>- Menganalisis jenis permintaan data</li> <li>- Menghubungi peminta data untuk melihat di aplikasi penyajian data online jika data tersedia</li> <li>- Meneruskan ke staff Pusat Data untuk segera menyiapkan kebutuhan data sebagaimana permintaan apabila data yang dimaksud tidak ada di aplikasi penyajian data online</li> </ul> |
| 3. | Staf Pusat Data        | <ul style="list-style-type: none"> <li>- Menerima Email / Surat permintaan dari koordinator Pusat Data dan Pelaporan untuk segera menyiapkan kebutuhan data sesuai permintaan</li> <li>- Menyiapkan Data sesuai Permintaan</li> <li>- Apabila data sudah siap, memberikan kepada Koordinator Pusat Data dan Pelaporan</li> </ul>                                             |
| 4. | Koordinator Pusat Data | <ul style="list-style-type: none"> <li>- Memeriksa kebenaran dan validitas datanya</li> <li>- Memberikan data kepada pihak yang meminta data</li> </ul>                                                                                                                                                                                                                      |

Gambar F.108 Prosedur Pelayanan Permintaan Data ITS



Gambar F.109 Prosedur Dokumentasi Konfigurasi Sistem Jaringan

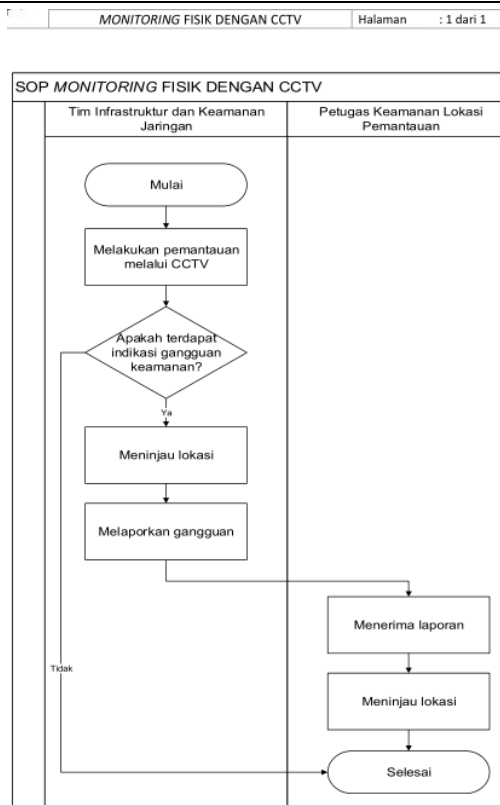
Gambar F.110 Prosedur *Monitoring Bandwidth*



Gambar F.111 Cacti

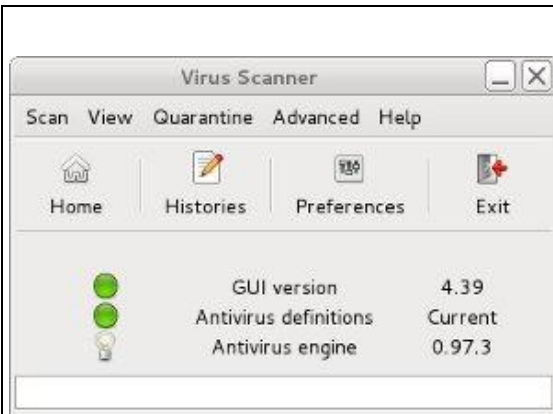


Gambar F.112 Perangkat Absensi  
Fingerprint

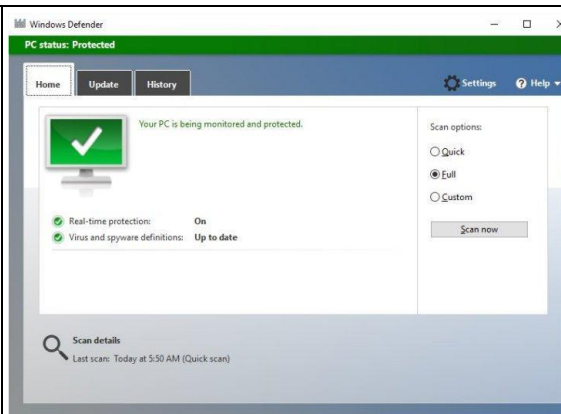


Gambar F.113 Prosedur *Monitoring* Fisik dengan CCTV





Gambar F.114 ClamAV



Gambar F.115 Windows Defender

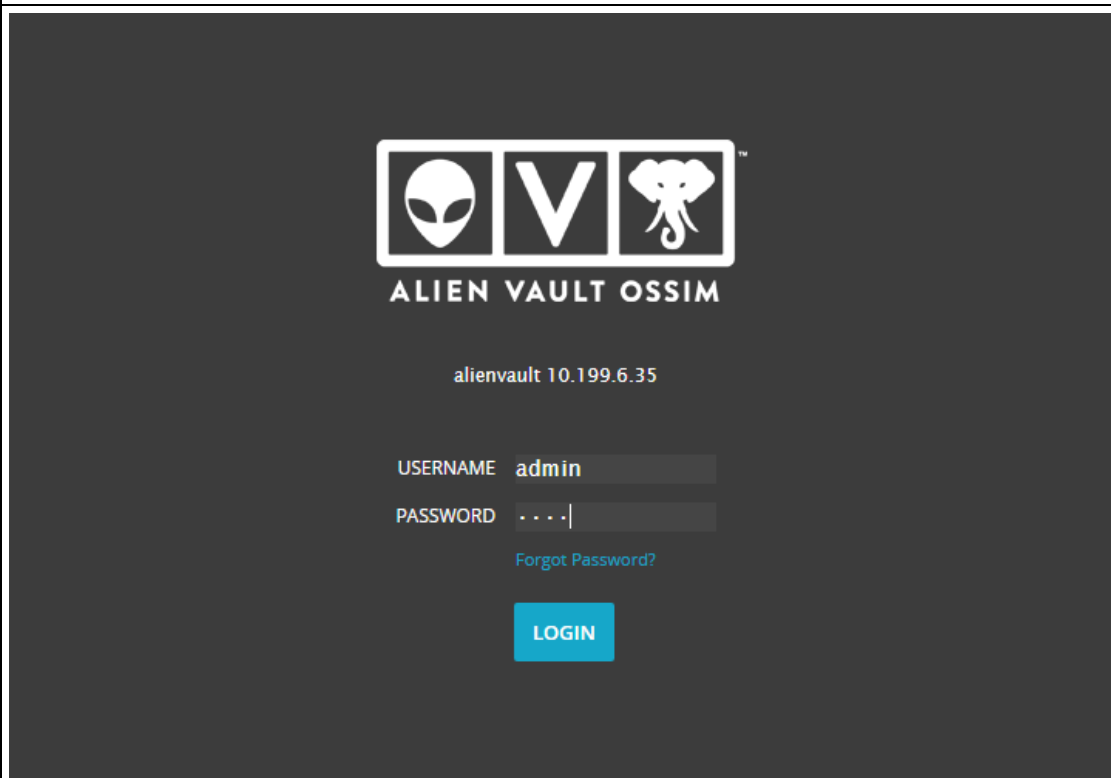
| <div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p><b>INSTITUT TEKNOLOGI SEPULUH NOPEMBER</b></p> <p><b>LEMBAGA PENGEMBANGAN TEKNOLOGI SISTEM INFORMASI</b></p> </div> </div> |             |                                                        |                  |                                 |                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|--------------------------------------------------------|------------------|---------------------------------|-------------------------------|
| RM – TSI.SIM - 02                                                                                                                                                                                                     |             |                                                        |                  | Revisi : 01                     |                               |
| BACK UP DATA                                                                                                                                                                                                          |             |                                                        |                  | Tanggal Terbit : 2 Oktober 2014 |                               |
|                                                                                                                                                                                                                       |             |                                                        |                  | Halaman : 1 dari 1              |                               |
| NO                                                                                                                                                                                                                    | NAMA PROSES | TAHAPAN PROSES                                         | KENDALI PROSES   | DOKUMEN TERKAIT                 | PENANGGUNG JAWAB              |
| 1                                                                                                                                                                                                                     | Perencanaan | Menentukan waktu backup harian, mingguan, atau bulanan | Rapat koordinasi | Rencana Kegiatan                | Koord. Pusat Pengembangan SIM |
| 2                                                                                                                                                                                                                     | Pelaksanaan | Melaksanakan backup sesuai dengan rencana jadwal       | Jadwal Back Up   | Hasil Data Back up              | Koord. Pusat Pengembangan SIM |
| 3                                                                                                                                                                                                                     | Monitoring  | Pengecekan pelaksanaan back up                         | Jadwal Back Up   | Hasil Data Back up              | Koord. Pusat Pengembangan SIM |

Gambar F.116 Prosedur *Backup Data*

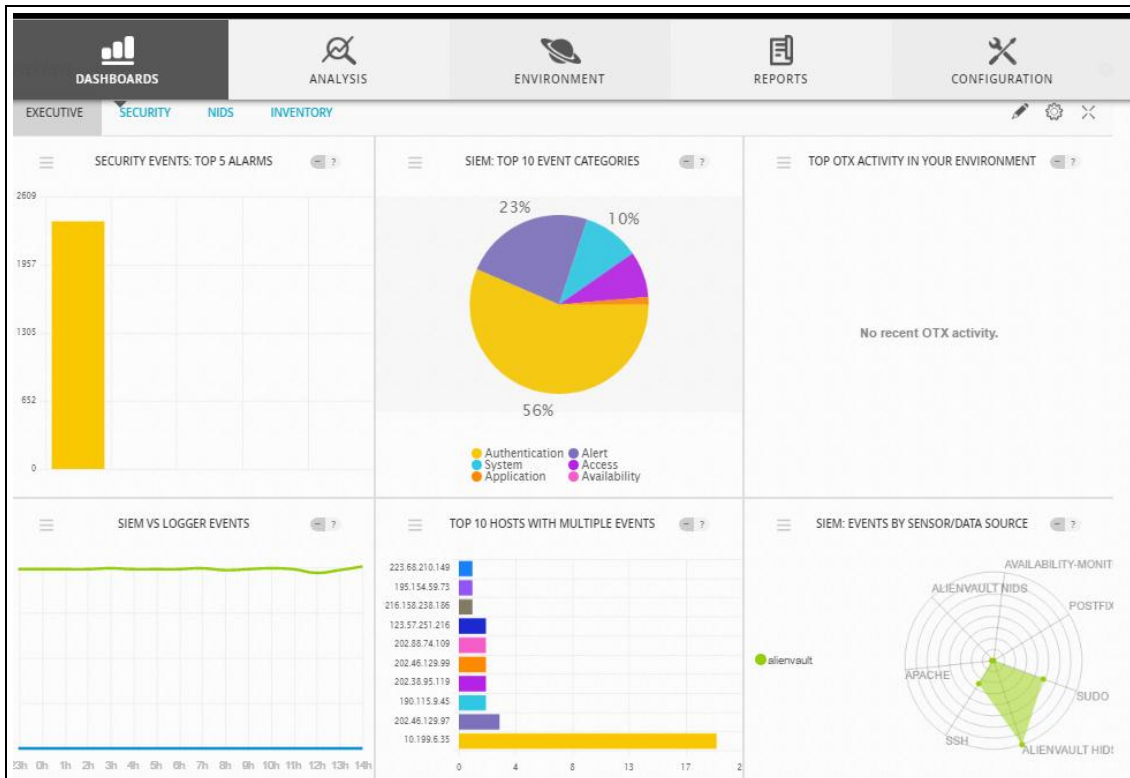


[illegible]

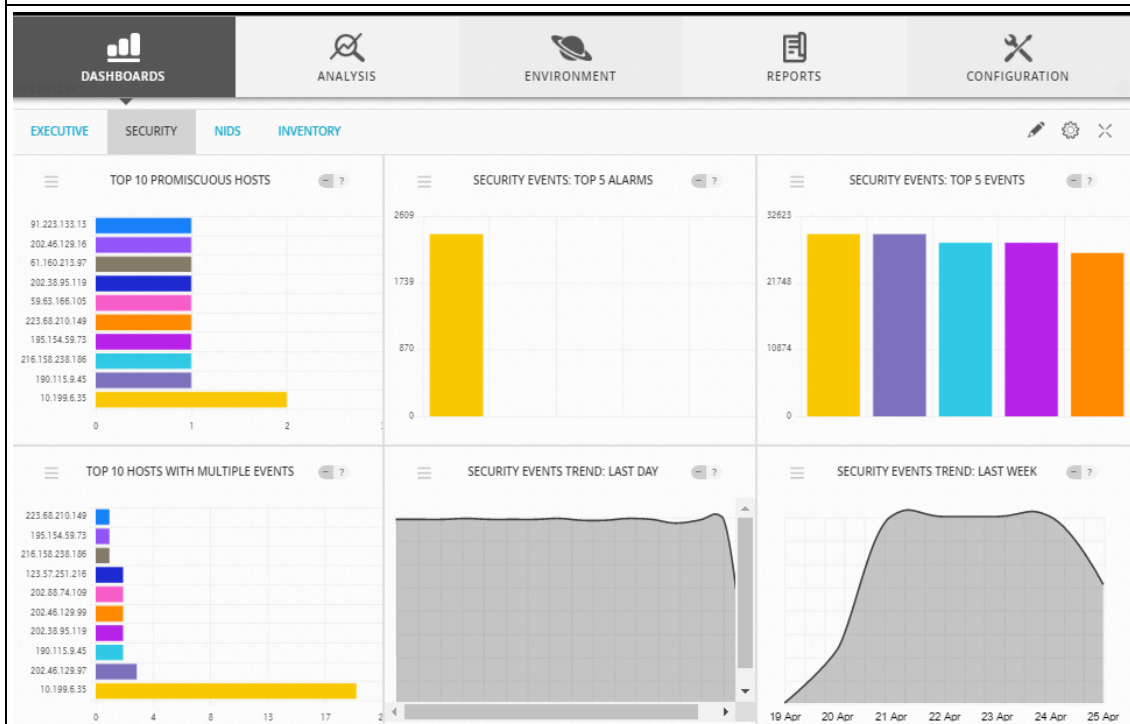
Gambar F.117 Form Rekap Kegiatan *Backup Database* dan Sistem SIM



Gambar F.118 Halaman *Login SIEM* AlienVault



Gambar F.119 *Dashboard SIEM AlienVault* yang Berisikan Laporan Keseluruhan Aktivitas Kejadian dan Keamanan



Gambar F.120 *Dashboard SIEM AlienVault* yang Berisikan Laporan Ancaman dan Kondisi Keamanan

| DASHBOARDS          |        | ANALYSIS                  |        | ENVIRONMENT |     | REPORTS              |                    | CONFIGURATION |  |
|---------------------|--------|---------------------------|--------|-------------|-----|----------------------|--------------------|---------------|--|
| DATE                | STATUS | INTENT & STRATEGY         | METHOD | RISK        | OTX | SOURCE               | DESTINATION        |               |  |
| 2017-04-20 05:55:08 | open   | Bruteforce Authentication | SSH    | 1           |     | 185.165.29.44:52305  | 202.46.129.218:ssh |               |  |
| 2017-04-20 04:38:36 | open   | Bruteforce Authentication | SSH    | 2           | N/A | 59.63.166.105:46430  | 202.46.129.218:ssh |               |  |
| 2017-04-20 02:33:42 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:11115  | 202.46.129.218:ssh |               |  |
| 2017-04-20 01:26:09 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:42621  | 202.46.129.218:ssh |               |  |
| 2017-04-20 00:19:38 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:60824  | 202.46.129.218:ssh |               |  |
| 2017-04-19 23:04:49 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:62668  | 202.46.129.218:ssh |               |  |
| 2017-04-19 21:54:07 | open   | Bruteforce Authentication | SSH    | 1           |     | 91.211.1.100:47564   | 202.46.129.218:ssh |               |  |
| 2017-04-19 21:31:07 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:28713  | 202.46.129.218:ssh |               |  |
| 2017-04-19 20:12:47 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:45084  | 202.46.129.218:ssh |               |  |
| 2017-04-19 19:57:10 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 118.182.117.68:48334 | 202.46.129.218:ssh |               |  |
| 2017-04-19 18:59:14 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:34244  | 202.46.129.218:ssh |               |  |
| 2017-04-19 12:46:00 | open   | Bruteforce Authentication | SSH    | 1           |     | 91.197.232.11:52414  | 202.46.129.218:ssh |               |  |
| 2017-04-19 09:00:19 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:29760  | 202.46.129.218:ssh |               |  |
| 2017-04-19 08:59:20 | open   | Bruteforce Authentication | SSH    | 1           |     | 91.197.232.108:40177 | 202.46.129.218:ssh |               |  |
| 2017-04-19 07:20:20 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:41667  | 202.46.129.218:ssh |               |  |
| 2017-04-19 06:04:42 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:26042  | 202.46.129.218:ssh |               |  |
| 2017-04-19 04:59:12 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:22861  | 202.46.129.218:ssh |               |  |
| 2017-04-19 03:53:22 | open   | Bruteforce Authentication | SSH    | 1           | N/A | 59.63.166.105:53643  | 202.46.129.218:ssh |               |  |

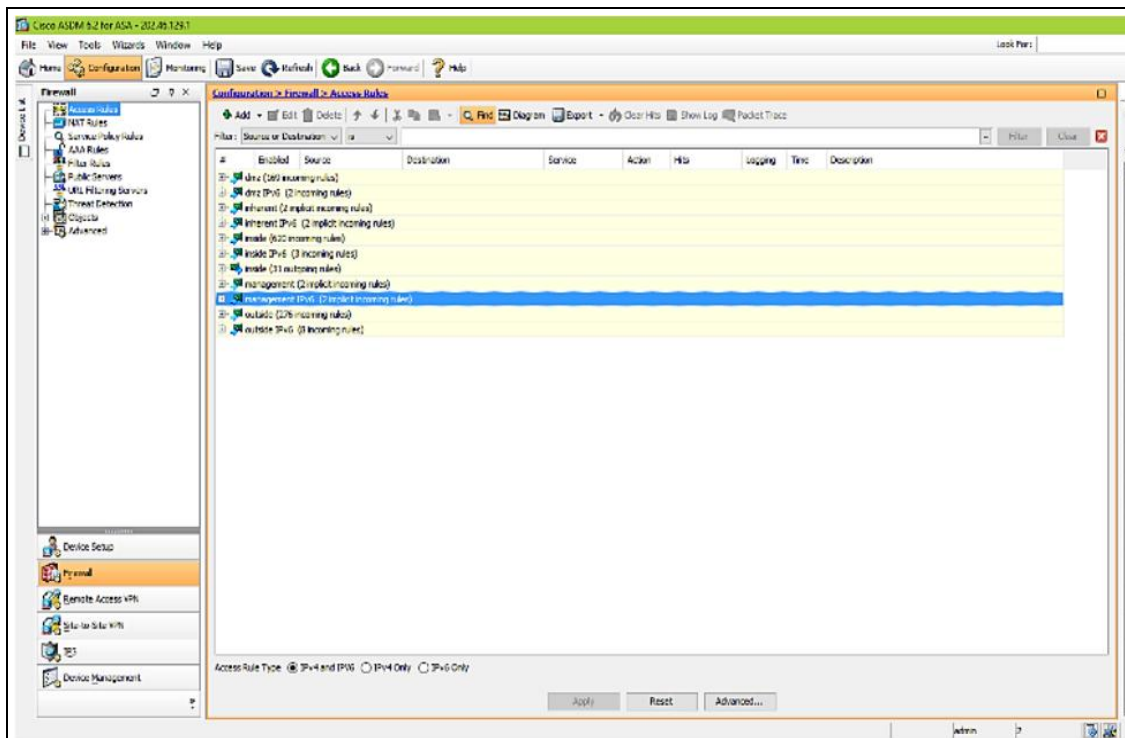
Gambar F.121 SIEM AlienVault yang Berisikan Serangan yang Terjadi

Gambar F.121 SIEM AlienVault yang Berisikan Serangan yang Terjadi

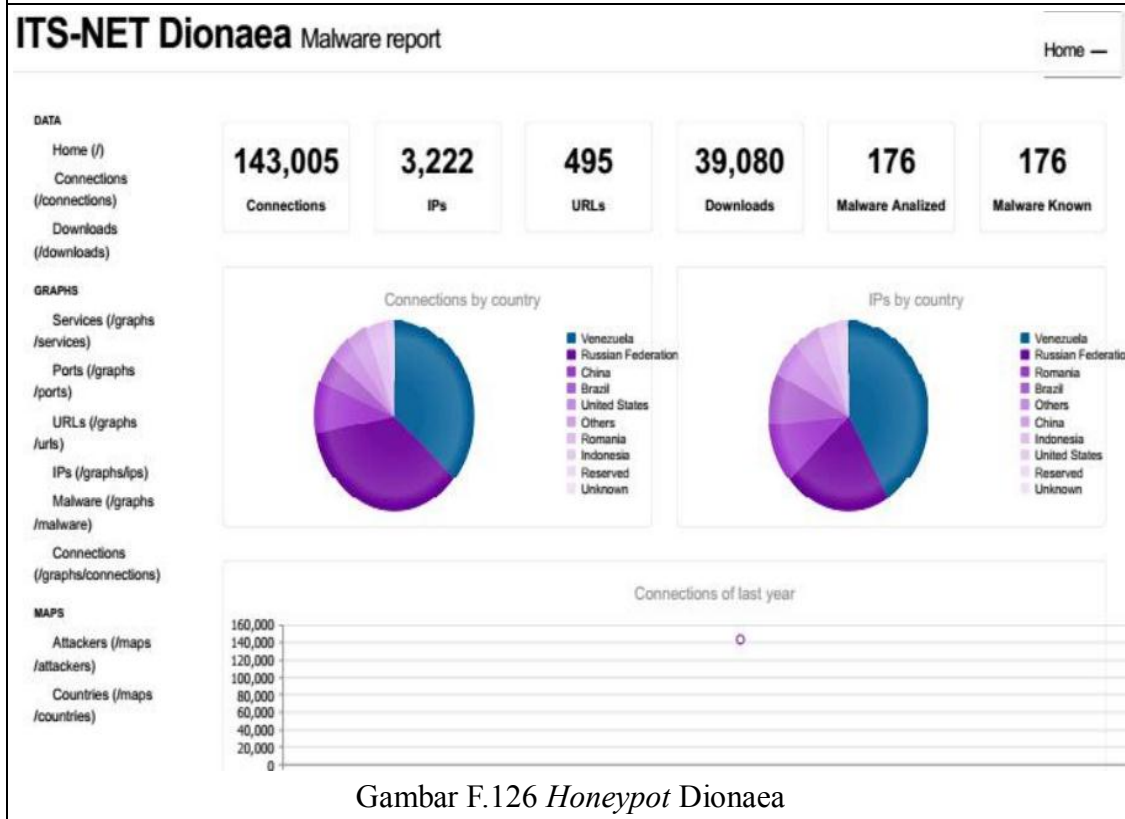
|                                                                       |       |    |                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |               |
|-----------------------------------------------------------------------|-------|----|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|
| ossec.noc.its.ac.id/analogs/detail.php?rule_id=31152&breakdown=source |       |    |                    | snort                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |               |
|                                                                       |       |    |                    | <pre> %20and%20=1 HTTP/1.1" 500 1 20306 195.154.181.15 -- [27/Nov/2 "GET /index.php?option=com_pccookbook&amp;page=viewuserrecipes&amp;user_id 9999999+UNION+SELECT+md5(3.1415)-- HTTP/1.1" 500 1 21689 195.1 /2016:20:16:19 +0700) "GET /index.php/webinars-categories?id=0%20%29 %20union%20select%20md5(3.1415)--%20%29 HTTP/1.1" 500 1 21689 19 [27/Nov/2016:20:15:42 +0700) "GET /index.php?option=com_contenthisto list%5Bordering%5D~&amp;item_id=1&amp;type_id=1&amp;list%5Bselect%5D= (select%201%20from%20(select%20count("),concat((select%200x6275677 nd(0)*2))x%20from%20information_schema.tables%20group%20by%20x) 20652 1471319875.511 0 10.113.8.115 TCP DENIED/407 3739 GET http://wallpaper.pcappstore.baidu.com/wallpaper/getTypeList - HIER_NON 62.210.88.198 -- [23/Nov/2016:17:42:17 +0700) "GET /index.php?option= id=20+UNION+SELECT+md5(3.1415)-- HTTP/1.1" 404 1390 14226 62.21 /2016:17:42:13 +0700) "GET /index.php?option=com_memorix&amp;task=resul searchplugin-theme&amp;Itemid=60&amp;ThemeID=- 8594+union+select+111,222,MD5(3.1415),444,555,666,777,888,999-- Aht 1390 14246 62.210.88.198 -- [23/Nov/2016:17:42:12 +0700) "GET /index.p option=com_redshop&amp;view=product&amp;task=addToCompare&amp;pid=24 %22%20and%20=0%20union%20select%201,2,3,4,5,6,7,8,md5(3.1415),1 18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,4 50,51,52,53,54,55,56,57,58,59,60,61,62,63%23&amp;cmd=add&amp;cid=20&amp;sid=0.4 HTTP/1.1" 404 1390 14256 62.210.88.198 -- [23/Nov/2016:17:42:12 --0700 /index.php?option=com_job&amp;controller=listcategory&amp;task=viewJob&amp;id_job 1--UNION+ALL+SELECT+1,md5(3.1415),3,4,5,6,7,8,9,10,11,12,13,14,15, 3,24,25,26,27,28,29,30,31,32,33,34,35,36,37,38,39,40,41,42-- HTTP/1.1" 40 62.210.88.198 -- [23/Nov/2016:17:42:11 +0700) "GET /index.php?option= cutid=113%20LIMIT%200,1%20UNION%20ALL%20SELECT%20NULL NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,N L,NULL,NULL,NULL,NULL,md5(3.1415),NULL,NULL,NULL,NULL,N L,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NU </pre> |               |
| 12809945                                                              | 31152 | 10 | 2016/11/23 5:42:19 | (zeus.its.ac.id) /var/log /whs/ulp.its.ac.id.access.log                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 62.210.88.198 |
| 12809945                                                              | 31152 | 10 | 2016/11/23 5:42:19 | (zeus.its.ac.id) /var/log /whs/ulp.its.ac.id.access.log                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | 62.210.88.198 |

Gambar F.122 Beberapa Server yang Disimpan File Log-nya didalam SIEM AlienVault



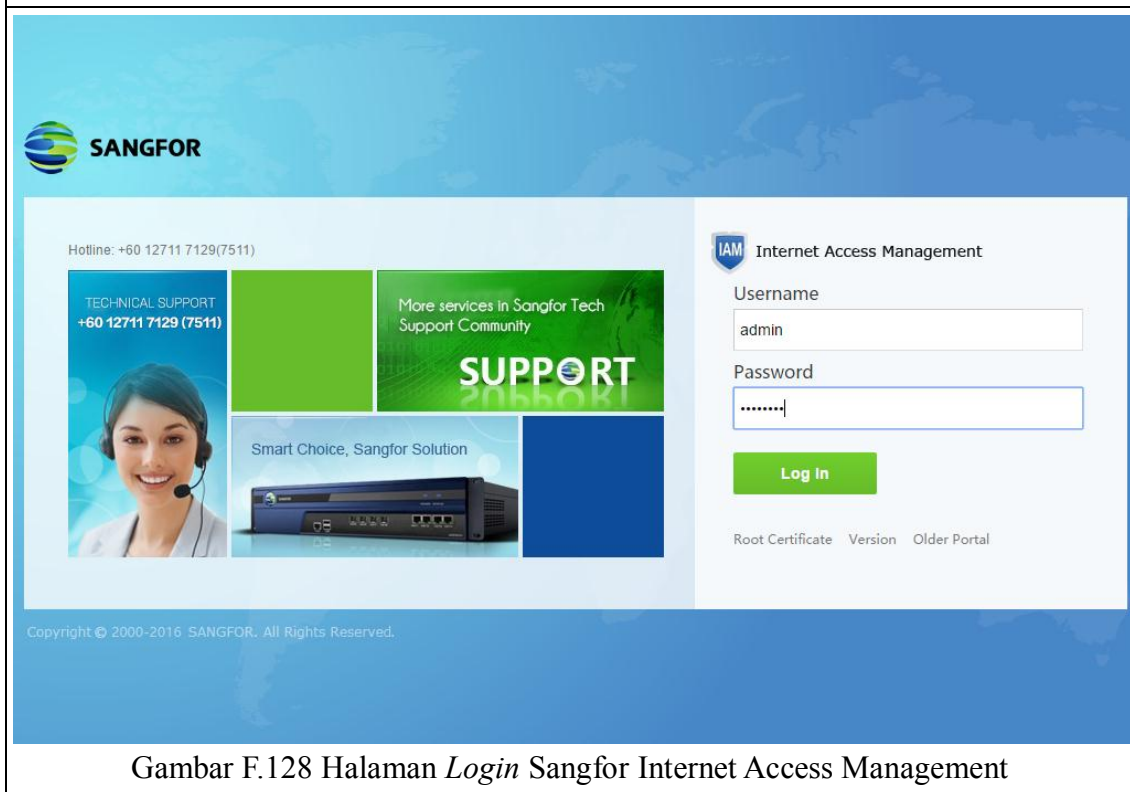
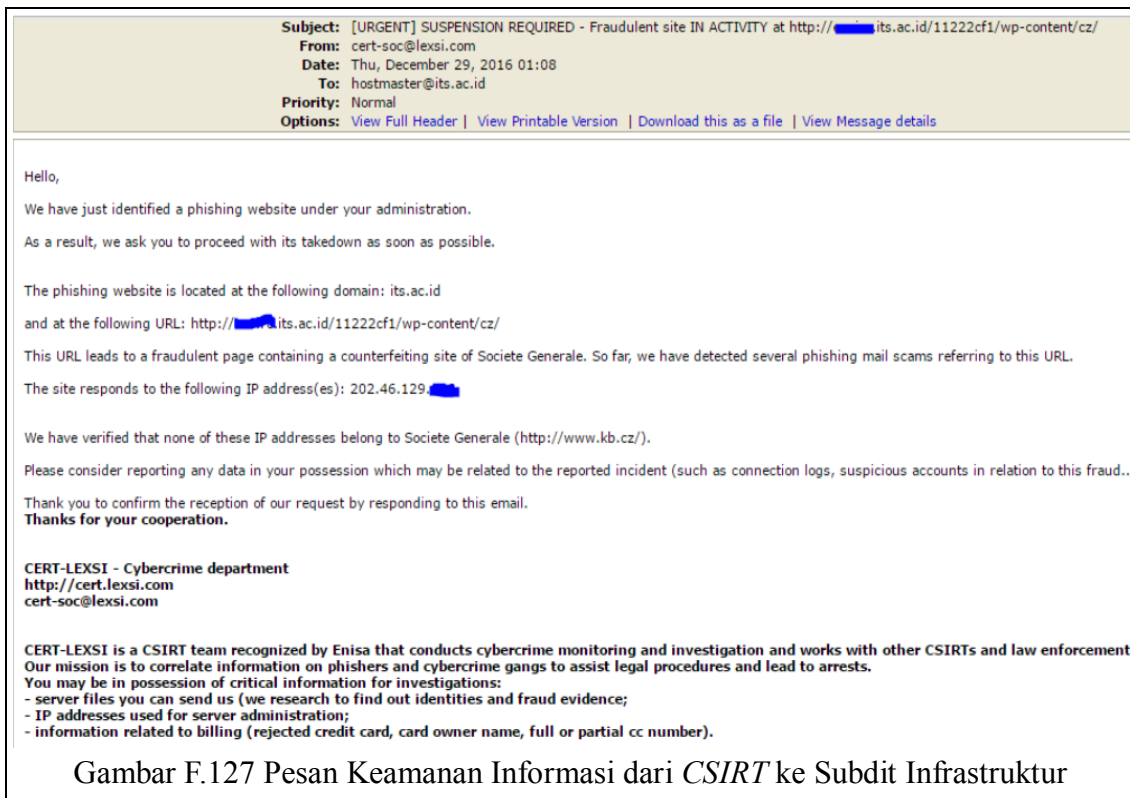


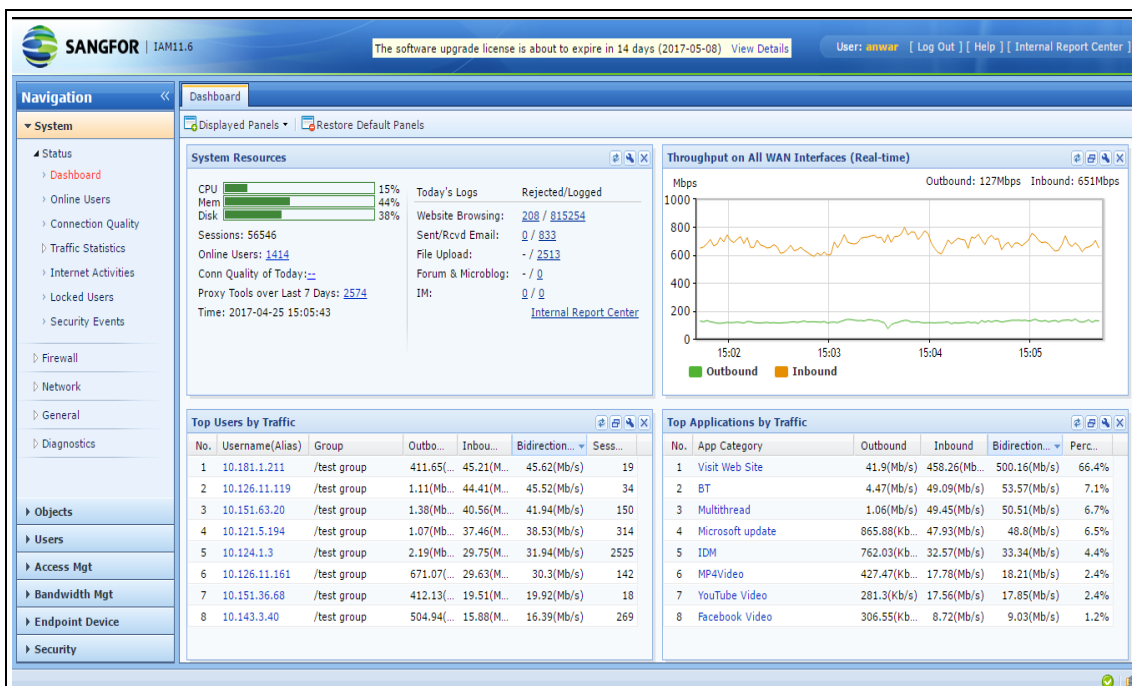
Gambar F.125 CISCO ASA Firewall (*Control Panel*)



Gambar F.126 *Honeypot* Dionaea







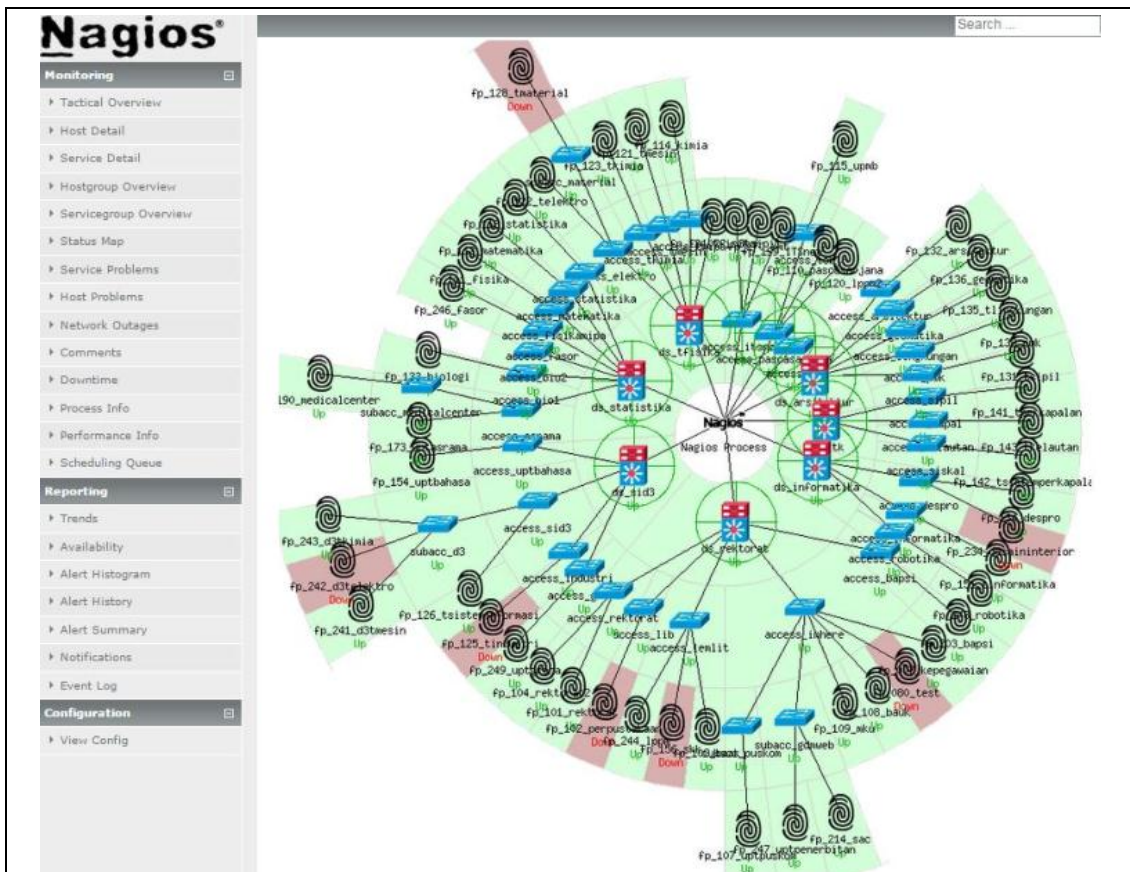
Gambar F.129 Halaman Awal Sangfor Internet Access Management

```

anta@proxy-66: ~
1480902409.881 2 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.883 2 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.883 295 10.132.19.10 TCP_MISS/302 771 GET http://adservr.adtechus.com/pubapi/3.0/9993.1/3581156/0/225/noperf=1:alla
bid:coor=yes;ristaq12@mhs.arch.its.ac.id DIRECT/152.163.66.131 -
1480902409.889 830 10.126.13.62 TCP_MISS/200 7961 CONNECT dt.adsafeprotected.com:443 nindahayu@is.its.ac.id DIRECT/69.172.216.11
1480902409.892 1 10.198.74.134 TCP_DENIED/407 1635 CONNECT gaa.apple.com:443 - NONE/- text/html
1480902409.894 1 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.894 0 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.914 4 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.914 4 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.922 1 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.922 1 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.926 30783 10.142.2.181 TCP_MISS/200 637373 CONNECT r3---an-2uuxa3vhug5onpu-cuie.googlevideo.com:443 hari_kristiono@ne.1
1480902409.934 0 10.170.1.113 TCP_DENIED/407 1665 CONNECT apil.reasonsecurity.com:443 - NONE/- text/html
1480902409.936 0 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.936 0 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.944 0 10.198.74.94 TCP_DENIED/407 1632 CONNECT 65.55.223.43:443 - NONE/- text/html
1480902409.947 289 10.132.19.10 TCP_MISS/200 34348 GET http://33across-d.openx.net/w/1.0/jstag?ristaq12@mhs.arch.its.ac.id DIRE
1480902409.952 327 10.132.19.10 TCP_MISS/200 34348 GET http://33across-d.openx.net/w/1.0/jstag?ristaq12@mhs.arch.its.ac.id DIRE
1480902409.953 2 10.111.3.222 TCP_DENIED/407 1656 CONNECT asldev.oes.avira.com:443 - NONE/- text/html
1480902409.953 2 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.953 2 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.956 301 10.132.19.10 TCP_MISS/200 34344 GET http://33across-d.openx.net/w/1.0/jstag?ristaq12@mhs.arch.its.ac.id DIRE
1480902409.958 0 10.170.1.113 TCP_DENIED/407 1665 CONNECT apil.reasonsecurity.com:443 - NONE/- text/html
1480902409.960 10074 10.198.73.216 TCP_MISS/200 39 CONNECT android.clients.google.com:443 emirrezal6@mhs.te.its.ac.id DIRECT/216.5
1480902409.961 0 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.977 0 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.977 0 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.996 2 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902409.996 2 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902410.004 1 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902410.006 1 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902410.012 1 10.111.3.222 TCP_DENIED/407 1656 CONNECT asldev.oes.avira.com:443 - NONE/- text/html
1480902410.019 0 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902410.019 0 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902410.025 1 10.198.74.37 TCP_DENIED/403 1525 CONNECT imap.gmail.com:993 - NONE/- text/html
1480902410.026 16383 10.170.92.137 TCP_MISS/200 13691 CONNECT na.ads.yahoo.com:443 ester15@mhs.ie.its.ac.id DIRECT/106.10.198.32 -
1480902410.033 0 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902410.034 1 10.170.83.222 TCP_DENIED/407 1644 CONNECT www.facebook.com:443 - NONE/- text/html
1480902410.048 7056 10.198.66.112 TCP_MISS/200 515261 CONNECT ri---an-2uuxa3vhug5onpu-cuie.googlevideo.com:443 arizah15@mhs.bio.i

```

Gambar F.130 Proxy (Squid)



Gambar F.131 Nagios



Gambar F.132 ITS Web Monitoring System





Search Results Power By USearch



1...

Gambar F.133 Pemblokiran *Website* Dilarang melalui Layanan *ISP*

ITS

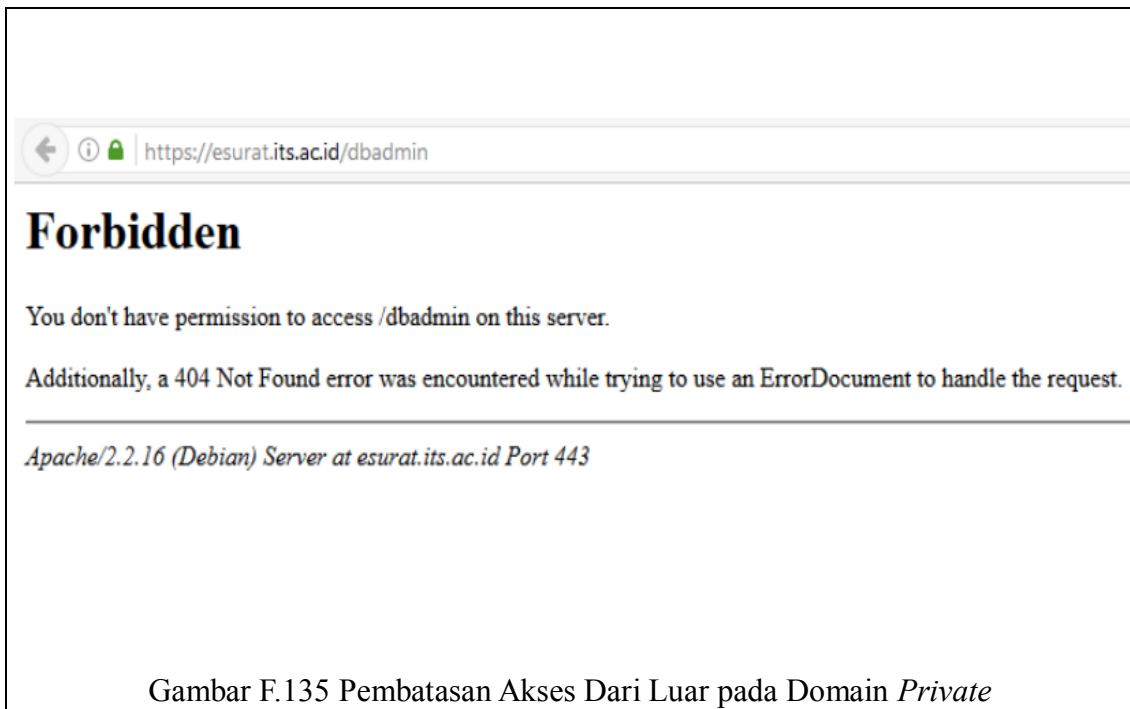
**Naah Lhoooo!**

Situs tidak dapat diakses karena mengandung unsur **PORNOGRAFI**. Jika anda merasa situs yang diakses tidak termasuk ke dalam kategori di atas silakan menghubungi:

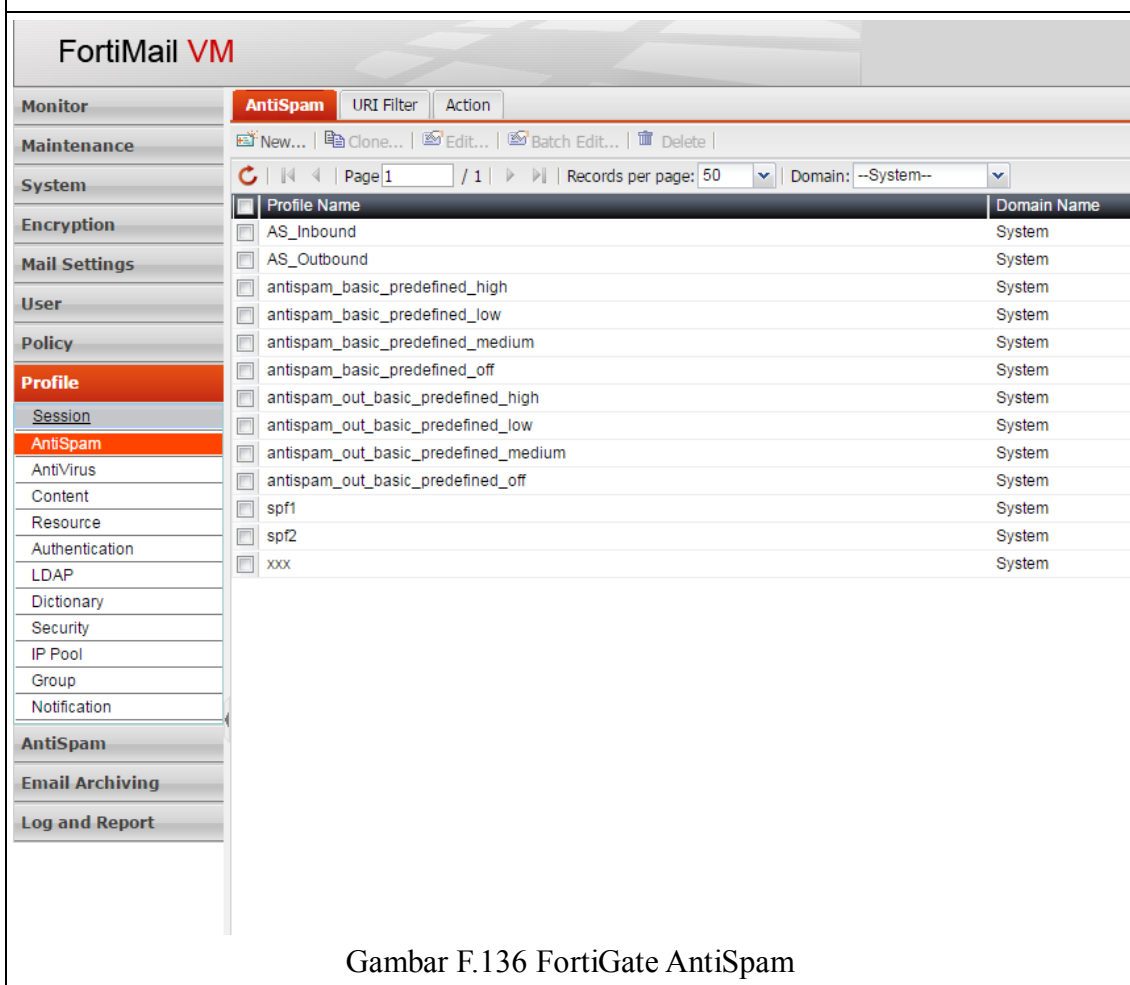
**LPTSI - [lptsi@its.ac.id](mailto:lptsi@its.ac.id)**

LPTSI

Gambar F.134 Pemblokiran *Website* Dilarang melalui Konfigurasi Perangkat



Gambar F.135 Pembatasan Akses Dari Luar pada Domain *Private*



Gambar F.136 FortiGate AntiSpam

**KESEPAKATAN BERSAMA  
MENJAGA KERAHASIAAN ASSET SISTEM INFORMASI INSTITUSI  
DILINGKUNGAN KAMPUS ITS**

Yang bertanda tangan dibawah ini :

Nama : INES DWI ANDINI  
 Identitas : NRP/KTP/NRP/identitaslainnya : 5110100218  
 Alamat : ASRAMA ITS BLOK J325 & PERUM BUMIAYU INDAH E21 RT 07 RW 02, MALANG  
 No.HP : 085646477549  
 E-mail : inesdwiandini@yahoo.com  
 SIM dikelola : ☒ Integra ☐ Cluster : Akademik  
☒ SIM lain : Aplikasi Persuratan

Yang selanjutnya disebut sebagai pihak I (pengelola sistem informasi)  
 Nama : Umi Laili Yuhana, S.Kom, M.Sc  
 NIP : 197606262005012002  
 Jabatan : Kepala Pusat Pengembangan Sistem Informasi BTSI- ITS

Yang selanjutnya disebut sebagai pihak II (penanggung jawab sistem informasi)  
 Pada tanggal 04 bulan oktober tahun 2013, antara pihak I dan Pihak II telah mengadakan kerjasama dimana Pihak I sebagai pengelola sistem informasi telah menyatakan sepakat untuk menjaga kerahasiaan aset institusi dengan cara sebagai berikut :

1. Menjaga kerahasiaan akses sistem informasi manajemen (SIM) yaitu berupa username, password, data, IP/Internet Protokol atau media apapun yang terhubung informasi tersebut agar tidak terbuka bagi pihak yang tidak berwenang.
2. Menjaga keutuhan dan keaslian data yang ada pada sistem informasi tersebut.
3. Menjaga agar akses pengguna yang legal terhadap data tidak ditolak oleh sistem informasi tersebut.
4. Menjaga data dan informasi yang telah tersimpan didalam media personal (komputer, flashdisk, storage, dll) dan segera menghilangkan/menghapus apabila sudah tidak dipergunakan.

Apabila pihak I dengan sengaja atau tidak melakukan tindakan yang tidak sesuai dengan kesepakatan yang telah dilakukan, maka pihak II berhak melakukan tindakan sesuai dengan sanksi akademik yang berlaku di ITS dan sanksi lain sesuai dengan undang – undang ITE yang berlaku.

Demikian kesepakatan bersama ini dibuat dan dilaksanakan dengan penuh tanggung jawab serta berlaku sampai dengan waktu yang tidak ditentukan.

Pihak II, Pihak I,  
Materai 6000  
 Umi Laili Yuhana, S.Kom, M.Sc Ines Dwi Andini

Gambar F.137 Kesepakatan Bersama Menjaga Kerahasiaan Aset Sistem Informasi Institusi Dilingkungan Kampus ITS

|                                                                                     |                                             |                                 |
|-------------------------------------------------------------------------------------|---------------------------------------------|---------------------------------|
|  | POB-TSI.YAN-02                              | Revisi : 01                     |
|                                                                                     | PROSEDUR OPERASIONAL BAKU (POB)             | Tanggal terbit : 2 Oktober 2014 |
|                                                                                     | LAYANAN PEMBUATAN SISTEM INFORMASI (INTERN) | Halaman : 2 dari 4              |

#### 1. Tujuan

Membuat pelayanan kepada pelanggan yang ingin dibuatkan sistem informasi baru ataupun sekedar menambahkan fitur baru pada sistem informasi yang sudah ada.

#### 2. Ruang Lingkup

Mengatur proses pelayanan pembuatan sistem informasi baru, maupun penambahan fitur pada sistem informasi eksisting yang diminta oleh pelanggan LPTSI, yakni dari unit dan jurusan di lingkungan ITS.

#### 3. Definisi

- Sistem informasi adalah suatu sistem yang berisi kumpulan informasi yang diperlukan bagi elemen terkait
- Unit adalah instansi atau lembaga yang berada di kampus ITS
- Jurusan adalah unit kerja yang mengelola jurusan atau program studi di kampus ITS.

#### 4. Dokumen terkait

- Form surat permohonan pembuatan sistem informasi
- Manual pembuatan rancangan sistem informasi berdasarkan *user requirements*.

#### 5. Rincian Prosedur

| NO | ENTITAS                                | AKTIVITAS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Unit/Jurusan                           | Mengajukan surat permohonan pembuatan sistem informasi baru atau penambahan fitur ke <i>Office</i> LPTSI ITS.                                                                                                                                                                                                                                                                                                                                                                                  |
| 2. | Pusat Layanan ( <i>Helpdesk</i> LPTSI) | Melakukan validasi surat, dan meneruskannya kepada Kepala LPTSI.                                                                                                                                                                                                                                                                                                                                                                                                                               |
| 3. | Ketua LPTSI                            | - Melakukan evaluasi terhadap permintaan unit/jurusan, apakah pembuatan sistem informasi baru atau penambahan fitur tersebut dinilai perlu atau tidak. Apabila dinilai tidak perlu, maka pihak unit/jurusan akan diberitahu bahwa permintaan tersebut ditolak dengan alasan tertentu.<br>- Melihat keadaan anggaran pada periode tersebut, apakah dinilai cukup atau tidak. Jika tidak, permintaan tersebut akan masuk <i>record</i> “daftar tunggu” untuk dicek lagi pada periode berikutnya. |
| 4. | Pusat Layanan ( <i>Analisis</i> )      | Memulai tahapan pembuatan sistem informasi dengan identifikasi kebutuhan pelanggan, yakni dengan menghubungi unit/jurusan terkait untuk mendapatkan data <i>user requirements</i> .                                                                                                                                                                                                                                                                                                            |
| 5. | Unit/Jurusan                           | Menyampaikan <i>user requirements</i> yang dimaksud untuk pembuatan sistem informasi baru atau penambahan fitur. Yakni berupa data dari <i>flowchart</i> proses bisnis, rancangan <i>database</i> , dan <i>user interface</i> .                                                                                                                                                                                                                                                                |
| 6. | Pusat Layanan ( <i>Analisis</i> )      | Melakukan analisis proses bisnis, perancangan <i>database</i> , dan <i>user interface</i> dari data yang didapat.                                                                                                                                                                                                                                                                                                                                                                              |
| 7. | Pusat Pengembangan ( <i>Desainer</i> ) | Menerima rancangan sistem informasi baru, ataupun rancangan penambahan fitur sistem informasi eksisting.                                                                                                                                                                                                                                                                                                                                                                                       |

Gambar F.138 Prosedur Layanan Pembuatan Sistem Informasi (Intern)

|                                                                                   |                                             |                                 |
|-----------------------------------------------------------------------------------|---------------------------------------------|---------------------------------|
|  | POB-TSI.YAN-01                              | Revisi : 01                     |
|                                                                                   | PROSEDUR OPERASIONAL BAKU                   | Tanggal terbit : 2 Oktober 2014 |
|                                                                                   | LAYANAN PERBAIKAN SISTEM INFORMASI (INTERN) | Halaman : 2 dari 2              |

- Tujuan**  
Membuat pelayanan kepada pengguna layanan LPTSI yang ingin mengajukan perbaikan ataupun pembaruan pada sistem informasi yang telah ada.
- Ruang Lingkup**  
Mengatur proses pelayanan perbaikan ataupun pembaruan pada sistem informasi eksisting yang diminta oleh pengguna layanan LPTSI yang berasal dari unit dan jurusan di ITS.
- Definisi**
  - Sistem informasi adalah suatu sistem yang berisi kumpulan informasi yang diperlukan bagi elemen terkait.
  - Pihak *internal* yang dimaksud adalah unit/jurusan yang berada di ITS.
- Dokumen Terkait**
  - Format surat permohonan pemutakhiran/perbaikan sistem informasi.
  - Standar pembuatan rancangan pengembangan *software*.
- Rincian Prosedur**

| NO | ENTITAS               | AKTIVITAS                                                                                                                                                                                   |
|----|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Unit/Jurusan          | Mengajukan surat permohonan pemutakhiran/perbaikan sistem informasi ke <i>Office</i> LPTSI ITS.                                                                                             |
| 2. | <i>Helpdesk</i> LPTSI | Melakukan validasi surat, dan meneruskan ke Analis SI.                                                                                                                                      |
| 3. | Analis SI             | Menghubungi unit/jurusan terkait untuk mendapatkan data <i>user requirements</i> .                                                                                                          |
| 4. | Unit/Jurusan          | Menyampaikan <i>user requirements</i> yang dimaksud untuk perbaikan/pemutakhiran SI. Yakni berupa data dari <i>flowchart</i> proses bisnis, rancangan database, dan <i>user interface</i> . |
| 5. | Analis SI             | Melakukan analisis proses bisnis, rancangan database, dan <i>user interface</i> dari data yang didapat.                                                                                     |
| 6. | Desainer SI           | Menerima rancangan pemutakhiran/perbaikan sistem informasi dari Analis SI.                                                                                                                  |
- Diagram Alir**  
Terlampir
- Record/Catatan Mutu**  
*Form* waktu pelayanan pembuatan sistem informasi.

Gambar F.139 Prosedur Layanan Perbaikan Sistem Informasi (Intern)

|                                                                                     |                                         |                                 |
|-------------------------------------------------------------------------------------|-----------------------------------------|---------------------------------|
|  | POB-TSI.SIM-05                          | Revisi : 01                     |
|                                                                                     | PROSEDUR OPERASIONAL BAKU (POB)         | Tanggal terbit : 2 Oktober 2014 |
|                                                                                     | PEMUTAKHIRAN/PERBAIKAN SISTEM INFORMASI | Halaman : 2 dari 3              |

- Tujuan**  
Menjelaskan proses pembuatan/pengembangan sistem informasi.
- Ruang Lingkup**  
Mengatur proses pembuatan/pengembangan sistem informasi yang diminta oleh pengguna layanan (*user*) terutama dari pihak internal ITS.
- Definisi**
  - Sistem informasi adalah
  - Pihak internal yang dimaksud adalah biro/unit/jurusan yang berada di ITS.
- Dokumen terkait**
  - Format surat permohonan pembuatan sistem informasi.
  - Form permintaan pembuatan/pemutakhiran sistem informasi dari Pusat Layanan.
  - Format baku standarisasi dokumentasi proses pembuatan SI.
- Rincian Prosedur**

| NO | ENTITAS              | AKTIVITAS                                                                                                                                                       |
|----|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Desainer SI          | - Menerima hasil analisis terhadap sistem informasi yang akan dibuat/dimutakhirkan.<br>- Membuat desain sistem informasi dari hasil analisis.                   |
| 2. | <i>Programmer</i> SI | - Membuat sistem informasi berdasarkan desain yang telah dibuat.<br>- Melakukan verifikasi dan validasi program yang telah dibuat hingga sesuai dengan harapan. |
| 3. | Dokumentator SI      | Mendokumentasikan proses pembuatan SI dengan format yang telah ditetapkan.                                                                                      |
- Diagram Alir**  
Terlampir.
- Record/Catatan Mutu**  
Dokumentasi proses pembuatan *software*.

Gambar F.140 Prosedur Pemutakhiran/Perbaikan Sistem Informasi

|                                                                                   |                                   |                                 |
|-----------------------------------------------------------------------------------|-----------------------------------|---------------------------------|
|  | PROSEDUR OPERASIONAL BAKU         | Tanggal terbit : 2 Oktober 2014 |
|                                                                                   | PROSES PENGUJIAN SISTEM INFORMASI | Halaman : 2 dari 4              |

- Tujuan**  
Menjelaskan prosedur proses pengujian sistem informasi.
- Ruang Lingkup**  
Mengatur proses pengujian sistem informasi hasil pengembangan sebelum diserahkan pada pengguna layanan (us LPTSI yang bersangkutan, terutama dari pihak internal ITS).
- Definisi**
  - Sistem informasi adalah aplikasi yang dibuat untuk mempermudah dan mengintegrasikan pekerjaan yang bersifat manual menjadi terkomputerisasi sehingga menghasilkan informasi yang dibutuhkan.
  - Pihak internal yang dimaksud adalah biro/unit/jurusan yang berada di ITS.
- Dokumen terkait**
  - Manual instalasi sistem pada server miniatur.
  - Manual pengujian sistem informasi.
  - Form permintaan pengujian sistem informasi.
- Rincian Prosedur**

| NO | ENTITAS       | AKTIVITAS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Programmer SI | <ul style="list-style-type: none"> <li>Menyediakan sistem informasi yang akan di uji coba.</li> <li>Melakukan instalasi sistem yang akan diuji coba pada server miniatur LPTSI.</li> </ul>                                                                                                                                                                                                                                                                                                       |
| 2. | Tim Penguji   | <ul style="list-style-type: none"> <li>Melakukan proses pengujian pertama pada sistem, yakni melakukan pengujian <i>function</i>, <i>accessability</i>, <i>user management</i>, dan <i>usability</i>.</li> <li>Jika ada masalah pada sistem, tim harus melaporkan pada <i>programmer</i> untuk direvisi.</li> <li>Jika sistem berjalan sesuai harapan, maka proses uji coba dilanjutkan oleh <i>user</i>.</li> </ul>                                                                             |
| 3. | User          | <ul style="list-style-type: none"> <li>Melakukan proses pengujian kedua pada sistem, yakni melakukan pengujian <i>function</i>, <i>accessability</i>, <i>user management</i>, dan <i>usability</i>.</li> <li>Jika ada masalah pada sistem, <i>user</i> harus melaporkan pada <i>programmer</i> untuk direvisi.</li> <li>Jika sistem berjalan sesuai harapan, maka <i>user</i> harus memberikan konfirmasi kepada pihak Pusat Pengembangan bahwa sistem sudah berjalan sesuai harapan.</li> </ul> |
| 4. | Programmer SI | Melakukan revisi pada sistem yang diuji coba.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Gambar F.141 Prosedur Proses Pengujian Sistem Informasi

|                                                                                     |                                   |                                 |
|-------------------------------------------------------------------------------------|-----------------------------------|---------------------------------|
|  | POB-TSI.SIM-04                    | Revisi : 01                     |
|                                                                                     | PROSEDUR OPERASIONAL BAKU (POB)   | Tanggal terbit : 2 Oktober 2014 |
|                                                                                     | PROSES INSTALASI SISTEM INFORMASI | Halaman : 2 dari 3              |

- Tujuan**  
Menjelaskan proses instalasi sistem informasi, yang telah selesai diuji coba, ke server ITS.
- Ruang Lingkup**  
Mengatur prosedur instalasi sistem informasi ke server ITS. Sistem informasi yang akan diinstal harus terlebih dahulu melalui prosedur uji cobanya.
- Definisi**  
Sistem informasi adalah aplikasi yang dibuat untuk mempermudah dan mengintegrasikan pekerjaan yang bersifat manual menjadi terkomputerisasi sehingga menghasilkan informasi yang dibutuhkan.
- Dokumen terkait**
  - Format surat permohonan pembuatan sistem informasi oleh unit.
  - Format baku standarisasi dokumentasi proses pembuatan SI.
- Rincian Prosedur**

| NO | ENTITAS                   | AKTIVITAS                                                                                                                                                                                                                                         |
|----|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Unit/Jurusan              | Setelah melakukan uji coba dengan baik, unit/jurusan terkait segera memberi konfirmasi kepada Kepala Pusat Pengembangan bahwa sistem informasi baru telah lulus uji.                                                                              |
| 2. | Kepala Pusat Pengembangan | <ul style="list-style-type: none"> <li>Melakukan verifikasi terhadap sistem informasi baru beserta kelengkapan dokumennya.</li> <li>Mengirim permintaan ijin pada Subbag Jaringan untuk instalasi sistem informasi baru ke server ITS.</li> </ul> |
| 3. | Staf PusBang              | <ul style="list-style-type: none"> <li>Melakukan registrasi sistem informasi baru pada <i>database software</i>.</li> <li>Melakukan proses instalasi sistem informasi baru ke server ITS setelah mendapat ijin dari Subbag Jaringan.</li> </ul>   |
- Diagram Alir**  
Terlampir
- Record/Catatan Mutu**

Gambar F.142 Prosedur Proses Instalasi Sistem Informasi





|                                               |                                 |
|-----------------------------------------------|---------------------------------|
| POB-TSI.YAN-08                                | Revisi : 01                     |
| PROSEDUR OPERASIONAL BAKU (POB)               | Tanggal terbit : 2 Oktober 2014 |
| LAYANAN SOSIALISASI SISTEM INFORMASI (INTERN) | Halaman : 2 dari 4              |

#### 1. Tujuan

Membuat pelayanan penyelenggaraan kegiatan sosialisasi sistem informasi baru yang telah dibuat dan diuji coba, sebelum nantinya diaplikasikan/digunakan secara penuh.

#### 2. Ruang Lingkup

Mengatur proses pelayanan sosialisasi sistem informasi baru maupun lama untuk memaksimalkan pengguna Peserta dalam kegiatan sosialisasi ini adalah penggunasistem informasi baruyang berasal dari unit/jurusan terkait.

#### 3. Definisi

Sistem informasi adalah suatu sistem yang berisi kumpulan informasi yang diperlukan bagi elemen terkait.

#### 4. Dokumen terkait

Format surat permohonan sosialisasi sistem informasi.

#### 5. Rincian Prosedur

| NO | ENTITAS                     | AKTIVITAS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Unit/Jurusan<br><br>PusBang | Mengajukan surat permintaan penyelenggaraan sosialisasi sistem informasi tertentu ditujukan kepada Ketua LPTSI ITS.<br>Mengirimkan pemberitahuan penyelesaian aplikasi sistem informasi baru, beserta permintaan untuk segera mengadakan sosialisasi kepada unit/jurusan terkait.                                                                                                                                                                                                                                                              |
| 2. | Service Desk LPTSI          | Melakukan validasi surat, dan meneruskan ke Ketua LPTSI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 3. | Ketua LPTSI                 | Melakukan evaluasi terhadap permintaan unit/jurusan, apakah permintaan tersebut dinilai mendesak atau tidak. Bila mendesak, permintaan akan dimasukkan daftar prioritas sosialisasi sistem informasi. Apabila dinilai tidak mendesak, maka permintaan tersebut akan dimasukkan daftar antrian sosialisasi sistem informasi.                                                                                                                                                                                                                    |
| 4. | Koordinator Pusat Pelayanan | - Membuat proposal kegiatan sosialisasi sistem informasi berdasarkan daftar prioritas atau daftar antrian sosialisasi sistem informasi<br>- Membentuk panitia pelaksana.                                                                                                                                                                                                                                                                                                                                                                       |
| 5. | Ketua LPTSI                 | Melakukan evaluasi dan persetujuan terhadap proposal kegiatan sosialisasi sistem informasi.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| 6. | Panitia Pelaksana           | - Mempersiapkan kegiatan, yakni berupa penyiapan materi dan pemateri, peserta kegiatan, tempat kegiatan, konsumsi, dan lain-lain yang terkait dengan berlangsungnya kegiatan.<br>- Melaksanakan kegiatan, yakni berupa pelaksanaan dan kontrol selama kegiatan berlangsung.<br>- Melakukan evaluasi kegiatan, berupa kekurangan atau masukan untuk kegiatan selanjutnya.<br>- Menyampaikan evaluasi terhadap sistem informasi yang telah didapat dari peserta selama berlangsungnya acara. Evaluasi ini disampaikan kepada Pusat Pengembangan. |
| 7. | Koordinator Pusat Pelayanan | Menyusun laporan kegiatan untuk dilaporkan kepada Ketua LPTSI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 8. | Ketua LPTSI                 | Melakukan evaluasi terhadap laporan kegiatan.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

Gambar F.143 Prosedur Layanan Sosialisasi Sistem Informasi (Intern)



|                                        |                                 |
|----------------------------------------|---------------------------------|
| POB-TSI.SIM-01                         | Revisi : 01                     |
| PROSEDUR OPERASIONAL BAKU (POB)        | Tanggal terbit : 2 Oktober 2014 |
| PROSES PEMBUATAN SISTEM INFORMASI BARU | Halaman : 2 dari 4              |

#### 1. Tujuan

Menjelaskan proses pembuatan sistem informasi baru.

#### 2. Ruang Lingkup

Mengatur proses pembuatan sistem informasi yang diminta oleh pengguna layanan (*user*) LPTSI, terutama dari internal ITS.

#### 3. Definisi

- Sistem informasi adalah aplikasi yang dibuat untuk mempermudah dan mengintegrasikan pekerjaan yang bersifat manual menjadi terkomputerisasi sehingga menghasilkan informasi yang dibutuhkan.
- Pihak internal yang dimaksud adalah biro/unit/jurusan yang berada di ITS.

#### 4. Dokumen terkait

- Format surat permohonan pembuatan sistem informasi.
- Form permintaan pembuatan sistem informasi dari Pusat Layanan.
- Format baku standarisasi dokumentasi proses pembuatan SI.

#### 5. Rincian Prosedur

| NO | ENTITAS             | AKTIVITAS                                                                                                                                                                                                                                                                                                                                                                            |
|----|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Desainer SI         | - Menerima hasil analisis terhadap sistem informasi yang akan dibuat/dimutakhirkan<br>- Membuat desain sistem informasi dari hasil analisis.                                                                                                                                                                                                                                         |
| 2. | Koordinator PusBang | - Melakukan analisis sumber daya yang diperlukan. Jika dirasa tidak cukup, akan dipertimbangkan untuk melakukan pembelian<br>- Melakukan perencanaan proyek pembuatan sistem informasi baru, meliputi SDM, jadwal kegiatan ( <i>gantchart</i> ), dan anggaran<br>- Menjalankan proyek pembuatan sistem informasi baru beserta anggota proyek yang telah ditentukan pada perencanaan. |
| 3. | Programmer SI       | Membuat sistem informasi berdasarkan <i>user requirements</i> dan desain yang telah dibuat.                                                                                                                                                                                                                                                                                          |
| 4. | Dokumentator SI     | Mendokumentasikan proses pembuatan SI dengan format yang telah ditetapkan.                                                                                                                                                                                                                                                                                                           |
| 5. | Koordinator PusBang | Melakukan <i>monitoring</i> dan <i>control</i> terhadap jalannya proyek, serta melakukan perbaikan/evaluasi bila diperlukan.                                                                                                                                                                                                                                                         |
| 6. | Programmer SI       | Melakukan verifikasi dan validasi program yang telah dibuat hingga sesuai dengan harapan.                                                                                                                                                                                                                                                                                            |

Gambar F.144 Prosedur Proses Pembuatan Sistem Informasi Baru

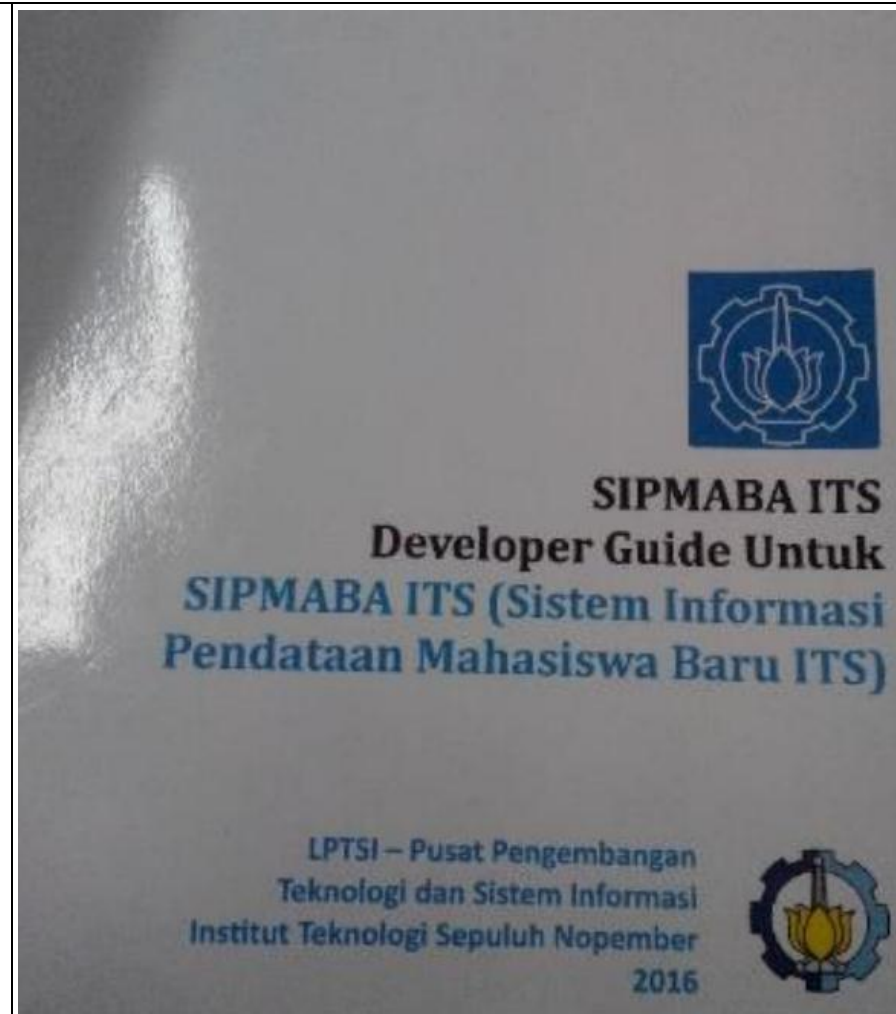


# OFFICE 365 ADMINISTRATION GUIDE

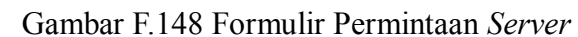
**Antonius D Simamora**

System Engineer | PT. Pasifik Cipta Mandiri  
Agustus 2016

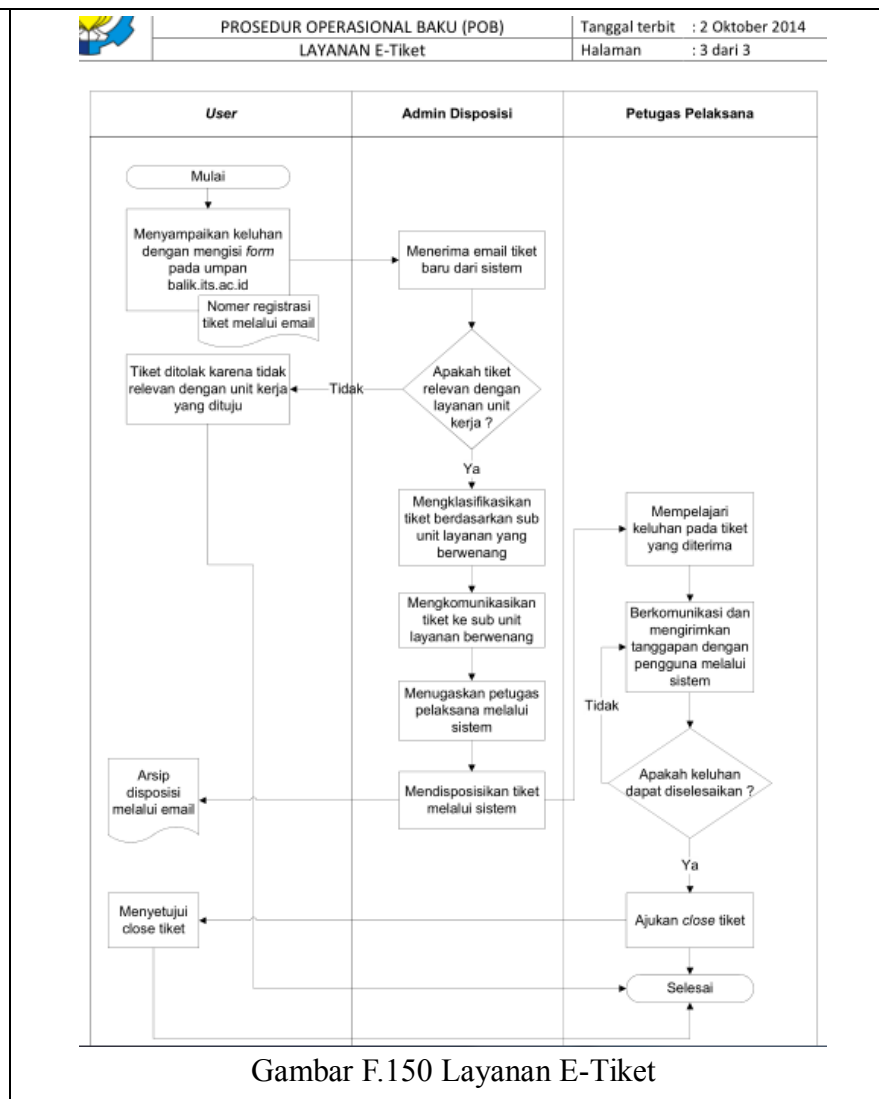
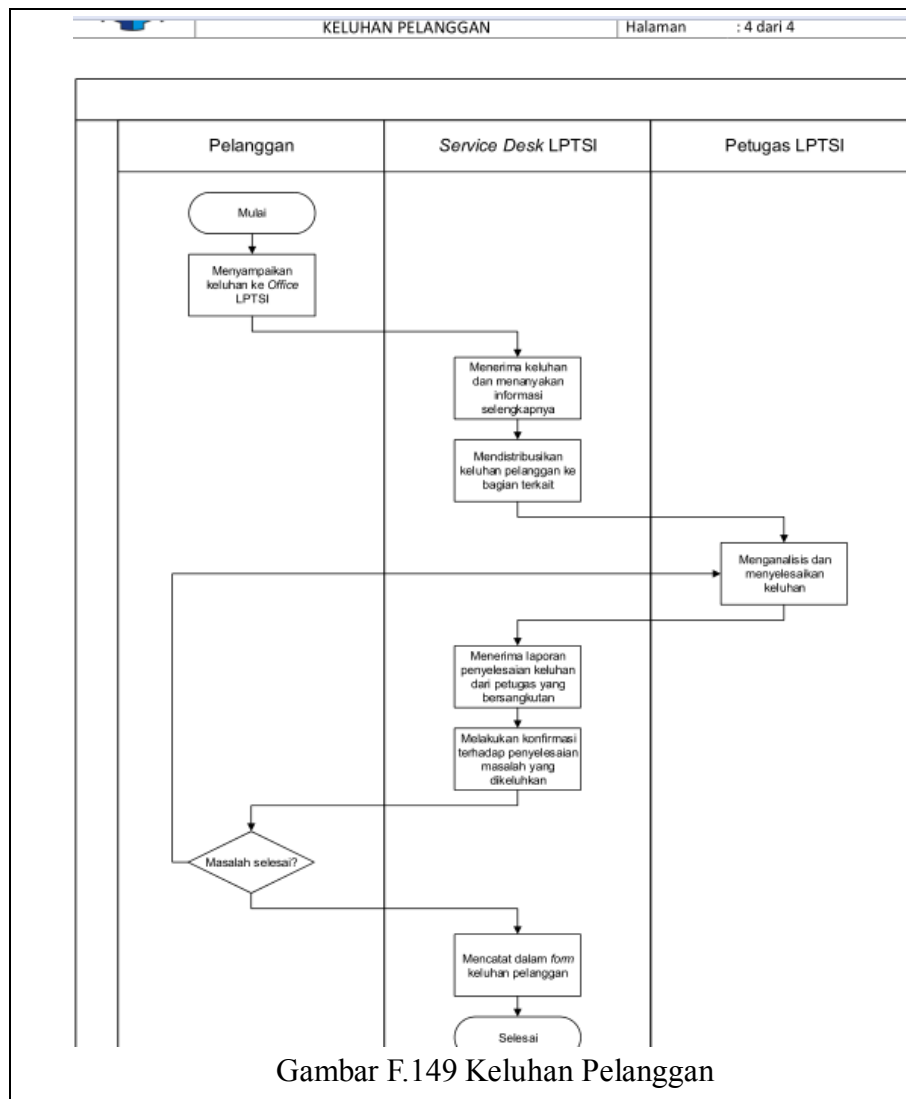
Gambar F.145 *User Guide*

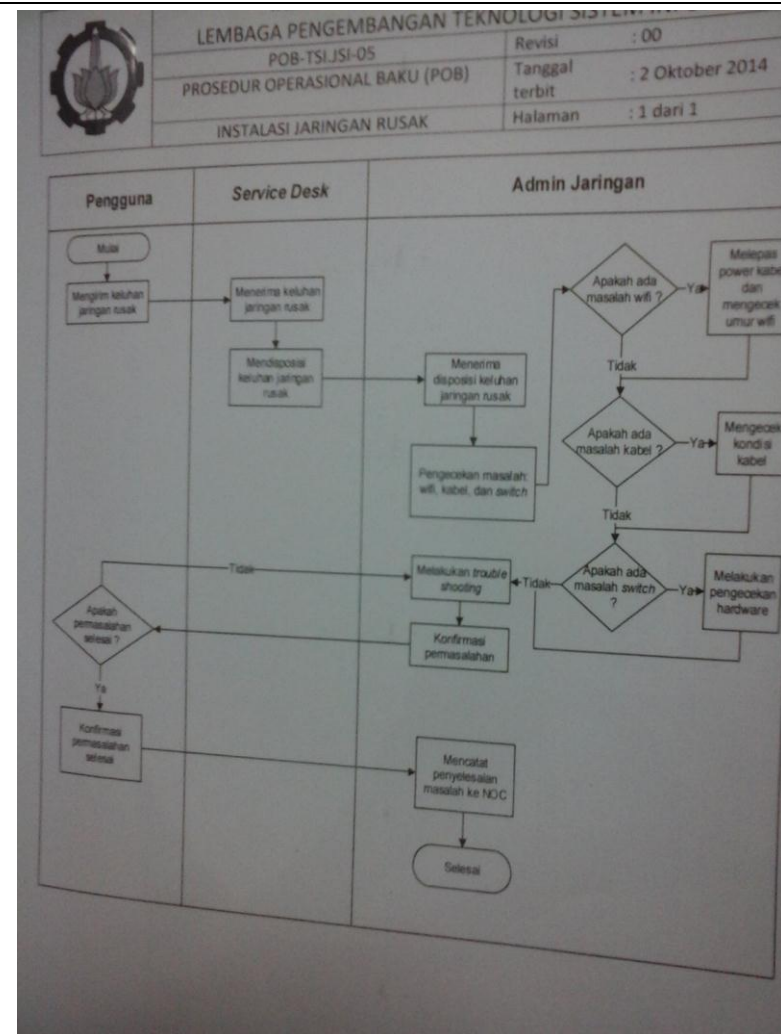
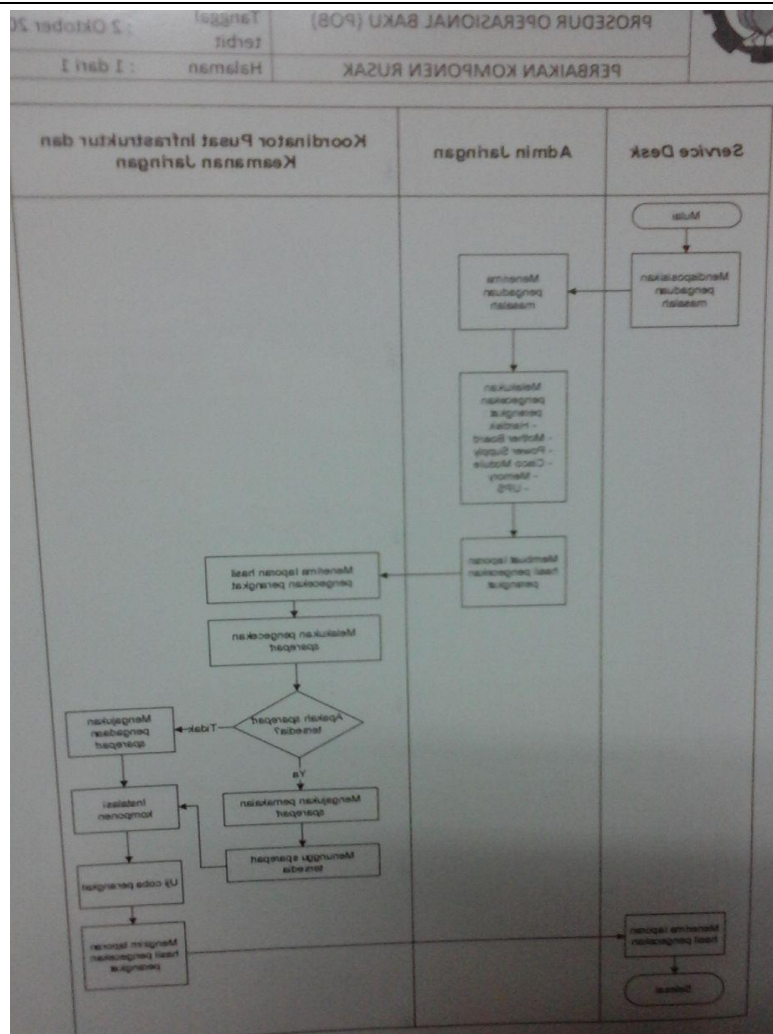


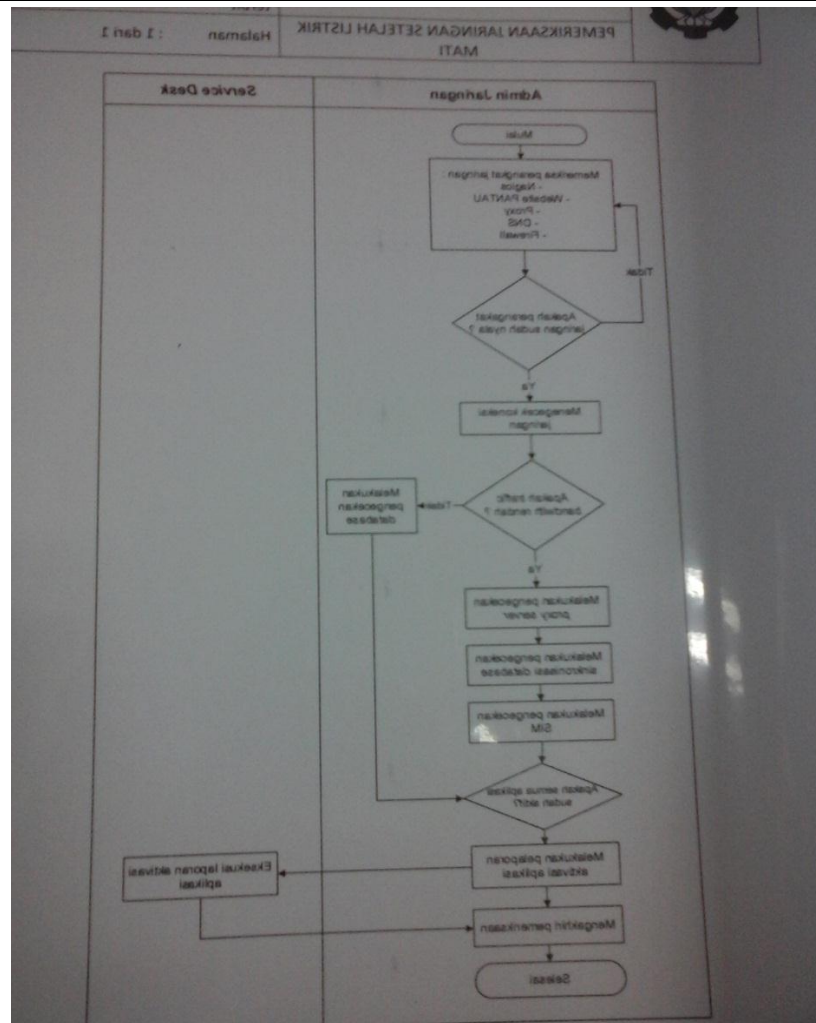
Gambar F.146 *Developer Guide*











Gambar F.153 Prosedur Pemeriksaan Jaringan Setelah Listrik Mati



Gambar F.154 Halaman Awal Umpan Balik (E-Tiket)



Institut  
Teknologi  
Sepuluh Nopember

### Input Umpan Balik

**Subject**

**Nama**

**Email**  
  
\*harus menggunakan email @its.ac.id

**Posmail**

**Layanan**

**Pesan**  

A Normal text =

Bold

Italic

Underline

**Prioritas**  
☒ **Low**
☐ **Medium**
☐ **Hardcore**

**Attachment File**  
 No file selected.  
 No file selected.  
 No file selected.  
format file \* ( .jpg , .png , .bmp , .doc , .xls , .pdf )

**Security Question : Hitunglah !**  
3 + 3 =

### Pencarian Nomer Tiket

### SERVICE DESK LPTSI



031-5947270  
PABX : 1132

Gambar F.155 Halaman Isi Keluhan Umpan Balik (E-Tiket)

## DAFTAR DOKUMEN EKSTERNAL

BAGIAN : LPTSI

TANGGAL : 2 Oktober 2014

| No. | SPESIFIKASI                                         | PENERBIT DOKUMEN | TAHUN | NO.REG | PARAF MR |
|-----|-----------------------------------------------------|------------------|-------|--------|----------|
| 1   | Peraturan Presiden RI no:70 Tahun 2012              | Softcopy         | 2012  |        |          |
| 2   | Petunjuk Penggunaan Aplikasi Pajak Honorarium       | BAUK ITS         | 2010  |        |          |
| 3   | Sosialisasi RBA Dalam Rangka Revisi RBA 2010        | BAUK ITS         | 2010  |        |          |
| 4   | PO Pendapatan & Pengelolaan Dana PNB BLU ITS        | BPP              | 2013  |        |          |
| 5   | Revisi PO Pendapatan & Pengelolaan Dana PNB BLU ITS | BPP              | 2014  |        |          |

Gambar F.156 Daftar Dokumen Eksternal

[Home](#)
[Tentang Unduh](#)
[Cara Download](#)
[Cara Aktivasi](#)

[Cari](#)


[LOGIN](#)


[Products](#)
[Solutions](#)
[Academia](#)
[Support](#)
[Community](#)
[Events](#)
[Company](#)

# MATLAB

MAJOR UPDATE

[Overview](#)
[Features](#)
[Code Examples](#)
[Videos](#)
[Webinars](#)
[What's New](#)
[Product Pricing](#)

[Trial software](#)
[Contact sales](#)

## The Language of Technical Computing

Millions of engineers and scientists worldwide use MATLAB® to analyze and design the systems and products transforming our world. MATLAB is in automobile active safety systems, interplanetary spacecraft, health monitoring devices, smart power grids, and LTE cellular networks. It is used for machine learning, signal processing, image processing, computer vision, communications, computational finance, control design, robotics, and much more.

**Math. Graphics. Programming.**

The MATLAB platform is optimized for solving engineering and scientific problems. The matrix-based MATLAB language is the world's most natural way to express



## Produk Lisensi

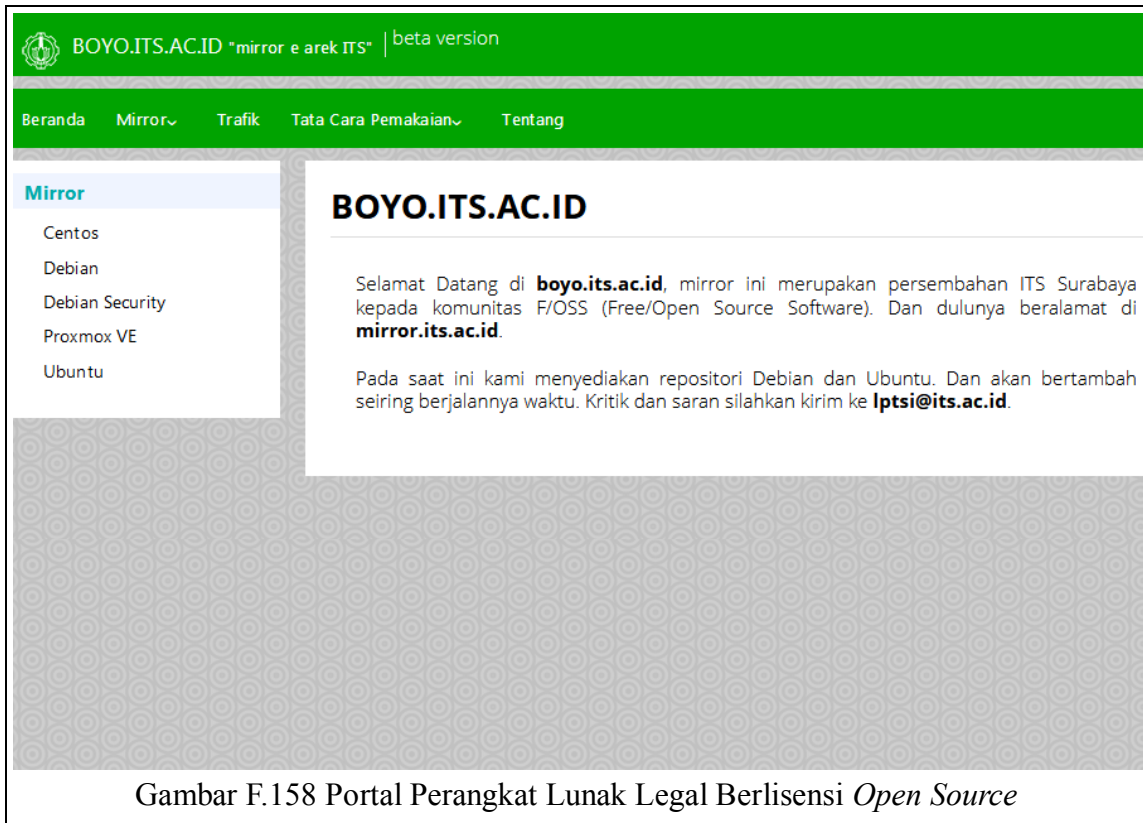






Gambar F.157 Portal Perangkat Lunak Legal Berlisensi *Full Version*







PROSEDUR OPERASIONAL BAKU (POB)  
LAYANAN PENYEDIAAN LEGAL SOFTWARE

Tanggal terbit : 2 Oktober 2014  
Halaman : 2 dari 4

1. Tujuan

Mengatur ketentuan-ketentuan terkait layanan *legal software*.

2. Ruang Lingkup

Mengatur proses layanan penyediaan *legal software*, yang meliputi proses analisis kebutuhan, pembelian, dan pengunggahan ke *server* ITS.

3. Definisi

*Legal software* merupakan segala perangkat lunak resmi yang disediakan oleh ITS untuk kebutuhan civitas akademik

4. Dokumen terkait

Form kebutuhan *software*

5. Rincian Prosedur

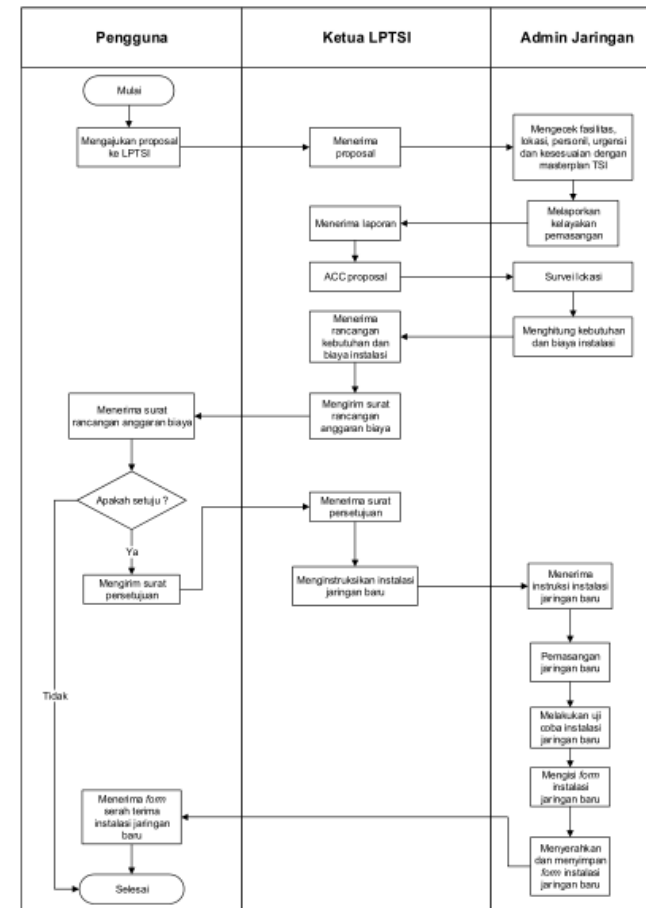
| NO | ENTITAS                   | AKTIVITAS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | Unit/Jurusan              | - Masing-masing unit/jurusan memberikan daftar kebutuhan <i>software</i> beserta spesifikasinya ke Ketua Pusat Layanan LPTSI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| 2. | Koordinator Pusat Layanan | - Mengumpulkan daftar <i>software</i> yang menjadi kebutuhan dari semua unit di ITS, baik yang baru maupun yang perlu pembaruan lisensi. Pengumpulan juga dapat dilakukan dengan meminta masing-masing unit untuk mengirimkan daftar kebutuhan <i>software</i> beserta spesifikasinya.<br>- Melakukan analisis spesifikasi dan harga <i>software</i> , sekaligus melakukan pencarian penawaran yang berkaitan dengan <i>software-software</i> tersebut.<br>- Membuat/menyusun daftar prioritas <i>software</i> yang akan dibeli.<br>- Memeriksa anggaran yang ada. Jika tidak mencukupi, harus dilakukan lagi analisis untuk mengurangi jumlah pengeluaran.<br>- Jika anggaran tercukupi, maka proposal pengadaan dibuat, kemudian diteruskan pada Ketua LPTSI. |
| 3. | Ketua LPTSI               | Melakukan evaluasi terhadap proposal pengadaan. Apakah dinilai boleh atau tidak untuk dikerjakan. Jika:<br>- Boleh, Ketua LPTSI mengirimkan surat permintaan pengadaan <i>software</i> ke Unit Layanan Pengadaan.<br>- Tidak, maka proposal harus direvisi berdasarkan rekomendasi Ketua LPTSI.                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 4. | Unit Layanan Pengadaan    | Melakukan proses pengadaan (pembelian).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 5. | Panitia Penerima Software | - Melakukan pemeriksaan terhadap <i>software</i> yang baru dibeli sebelum diputuskan untuk dipakai/diterima. Jika <i>software</i> yang bersangkutan tidak sesuai dengan harapan, maka dikembalikan pada ULP.<br>- <i>Software</i> yang sesuai akan dilakukan penerimaan secara legal/resmi.                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| 6. | Subbag Jaringan           | Menerima <i>software</i> yang telah diterima secara resmi, dan melakukan pengunggahan ke <i>server</i> ITS.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Gambar F.159 Prosedur Layanan Penyediaan Legal Software



PROSEDUR OPERASIONAL BAKU (POB)  
INSTALASI JARINGAN BARU

Tanggal terbit : 7 Januari 2013  
Halaman : 1 dari 1



Gambar F.160 Prosedur Instalasi Jaringan Baru

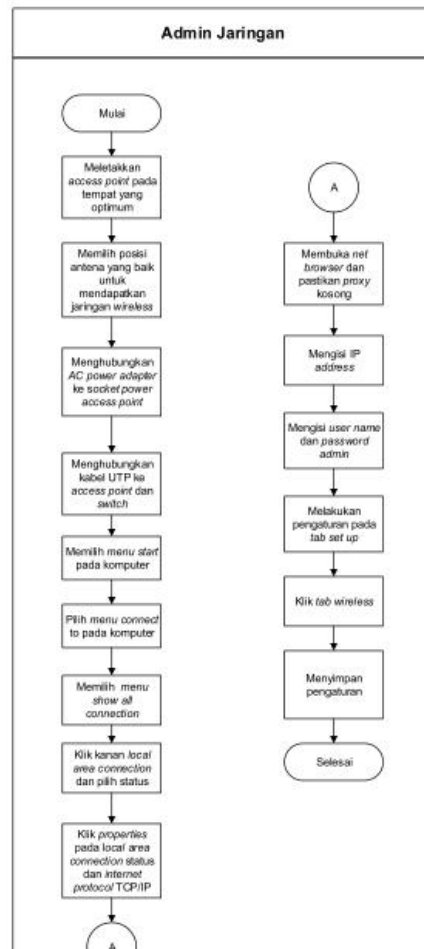


PROSEDUR OPERASIONAL BAKU (POB)

Tanggal terbit : 7 Januari 2013

INSTALASI ACCESS POINT

Halaman : 1 dari 1



Gambar F.161 Instalasi Access Point

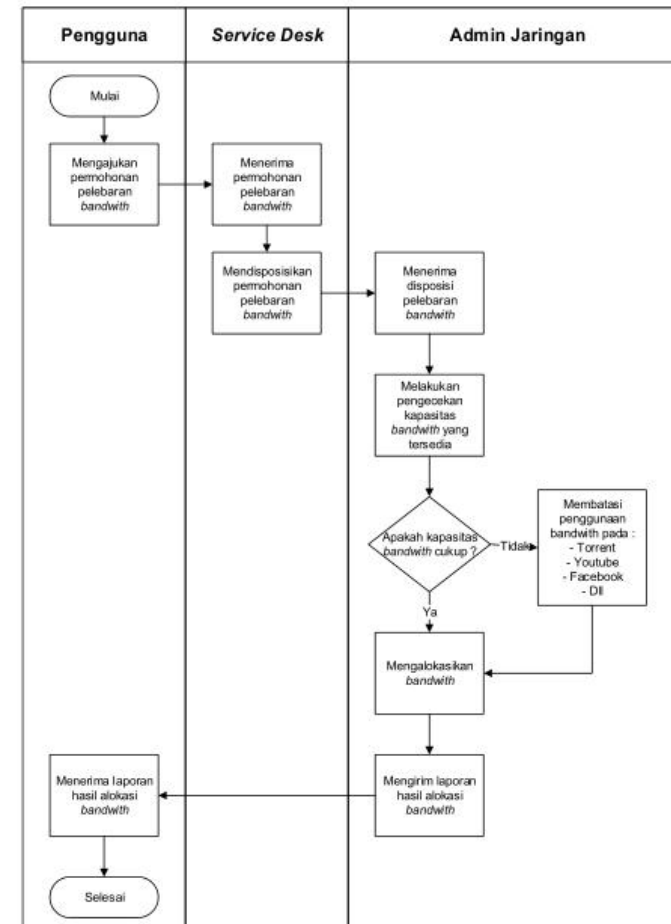


PROSEDUR OPERASIONAL BAKU (POB)

Tanggal terbit : 7 Januari 2013

PELEBARAN BANDWIDTH

Halaman : 1 dari 1



Gambar F.162 Prosedur Pelebaran Bandwidth



|  |                                     | <b>SASARAN MUTU</b>                                                               |               |                                                                  | Tanggal Terbit : 7 Januari 2014 |                                          |
|-----------------------------------------------------------------------------------|-------------------------------------|-----------------------------------------------------------------------------------|---------------|------------------------------------------------------------------|---------------------------------|------------------------------------------|
|                                                                                   |                                     |                                                                                   |               |                                                                  | Halaman : 1 dari 2              |                                          |
| NO                                                                                | SASARAN MUTU                        | KRITERIA KEBERHASILAN                                                             | TARGET        | METODE PENGKURAN                                                 | ALAT UKUR                       | PENANGGUNG JAWAB                         |
| <b>PUSAT PENGELOLAAN DAN LAYANAN TIK</b>                                          |                                     |                                                                                   |               |                                                                  |                                 |                                          |
| 1                                                                                 | Proses pembuatan Domain dan Hosting | Lama waktu mulai dari permintaan sampai dengan penyerahan akun domain dan hosting | 1 hari kerja  | (Waktu penyerahan – Waktu masuk permintaan)                      | Pencatatan melalui NOC          | Koord. Pusat Pengelolaan dan Layanan TIK |
| <b>PUSAT PENGEMBANGAN SIM</b>                                                     |                                     |                                                                                   |               |                                                                  |                                 |                                          |
| 2                                                                                 | Pengembangan SIM                    | Prosentase penyelesaian                                                           | 100%          | (Jumlah modul yang selesai / Jumlah seluruh target modul) X 100% | Uji Coba SIM                    | Koord. Pusat Pengembangan SIM            |
| 3                                                                                 | Dokumentasi SIM                     | Prosentase penyelesaian                                                           | 100%          | (Jumlah selesai / Jumlah target) X 100%                          | File Dokumentasi                | Koord. Pusat Pengembangan SIM            |
| 4                                                                                 | Backup SIM                          | Frekuensi Back up                                                                 | Sesuai jadwal | Membandingkan kesesuaian jadwal back up dengan pelaksanaan       | Jadwal Backup per Tahun         | Koord. Pusat Pengembangan SIM            |
| 5                                                                                 | Backup Database                     | Frekuensi Back up                                                                 | Sesuai jadwal | Membandingkan kesesuaian jadwal back up dengan pelaksanaan       | Jadwal Backup per Tahun         | Koord. Pusat Pengembangan SIM            |
| <b>PUSAT DATA DAN PELAPORAN</b>                                                   |                                     |                                                                                   |               |                                                                  |                                 |                                          |
| 6                                                                                 | Pemenuhan Permintaan Data           | Ketepatan waktu                                                                   | 3 hari kerja  | waktu pemenuhan data – waktu permintaan data                     | list kebutuhan data             | Koord. Pusat Data dan Pelaporan          |
| 7                                                                                 | Pelaporan PDPT DIKTI                | Ketepatan waktu                                                                   | 7 hari kerja  | waktu pemenuhan data – waktu permintaan data                     | list kebutuhan data             | Koord. Pusat Data dan Pelaporan          |

Gambar F.163 Sasaran Mutu

|  |                                                   | <b>SASARAN MUTU</b>        |                                                 |                                                                     | Tanggal Terbit : 7 Januari 2014 |                                                 |
|-----------------------------------------------------------------------------------|---------------------------------------------------|----------------------------|-------------------------------------------------|---------------------------------------------------------------------|---------------------------------|-------------------------------------------------|
|                                                                                   |                                                   |                            |                                                 |                                                                     | Halaman : 2 dari 2              |                                                 |
| NO                                                                                | SASARAN MUTU                                      | KRITERIA KEBERHASILAN      | TARGET                                          | METODE PENGKURAN                                                    | ALAT UKUR                       | PENANGGUNG JAWAB                                |
| 8                                                                                 | Pengumpulan Data                                  | Ketepatan waktu            | 3 x 7 hari Kerja                                | (waktu pemenuhan data) – (waktu permintaan data)                    | list kebutuhan data             | Koord. Pusat Data dan Pelaporan                 |
| 9                                                                                 | Proses validasi data                              | Ketepatan waktu            | 7 hari kerja                                    | (waktu menyelesaikan validasi data) – (waktu memulai validasi data) | rencana kegiatan                | Ketua Lembaga                                   |
| 10                                                                                | Pengukuran Tingkat Kepuasan Stakeholder ITS       | Jumlah responden           | 15% dari jumlah populasi masing-masing kelompok | (Jumlah responden aktual / Jumlah target sampel) X 100%             | Rekapitulasi Kuisioner          | Koord. Pusat Data dan Pelaporan                 |
| 11                                                                                | Pengukuran Tingkat Kepuasan Stakeholder ITS       | Tingkat Kepuasan (skala 4) | 3,6                                             | Skala Kepuasan 1 - 4                                                | Rekapitulasi Kuisioner          | Koord. Pusat Data dan Pelaporan                 |
| <b>PUSAT INFRASTRUKTUR DAN KEAMANAN INFORMASI</b>                                 |                                                   |                            |                                                 |                                                                     |                                 |                                                 |
| 12                                                                                | Keluhan Layanan Sistem Jaringan                   | Lama Waktu Penanganan      | 1 hari kerja                                    | (waktu penyelesaian) - (waktu keluhan diterima)                     | Pencatatan melalui NOC          | Koord. Pusat Infrastruktur & Keamanan Informasi |
| 13                                                                                | Ketersediaan Sistem Backup Power (UPS dan Genset) | % Ketersediaan             | 95%                                             | (Lama waktu suplai listrik down/Total waktu layanan 1 tahun) X 100% | Pencatatan melalui NOC          | Koord. Pusat Infrastruktur & Keamanan Informasi |
| Dibuat Oleh :                                                                     |                                                   |                            | Disetujui Oleh :                                |                                                                     |                                 |                                                 |
|                                                                                   |                                                   |                            |                                                 |                                                                     |                                 |                                                 |

Gambar F.164 Sasaran Mutu (lanj.)

**Subject:** Undelivered Mail Returned to Sender  
**From:** "Mail Delivery System" <MAILER-DAEMON@gemini.its.ac.id>  
**Date:** Thu, October 26, 2017 15:23  
**To:** widya@its.ac.id  
**Priority:** Normal  
**Options:** [View Full Header](#) | [View Printable Version](#) | [Download this as a file](#) | [View](#)

This is the mail system at host gemini.its.ac.id.

I'm sorry to have to inform you that your message could not be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to postmaster.

If you do so, please include this problem report. You can delete your own text from the attached returned message.

The mail system

```
<pengujianalamatemailsalah@gmail.com>: host
gmail-smtp-in.l.google.com[2404:6800:4003:c03::1a] said: 550-5.1.1 The
email account that you tried to reach does not exist. Please try 550-5.1.1
double-checking the recipient's email address for typos or 550-5.1.1
unnecessary spaces. Learn more at 550 5.1.1
https://support.google.com/mail/?p=NoSuchUser 137si3047633pgd.45 - gsmt
(in reply to RCPT TO command)
```

Gambar F.165 Informasi Gagal Mengirimkan *Email* (Layanan *Email* Mandiri)

 **Mail Delivery Subsystem** <mailer-daemon@googlemail.com>  
to me ▾



### Address not found

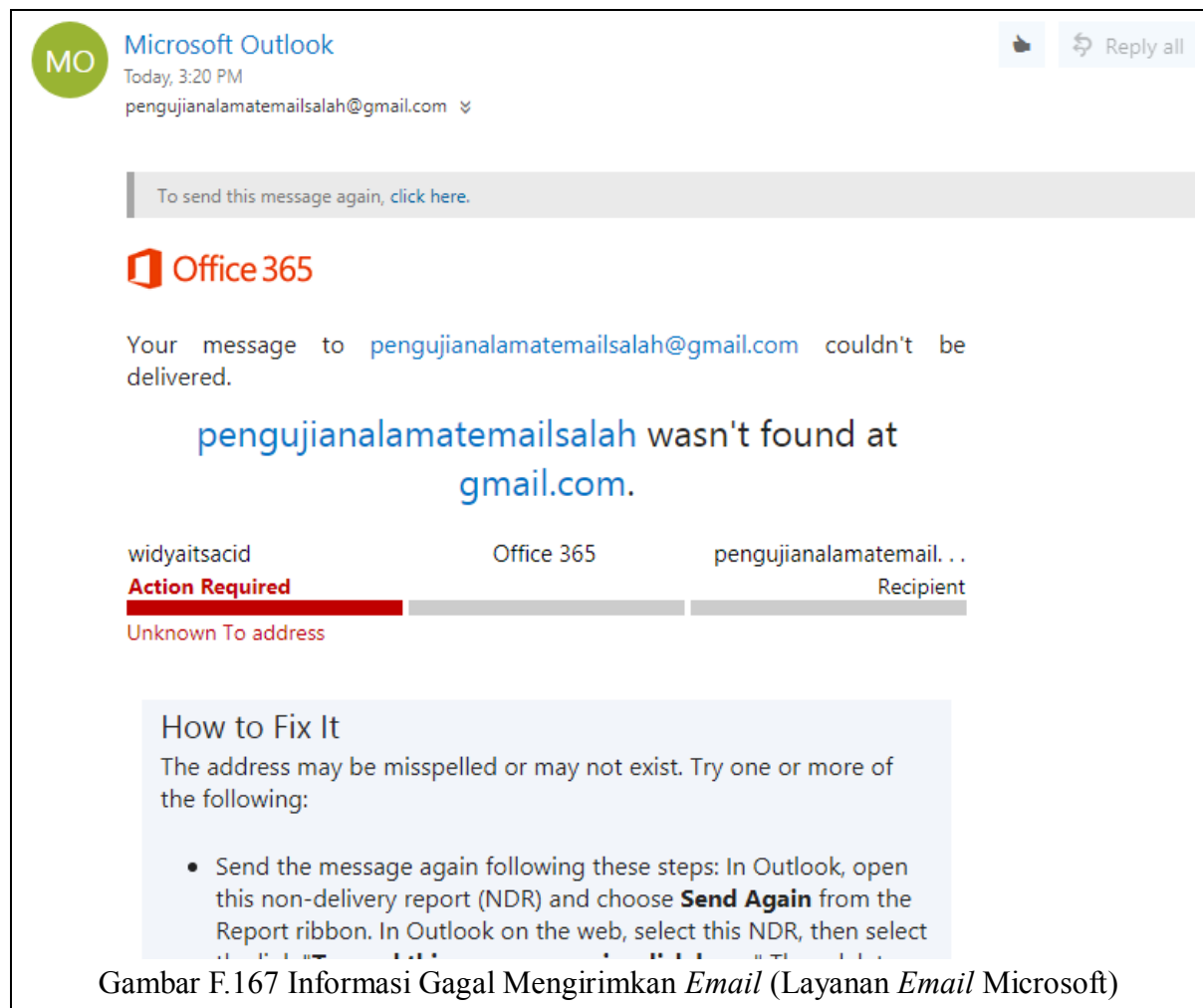
Your message wasn't delivered to **pengujianalamatemailsalah@gmail.com** because the address couldn't be found. Check for typos or unnecessary spaces and try again.

[LEARN MORE](#)

The response was:

```
550-5.1.1 The email account that you tried to reach does not exist. Please try 550
address for typos or 550-5.1.1 unnecessary spaces. Learn more at 550 5.1.1 https://su
s66sor1378896oih.128 - gsmt
```

Gambar F.166 Informasi Gagal Mengirimkan *Email* (Layanan *Email* Google)



Direktorat Pengembangan Teknologi Sistem Informasi ITS  
**RUANG LINGKUP SISTEM MANAJEMEN  
KEAMANAN INFORMASI**

|                |                                                                  |
|----------------|------------------------------------------------------------------|
| Nama Dokumen   | Dokumen Ruang Lingkup Sistem Manajemen Keamanan Informasi (SMKI) |
| Versi          | 1                                                                |
| Tanggal        | 28/10/2017                                                       |
| Dibuat oleh    | Furqon Mauladani                                                 |
| Disetujui oleh |                                                                  |

## **1. Tujuan**

Tujuan dari dokumen ini adalah menjelaskan secara rinci mengenai ruang lingkup dan batasan penerapan SMKI pada DPTSI-ITS.

## **2. Ruang Lingkup**

### **2.1. Karakteristik Bisnis**

Karakteristik atau proses bisnis dari organisasi adalah sebagai berikut:

- DPTSI bertugas untuk mengelola, mengordinasikan, mengendalikan, dan mengembangkan berbagai fasilitas TIK disekitar lingkungan universitas Institut Teknologi Sepuluh Nopember.
- Layanan *email* ITS digunakan dosen, mahasiswa dan karyawan untuk keperluan berkirim pesan, serta sebagai alat autentikasi ketika menggunakan fasilitas *internet* di area kampus dan berbagai sistem informasi terpadu yang disediakan oleh DPTSI-ITS.
- DPTSI-ITS memiliki 3 bentuk layanan *email* yaitu layanan yang dikelola secara mandiri oleh DPTSI-ITS (<https://webmail.its.ac.id>) yang hanya dapat dipilih oleh karyawan dan dosen, layanan yang bekerjasama dengan Google (<https://mail2.its.ac.id>), dan layanan *email* yang bekerjasama dengan Microsoft (<https://login.microsoftonline.com>) yang khusus untuk pimpinan saja seperti Kasubag/Kasubdit sampai keatas.
- Sebanyak 35 orang yang bekerja di DPTSI-ITS dengan jumlah karyawan pada Subdit Infrastruktur dan Keamanan Teknologi Informasi sebanyak 8 orang, Subdit Pengembangan Sistem Informasi sebanyak 14 orang, dan Subdit Layanan Teknologi dan Sistem Informasi sebanyak 9 orang. Empat

karyawan lainnya adalah Direktur DPTSI-ITS, Sekertaris, Bendahara Pengeluaran Pembantu, dan Pembantu Administrasi Umum.

## **2.2. Departemen/Unit Fungsional**

Ruang lingkup SMKI meliputi beberapa bagian sebagai berikut:

- Pihak manajemen yang terdiri dari Rektor ITS, Direktur DPTSI-ITS dan Kasubdit sebagai perencana, pengorganisasi, pemimpin dan pengendali pelaksanaan aktifitas sehari-hari organisasi.
- Subdirektorat Infrastruktur & Keamanan Informasi yang bertugas terhadap jaringan dan koneksi antara klien/pengguna dengan *server* yang digunakan untuk *email* ITS.
- Subdirektorat Pelayanan Teknologi dan Sistem Informasi yang bertugas terhadap administrasi akun *email* ITS, seperti membuat akun, merubah *password* atau data akun, dan menghapus akun.
- Subdirektorat Pengembangan Sistem Informasi yang bertugas terhadap pengembangan sistem dan antarmuka Webmail ITS.
- Direktorat SDM dan Organisasi bertanggung jawab secara keseluruhan terhadap karyawan di organisasi, termasuk persyaratan perekrutan, pemberian sangsi dan pemberhentian bagi setiap karyawan.
- Bendahara Pengeluaran Pembantu bertanggung jawab terhadap manajemen anggaran belanja secara keseluruhan dalam penerapan SMKI.
- Direktorat Sarana dan Prasarana bertanggung jawab terhadap keamanan fisik dan administrasi umum tempat fisik organisasi.

## **2.3. Topologi Jaringan**

Topologi jaringan yang ada di DPTSI-ITS dapat dilihat pada Gambar 4.9.

## **2.4. Lokasi**

Lokasi dimana SMKI akan dijalankan adalah Direktorat Pengembangan Teknologi dan Sistem Informasi di gedung ITS Research Center, lantai 3, Sukolilo, Surabaya 60111.

## **2.5. Komitmen dan Sumber Daya**

Pihak manajemen berkomitmen dan mendukung dalam penerapan SMKI. Dukungan dapat berupa uang, waktu atau sumber daya lainnya yang dibutuhkan sesuai kebutuhan dan kemampuan DPTSI-ITS.

## 2.6. Pengecualian pada Ruang Lingkup

Pengecualian yang tidak termasuk kedalam ruang lingkup adalah sebagai berikut:

1. Layanan *email* yang dikelola mandiri oleh jurusan/unit lain di ITS ataupun layanan *email* yang bekerjasama dengan Google dan Microsoft.
2. *Server* yang dikelola oleh DPTSI-ITS namun tidak berkaitan dengan *email* ITS, misalnya *website* ITS (<https://its.ac.id>), *website* DPTSI-ITS (<https://dptsi.its.ac.id>), *Integra* ITS (<https://integra.its.ac.id>), *LPSE* (<https://lpse.its.ac.id>) untuk pengadaan barang/layanan secara elektronik yang dimiliki oleh ULP-ITS, *E-Aset* (<https://e-aset.its.ac.id>) untuk inventaris aset BMN yang dimiliki oleh BAUK-ITS, *Umpan Balik/E-Tiket* (<https://umpanbalik.its.ac.id>) untuk pelaporan keluhan yang dimiliki oleh Subdit Pelayanan, portal unduh perangkat lunak (<https://unduh.its.ac.id>), dan lainnya.
3. Perangkat jaringan, *server*, komputer dan aset informasi lainnya yang berada diluar kantor DPTSI-ITS, misalnya yang dipasang disetiap jurusan/unit.

*Halaman ini sengaja dikosongkan*

Direktorat Pengembangan Teknologi Sistem Informasi ITS

# KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI

|                |                                                              |
|----------------|--------------------------------------------------------------|
| Nama Dokumen:  | Dokumen Kebijakan Sistem Manajemen Keamanan Informasi (SMKI) |
| Versi          | 1                                                            |
| Tanggal        | 28/10/2017                                                   |
| Dibuat oleh    | Furqon Mauladani                                             |
| Disetujui oleh |                                                              |

## 1. Pendahuluan

Tujuan dari dokumen ini adalah menunjang tujuan bisnis dengan memastikan *confidentiality*, *integrity*, dan *availability* dari setiap aset informasi yang penting bagi DPTSI-ITS.

## 2. Ruang Lingkup

Kebijakan SMKI melingkupi layanan TIK yang terkait, termasuk (dan tidak terbatas pada) beberapa departemen/unit dan layanan sebagai berikut:

- Subdirektorat Infrastruktur & Keamanan Informasi.
- Subdirektorat Pelayanan Teknologi dan Sistem Informasi.
- Subdirektorat Pengembangan Sistem Informasi.
- Ruang pusat data.
- Webmail ITS.
- Perangkat keras/lunak/jaringan, data, karyawan dan vendor yang berkaitan dengan Webmail ITS.

## 3. Sasaran

Sasaran yang harus dicapai dalam SMKI adalah sebagai berikut:

1. Sasaran dari penerapan SMKI adalah melindungi aset informasi yang dikelola oleh DPTSI-ITS dari segala resiko terkait keamanan informasi yang ada dan mendukung proses bisnis di ITS.
2. Menyediakan pelatihan yang diperlukan kepada karyawan, dosen dan mahasiswa untuk memastikan keamanan informasi.
3. Melakukan penilaian dan penanganan resiko untuk menunjang proses SMKI.



4. Melakukan audit internal dan tinjauan pihak manajemen untuk memastikan penerapan dan kesesuaian SMKI.

#### **4. Hasil yang Diharapkan**

Hasil yang diharapkan dari penerapan SMKI adalah sebagai berikut:

- Terlindunginya aspek *confidentiality*, *integrity* dan *availability* dari keseluruhan aset informasi yang dikelola oleh DPTSI-ITS
- Meningkatkan keamanan, kepercayaan dan kenyamanan pemangku kepentingan di DPTSI-ITS.

#### **5. Peran dan Tanggung Jawab**

Peran dan tanggung jawab pada SMKI adalah sebagai berikut:

1. Pimpinan bertanggung jawab dalam memastikan tersedianya sumber daya yang dibutuhkan SMKI, serta kesesuaian kebijakan dan sasaran keamanan informasi dengan arah strategis organisasi. Selain itu bertugas mengkomunikasikan pentingnya kepatuhan dan mendukung kontribusi setiap pemangku kepentingan terhadap SMKI.
2. Komite pengendali SMKI bertanggung jawab untuk memastikan dan meninjau kesesuaian penerapan dan peningkatan SMKI. Selain itu bertugas menyediakan arahan yang jelas pada strategi SMKI organisasi dalam mengelola keamanan informasi dan mendukung pimpinan untuk mencapai sasaran strategis organisasi.
3. Tim pemimpin SMKI bertanggung jawab dalam merencanakan, mengerakkan, dan mengatur aktifitas yang berkaitan dengan SMKI. Selain itu bertugas mengelola resiko dan beberapa dokumen terkait SMKI.
4. Tim penerapan SMKI bertanggung jawab untuk melakukan dan menerapkan semua aktifitas SMKI yang direncanakan oleh tim pemimpin SMKI.
5. Perlindungan terhadap *confidentiality*, *integrity* dan *avalability* dari setiap aset informasi merupakan tanggung jawab dari pemilik ataupun pengguna pada masing-masing aset.

#### **6. Kebijakan/Dokumen Terkait**

Kebijakan atau dokumen yang terkait dengan dokumen ini adalah sebagai berikut:

1. Dokumen [Ruang Lingkup SMKI] dapat dilihat pada Lampiran G.
2. Susunan tim pengelola SMKI dapat dilihat pada Gambar 4.10.
3. Kriteria resiko dapat dilihat pada Tabel 4.1.

Direktorat Pengembangan Teknologi Sistem Informasi ITS

# PROSES PENILAIAN RESIKO

|                |                                 |
|----------------|---------------------------------|
| Nama Dokumen:  | Laporan Proses Penilaian Risiko |
| Versi          | 1                               |
| Tanggal        | 28/10/2017                      |
| Dibuat oleh    | Furqon Mauladani                |
| Disetujui oleh |                                 |

## 1. Pendahuluan

Tujuan dari dokumen ini adalah mendefinisikan metodologi untuk penilaian risiko keamanan informasi, seperti identifikasi risiko, analisis risiko dan evaluasi risiko berdasarkan dokumen standar SNI ISO/IEC 27005:2013 dan SNI ISO/IEC 27001:2013. Dokumen ini juga melaporkan hasil dari proses penilaian risiko.

## 2. Tahapan Penilaian Risiko

Beberapa tahapan dalam penilaian risiko adalah sebagai berikut:

1. Identifikasi aset yang kritis yang berfungsi sebagai pengolah, pengirim maupun media/penyimpanan informasi, ancaman yang mengganggu aspek keamanan informasi seperti *confidentiality*, *integrity* dan *availability* terhadap aset tersebut, kontrol keamanan pada ketiga area seperti *administrative*, *physical*, dan *technical* yang melindungi aset dari ancaman, dan kerentanan pada keamanan informasi yang dapat dieksploitasi oleh ancaman.
2. Pemilik risiko harus memberikan penilaian dampak dari ancaman yang ada berdasarkan Tabel I.1.

Tabel I.1 Skala Nilai Dampak

| Nilai |               | Kriteria Dampak                   |
|-------|---------------|-----------------------------------|
| 1     | <i>Low</i>    | Gangguan layanan $\leq 2$ hari.   |
| 2     | <i>Medium</i> | Gangguan layanan 3 - 6 hari.      |
| 3     | <i>High</i>   | Gangguan layanan $\geq 1$ minggu. |

3. Pemilik risiko harus memberikan penilaian kemungkinan dari ancaman yang ada berdasarkan Tabel I.2.

Tabel I.2 Skala Nilai Kemungkinan

| Nilai |                 | Kriteria Kemungkinan                                                                                                                                   |
|-------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1     | <i>Unlikely</i> | Kejadian bisa terjadi (berulang) pada suatu waktu.                                                                                                     |
| 2     | <i>Possible</i> | <ul style="list-style-type: none"> <li>• Telah terjadi di masa lalu.</li> <li>• Kejadian mungkin kerap terjadi (berulang) pada suatu waktu.</li> </ul> |
| 3     | <i>Likely</i>   | Kejadian akan terjadi (berulang) pada sebagian besar keadaan.                                                                                          |

4. Hitung level resiko dengan menggunakan metode perkalian antara nilai dampak dan kemungkinan.
5. Petakan keseluruhan hasil sebelumnya yang saling berhubungan kedalam lembar kerja penilaian resiko.
6. Evaluasi resiko dengan membandingkan level resiko pada lembar kerja penilaian resiko dengan kriteria resiko dari dokumen [Kebijakan SMKI].
7. Untuk resiko yang memiliki level resiko yang berada diatas skala nilai resiko yang bisa diterima artinya resiko akan ditangani nantinya dan untuk resiko yang level resikonya sama dengan atau dibawah skala nilai resiko yang bisa diterima artinya resiko dapat dibiarkan dan diterima.
8. Urutkan setiap resiko berdasarkan level resikonya.

### 3. Komunikasi dan Konsultasi

Laporan [Proses Penilaian Resiko] harus didokumentasikan dan dilaporkan ke pemangku kepentingan yang tepat, serta dijaga oleh tim pemimpin SMKI selaku yang bertanggung jawab dalam pengelolaan dokumen terkait SMKI.

### 4. Pengawasan dan Peninjauan

Pimpinan bersama dengan komite pengendali SMKI harus melakukan peninjauan terhadap resiko yang ada saat ini dan memperbarui dokumen [Proses Penilaian Resiko] dengan cara penambahan resiko baru, ataupun pembaharuan nilai resiko yang ada pada aspek nilai dampak dan kemungkinannya. Hal ini dikarenakan resiko yang bisa muncul baru dan berubah-ubah sepanjang waktu. Peninjauan dapat dilakukan setahun sekali, atau bisa saja lebih bila terjadi perubahan signifikan pada organisasi, teknologi, tujuan bisnis atau lingkungan bisnis.

### 5. Laporan Proses Penilaian Resiko

Hasil dari proses penilaian resiko dapat dilihat pada halaman dibawah ini.

Tabel I.3 Daftar Inventaris Aset

| Nomor Aset | Tipe Aset | Aset                         | Pemilik Aset         | Pemilik Resiko         | Lokasi                                     |
|------------|-----------|------------------------------|----------------------|------------------------|--------------------------------------------|
| AS1        | Informasi | Daftar inventaris aset       | Subdit Infrastruktur | Kasubdit Infrastruktur | Subdit Infrastruktur, dan kantor DPTSI-ITS |
| AS2        |           | Dokumen konfigurasi          | Subdit Infrastruktur | Kasubdit Infrastruktur | Subdit Infrastruktur                       |
| AS3        |           | <i>File log</i>              | Subdit Infrastruktur | Kasubdit Infrastruktur | <i>Server</i>                              |
| AS4        |           | Kunci enkripsi VPN           | Subdit Infrastruktur | Kasubdit Infrastruktur | Kantor DPTSI-ITS                           |
| AS5        |           | Sertifikat <i>TLS</i>        | Subdit Infrastruktur | Kasubdit Infrastruktur | Subdit Infrastruktur, dan <i>server</i>    |
| AS6        |           | <i>Database email</i>        | Subdit Pelayanan     | Kasubdit Pelayanan     | <i>Server</i>                              |
| AS7        |           | ISO 9000                     | Subdit Pelayanan     | Kasubdit Pelayanan     | Subdit Pelayanan                           |
| AS8        |           | Materi pelatihan/sosialisasi | Subdit Pelayanan     | Kasubdit Pelayanan     | Subdit Pelayanan                           |
| AS9        |           | Daftar inventaris SIM        | Subdit Pengembangan  | Kasubdit Pengembangan  | Subdit Pengembangan                        |
| AS10       |           | <i>Developer Guide</i>       | Subdit Pengembangan  | Kasubdit Pengembangan  | Subdit Pengembangan                        |
| AS11       |           | <i>User Guide</i>            | Subdit Pengembangan  | Kasubdit Pengembangan  | Subdit Pengembangan                        |
| AS12       |           | Perencanaan SIM              | Subdit Pengembangan  | Kasubdit Pengembangan  | Subdit Pengembangan                        |

|      |                      |                                    |                      |                        |                      |
|------|----------------------|------------------------------------|----------------------|------------------------|----------------------|
| AS13 | Informasi<br>(lanj.) | <i>Source code</i>                 | Subdit Pengembangan  | Kasubdit Pengembangan  | Subdit Pengembangan  |
| AS14 | Perangkat<br>keras   | <i>Server</i>                      | Subdit Infrastruktur | Kasubdit Infrastruktur | Pusat data           |
| AS15 |                      | <i>Server backup</i>               | Subdit Infrastruktur | Kasubdit Infrastruktur | Pusat data           |
| AS16 |                      | Frey Internet Router               | Subdit Infrastruktur | Kasubdit Infrastruktur | Pusat data           |
| AS17 |                      | Sangfor Internet Access Management | Subdit Infrastruktur | Kasubdit Infrastruktur | Pusat data           |
| AS18 |                      | <i>Core switch</i>                 | Subdit Infrastruktur | Kasubdit Infrastruktur | Pusat data           |
| AS19 |                      | <i>Distribution switch</i>         | Subdit Infrastruktur | Kasubdit Infrastruktur | Pusat data           |
| AS20 |                      | <i>Access switch</i>               | Subdit Infrastruktur | Kasubdit Infrastruktur | Kantor DPTSI-ITS     |
| AS21 |                      | <i>Access point</i>                | Subdit Infrastruktur | Kasubdit Infrastruktur | Kantor DPTSI-ITS     |
| AS22 |                      | Cisco ASA Firewall                 | Subdit Infrastruktur | Kasubdit Infrastruktur | Pusat data           |
| AS23 |                      | Fortigate Anti-Spam                | Subdit Infrastruktur | Kasubdit Infrastruktur | Pusat data           |
| AS24 |                      | Komputer                           | Subdit Infrastruktur | Kasubdit Infrastruktur | Subdit Infrastruktur |
| AS25 |                      |                                    |                      | Kasubdit Pelayanan     | Subdit Pelayanan     |

|      |                         |                           |                              |                        |                      |
|------|-------------------------|---------------------------|------------------------------|------------------------|----------------------|
| AS26 | Perangkat keras (lanj.) | Komputer (lanj.)          | Subdit Infrastruktur (lanj.) | Kasubdit Pengembangan  | Subdit Pengembangan  |
| AS27 |                         | Laptop dinas              | Subdit Infrastruktur         | Kasubdit Infrastruktur | Subdit Infrastruktur |
| AS28 |                         |                           |                              | Kasubdit Pelayanan     | Subdit Pelayanan     |
| AS29 |                         |                           |                              | Kasubdit Pengembangan  | Subdit Pengembangan  |
| AS30 | Perangkat lunak         | <i>DNS</i> (BIND)         | Subdit Infrastruktur         | Kasubdit Infrastruktur | <i>Server</i>        |
| AS31 |                         | <i>Proxy</i> (Squid)      | Subdit Infrastruktur         | Kasubdit Infrastruktur | <i>Server</i>        |
| AS32 |                         | Nagios                    | Subdit Infrastruktur         | Kasubdit Infrastruktur | <i>Server</i>        |
| AS33 |                         | Open VPN                  | Subdit Infrastruktur         | Kasubdit Infrastruktur | <i>Server</i>        |
| AS34 |                         | <i>SIEM</i> AlienVault    | Subdit Infrastruktur         | Kasubdit Infrastruktur | <i>Server</i>        |
| AS35 |                         | ITS Web Monitoring System | Subdit Pelayanan             | Kasubdit Pelayanan     | <i>Server</i>        |
| AS36 |                         | Webmail ITS               | Subdit Pelayanan             | Kasubdit Pelayanan     | <i>Server</i>        |
| AS37 |                         | Git ITS                   | Subdit Pengembangan          | Kasubdit Pengembangan  | <i>Server</i>        |
| AS38 | Jaringan komunikasi     | <i>Internet</i>           | Subdit Infrastruktur         | Kasubdit Infrastruktur | Kantor DPTSI-ITS     |
| AS39 |                         | <i>Intranet</i>           | Subdit Infrastruktur         | Kasubdit Infrastruktur | Kantor DPTSI-ITS     |

|      |                     |                                 |                                 |                        |                      |
|------|---------------------|---------------------------------|---------------------------------|------------------------|----------------------|
| AS40 | Fasilitas fisik     | <i>Disaster recovery center</i> | PT. Telkom                      | Kasubdit Infrastruktur | Telkom Gubeng        |
| AS41 |                     | Pusat data                      | Subdit Infrastruktur            | Kasubdit Infrastruktur | Subdit Infrastruktur |
| AS42 | Perangkat pelengkap | Kabel <i>fiber optic</i>        | Subdit Infrastruktur            | Kasubdit Infrastruktur | Lingkungan ITS       |
| AS43 |                     | Kabel listrik                   | Direktorat Sarana dan Prasarana | Kasubdit Infrastruktur | Lingkungan ITS       |
| AS44 |                     | Kabel <i>UTP</i>                | Subdit Infrastruktur            | Kasubdit Infrastruktur | Kantor DPTSI-ITS     |
| AS45 |                     | <i>Diesel generator</i>         | Subdit Infrastruktur            | Kasubdit Infrastruktur | Kantor DPTSI-ITS     |
| AS46 |                     | <i>UPS</i>                      | Subdit Infrastruktur            | Kasubdit Infrastruktur | Kantor DPTSI-ITS     |
| AS47 |                     | Listrik PLN                     | Direktorat Sarana dan Prasarana | Kasubdit Infrastruktur | Kantor DPTSI-ITS     |
| AS48 |                     | Sistem pendingin ruangan        | Direktorat Sarana dan Prasarana | Kasubdit Infrastruktur | Kantor DPTSI-ITS     |
| AS49 |                     | Pengguna Webmail ITS            | Subdit Pelayanan                | Kasubdit Pelayanan     | Lingkungan ITS       |
| AS50 | Orang               | Subdit Infrastruktur            | Direktorat SDM dan Organisasi   | Direktur DPTSI-ITS     | Kantor DPTSI-ITS     |
| AS51 |                     | Subdit Pelayanan                | Direktorat SDM dan Organisasi   | Direktur DPTSI-ITS     | Kantor DPTSI-ITS     |
| AS52 |                     | Subdit Pengembangan             | Direktorat SDM dan Organisasi   | Direktur DPTSI-ITS     | Kantor DPTSI-ITS     |
|      |                     |                                 |                                 |                        |                      |

Tabel I.4 Daftar Ancaman

| Nomor Ancaman | Sumber Ancaman                  | Ancaman                                            | Aspek CIA | Aset yang Terganggu                     |
|---------------|---------------------------------|----------------------------------------------------|-----------|-----------------------------------------|
| AN1           | Bencana Alam                    | Kebakaran                                          | A         | AS41                                    |
| AN2           |                                 | Petir                                              | A         | AS47                                    |
| AN3           | Lingkungan/<br>kegagalan teknis | Gangguan elektromagnetik                           | A         | AS44                                    |
| AN4           |                                 | Gangguan sinyal dari perangkat lain                | A         | AS21                                    |
| AN5           |                                 | Hubungan arus pendek                               | A         | AS43                                    |
| AN6           |                                 | Kegagalan dalam memulihkan data                    | A         | AS15, AS40                              |
| AN7           |                                 | Kegagalan daya listrik                             | A         | AS47                                    |
| AN8           |                                 | Kegagalan koneksi                                  | A         | AS38                                    |
| AN9           |                                 | Kegagalan perangkat jaringan                       | A         | AS16-AS23                               |
| AN10          |                                 | Kegagalan perangkat keras                          | A         | AS14, AS15, AS24-AS29, AS45, AS46, AS48 |
| AN11          |                                 | Kegagalan perangkat lunak                          | A         | AS30-AS37                               |
| AN12          |                                 | Kerusakan kabel                                    | A         | AS42-AS44                               |
| AN13          |                                 | Lambatnya koneksi jaringan                         | A         | AS38                                    |
| AN14          |                                 | Penurunan kondisi media penyimpanan                | A         | AS14, AS15                              |
| AN15          |                                 | Tidak sesuainya kondisi temperatur                 | A         | AS41                                    |
| AN16          | Ketidak-sengajaan manusia       | Kurang kualifikasi dalam mengkonfigurasi perangkat | I         | AS50                                    |
| AN17          |                                 | Kesalahan dalam melayani pelanggan                 | I         | AS51                                    |
| AN18          |                                 | Kesalahan dalam membuat sistem informasi           | I         | AS52                                    |



|      |                                   |                                                       |           |                                                |
|------|-----------------------------------|-------------------------------------------------------|-----------|------------------------------------------------|
| AN19 | Ketidak-sengajaan manusia (lanj.) | Kesalahan dalam menggunakan perangkat TIK             | C + I     | AS49-AS52                                      |
| AN20 |                                   | Kesalahan konfigurasi                                 | C + I + A | AS14-AS23, AS30-AS34, AS37                     |
| AN21 |                                   | Kesalahan pembuatan data                              | I         | AS1, AS2, AS7-AS12                             |
| AN22 |                                   | Kesalahan pembuatan yang menyebabkan <i>bug/error</i> | C + I + A | AS13                                           |
| AN23 |                                   | Kesalahan/ <i>bug</i> pada perangkat lunak            | I + A     | AS14, AS15, AS24-AS29                          |
| AN24 |                                   | Kerusakan/kehilangan data                             | I + A     | AS1-AS13                                       |
| AN25 |                                   | Penyingkapan informasi                                | C         | AS1, AS2, AS4, AS5, AS7, AS9, AS10, AS12, AS13 |
| AN26 |                                   | Waktu <i>log</i> tidak sama                           | I         | AS3                                            |
| AN27 |                                   | Kegagalan akibat penggunaan melebihi batas kapasitas  | A         | AS14-AS23                                      |
| AN28 |                                   | Absensi karyawan                                      | A         | AS50-AS52                                      |
| AN29 | Kesengajaan manusia               | Akses tanpa izin                                      | C + I + A | AS3, AS6, AS14-AS34, AS36, AS37, AS39, AS41    |
| AN30 |                                   | Aktifitas <i>worm</i>                                 | C + I + A | AS39                                           |
| AN31 |                                   | <i>Denial of service</i>                              | A         | AS14                                           |
| AN32 |                                   | Gangguan ke sistem oleh vendor                        | C + I     | AS40                                           |
| AN33 |                                   | Kode berbahaya pada <i>source code</i>                | C + I     | AS13                                           |
| AN34 |                                   | Pencurian dokumen/media penyimpanan                   | C + A     | AS1, AS2, AS4, AS5, AS7, AS9, AS10, AS12, AS13 |
| AN35 |                                   | Pencurian perangkat jaringan                          | C + A     | AS16-AS23                                      |

|      |                             |                                                      |           |                       |
|------|-----------------------------|------------------------------------------------------|-----------|-----------------------|
| AN36 | Kesengajaan manusia (lanj.) | Pencurian perangkat keras                            | C + A     | AS14, AS15, AS24-AS29 |
| AN37 |                             | Pencurian perangkat pelengkap                        | A         | AS45, AS46, AS48      |
| AN38 |                             | Penggunaan perangkat lunak ilegal                    | C + I + A | AS24-AS29             |
| AN39 |                             | Penghapusan <i>log</i> tanpa izin                    | I + A     | AS3                   |
| AN40 |                             | Penyalahgunaan hak akses dan tindakan ilegal lainnya | I + A     | AS49-AS52             |
| AN41 |                             | Penyebaran <i>malware</i>                            | C + I + A | AS14, AS15, AS24-AS29 |
| AN42 |                             | Penyimpangan data yang dimasukkan                    | I         | AS6                   |
| AN43 |                             | Perubahan konfigurasi tanpa izin                     | I         | AS14-AS37             |
| AN44 |                             | <i>Sniffing</i>                                      | C         | AS39                  |
| AN45 |                             | <i>Spam</i>                                          | A         | AS36                  |
| AN46 |                             | Terkena aktifitas <i>social engineering</i>          | C         | AS49-AS52             |

Tabel I.5 Daftar Kelompok Kontrol Keamanan Saat Ini

| Kode                  | Kontrol Keamanan                  | Keterangan                                                                                                                                                                                                                                                     |
|-----------------------|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Administrative</i> |                                   |                                                                                                                                                                                                                                                                |
| A1                    | Peran dan tanggung jawab karyawan | Peran dan tanggung jawab yang dimiliki oleh karyawan di DPTSI-ITS (Subdit Infrastruktur, Subdit Pelayanan, dan Subdit Pengembangan) baik terhadap aset maupun aktifitas tertentu yang telah ditetapkan (A.6.1.1 dan A.8.1.2).                                  |
| A2                    | Uraian Tugas                      | Dokumen didalam ISO 9000 yang berisi pembagian dan penjelasan tugas setiap fungsi kerja atau jabatan berikut standar kompetensi yang dibutuhkan (A.6.1.2). Dengan adanya pembagian tugas, tidak ada satupun tugas sensitif dilakukan oleh satu orang dari awal |

|    |                                     |                                                                                                                                                                                                                                                                                                                                                                      |
|----|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    |                                     | sampai akhir. Selain itu terdapat peninjauan dan persetujuan aktifitas dari karyawan lainnya.                                                                                                                                                                                                                                                                        |
| A3 | Menghubungi vendor                  | Karyawan dapat menghubungi vendor perangkat untuk masalah pada perangkat (jika garansi masih ada), <i>ISP</i> untuk masalah pada koneksi <i>internet</i> , dan lainnya (A.6.1.3 dan A.11.2.4).                                                                                                                                                                       |
| A4 | Menghubungi unit lain di ITS        | Karyawan dapat menghubungi unit lain jika terdapat insiden/masalah atau keperluan operasional, seperti ULP-ITS untuk pengadaan layanan/barang jika terdapat perangkat rusak yang harus diganti, Hukortala-ITS untuk penanganan hukum jika ada pelanggaran didalam ITS, Direktorat SDM dan Organisasi untuk penanganan dan pengadaan karyawan, dan lainnya (A.6.1.3). |
| A5 | Menghubungi <i>forum</i>            | Karyawan dapat mengunjungi beberapa forum atau <i>website</i> tentang komputer atau keamanan informasi untuk mendapatkan ilmu dan menangani masalah yang ada (A.6.1.4).                                                                                                                                                                                              |
| A6 | Manajemen proyek                    | Setiap proyek seperti pengembangan sistem informasi terpadu, pemasangan/perluasan infrastruktur jaringan, dan lainnya dilakukan perencanaan dan pengelolaan keamanan informasinya (A.6.1.5).                                                                                                                                                                         |
| A7 | <i>Background check</i>             | Proses memastikan kesesuaian <i>curriculum vitae</i> pelamar beserta kelengkapannya (KTP/paspor, SKCK, sertifikat akademis/profesional). Selain itu dinilai juga kemampuan karyawan melalui wawancara dan tes tertulis (A.7.1.1).                                                                                                                                    |
| A8 | Kompetisi Sumber Daya               | Dokumen didalam ISO 9000 yang berisi rincian persyaratan untuk setiap fungsi kerja atau jabatan yang ada ( <i>job requirement</i> ) (A.7.1.1).                                                                                                                                                                                                                       |
| A9 | Pengarahan sebelum penempatan kerja | Karyawan yang baru masuk akan dijelaskan peran dan tanggung jawab yang akan diemban oleh Direktur DPTSI-ITS, lalu Kasubdit akan menjelaskan lagi secara rinci jika karyawan tersebut ditempatkan di Subdit tertentu (A.7.1.2).                                                                                                                                       |

|     |                                   |                                                                                                                                                                                                                                                                                                                                                                |
|-----|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A10 | Pelaporan pelanggaran             | Pelaporan karyawan yang melanggar ke atasan langsungnya, jika tidak bisa diselesaikan oleh atasan langsungnya maka atasan tersebut melaporkan ke atasannya selama pelanggaran bukan yang mengarah ke tindak hukum (A.7.2.1).                                                                                                                                   |
| A11 | Program kesadaran keamanan        | Program yang diadakan untuk meningkatkan kesadaran akan keamanan informasi. Program yang dilakukan seperti <i>posting</i> secara berkala di <i>website</i> DPTSI-ITS, poster yang ditempel di mading disekitar ITS, atau seminar (A.7.2.2).                                                                                                                    |
| A12 | Sosialisasi pelatihan sistem      | Sosialisasi tentang SIM atau layanan TIK yang dikembangkan oleh DPTSI-ITS yang diadakan untuk pengenalan dan penggunaannya kepada pemangku kepentingan terkait di ITS (A.7.2.2).                                                                                                                                                                               |
| A13 | Pelatihan kerja                   | Pelatihan atau sertifikasi kerja yang diadakan untuk meningkatkan kemampuan karyawan DPTSI-ITS dalam bekerja (A.7.2.2).                                                                                                                                                                                                                                        |
| A14 | Matriks Kebutuhan Pelatihan SDM   | Dokumen didalam ISO 9000 yang berisi perencanaan pelatihan yang akan diberikan kepada setiap karyawan kedalam format matriks (A.7.2.2).                                                                                                                                                                                                                        |
| A15 | Sangsi                            | Hukuman disiplin tertulis bagi karyawan, dosen dan mahasiswa yang melanggar beberapa ketentuan ataupun keamanan informasi dilingkungan ITS. (A.7.2.3).                                                                                                                                                                                                         |
| A16 | Daftar inventaris                 | <ul style="list-style-type: none"> <li>• Untuk aset BMN didokumentasikan kedalam E-Aset dan <i>file</i> Daftar Inventaris Aset.</li> <li>• Untuk sistem informasi yang dikembangkan didokumentasikan kedalam <i>file</i> Daftar Inventaris SIM.</li> <li>• Untuk aset berupa data/informasi didokumentasikan kedalam Daftar Rekaman Mutu (A.8.1.1).</li> </ul> |
| A17 | Kebijakan penggunaan <i>email</i> | Peraturan yang berisikan apa yang tidak boleh dilakukan, sangsi jika melanggar dan tanggung jawab pihak DPTSI-ITS terhadap <i>email</i> (A.8.1.3).                                                                                                                                                                                                             |
| A18 | Instruksi kerja                   | Dokumen didalam ISO 9000 yang berisi tata cara penggunaan aset, seperti penggunaan <i>switch/hub</i> ,                                                                                                                                                                                                                                                         |

|     |                                                   |                                                                                                                                                                                                                                                                                                                                                                                           |
|-----|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                                   | <i>router, server, HT (walkie-talkie), scanner</i> dan APAR (A.8.1.3).                                                                                                                                                                                                                                                                                                                    |
| A19 | Pengembalian aset                                 | Pengecekan dan pengembalian aset yang dipinjam oleh karyawan yang berhenti atau mutasi kerja (contohnya laptop dinas) (A.8.1.4).                                                                                                                                                                                                                                                          |
| A20 | Klasifikasi informasi                             | Klasifikasikan kerahasiaan informasi terkait data ataupun informasi yang disimpan di sistem informasi terpadu yang dibangun. Klasifikasi masih berbentuk arahan dari Wakil Rektor III (A.8.2.1).                                                                                                                                                                                          |
| A21 | Prosedur pemusnahan dokumen                       | Proses pemusnahan dokumen yang tidak diperlukan lagi sesuai dengan masa waktu simpan yang tertera pada Daftar Rekaman Mutu (A.8.3.2).                                                                                                                                                                                                                                                     |
| A22 | Panduan akses <i>internet</i> dan <i>intranet</i> | Tata cara pengaksesan layanan <i>internet</i> dan <i>intranet</i> di kawasan ITS yang disediakan oleh DPTSI-ITS (A.9.1.2).                                                                                                                                                                                                                                                                |
| A23 | Prosedur pembuatan akun <i>email</i>              | Proses pendaftaran akun <i>email</i> bagi mahasiswa baru dilakukan secara <i>online</i> , sedangkan untuk karyawan atau dosen dilakukan dengan mengirimkan surat permohonan yang ditandatangani oleh kepala jurusan/unit (A.9.2.1).                                                                                                                                                       |
| A24 | Prosedur penghapusan akun <i>email</i>            | Proses penghapusan akun <i>email</i> bagi dosen, karyawan dan mahasiswa yang dilakukan ketika surat keterangan resmi dari unit/jurusan yang menyatakan bahwa pengguna akun sudah keluar/lulus dari ITS. Layanan <i>email</i> yang bekerjasama dengan Microsoft tidak ada penghapusan akun, yang ada adalah perubahan <i>password</i> karena akun bersifat melekat pada jabatan (A.9.2.1). |
| A25 | Penyediaan hak akses                              | Pemberian hak akses kepada karyawan melalui otorisasi dari pemilik aset dan verifikasi kesesuaian hak akses dengan karyawan. Hak akses mencakup <i>server</i> , perangkat lunak, perangkat jaringan, perangkat <i>fingerprint</i> , dan lainnya (A.9.2.2 dan A.9.2.3).                                                                                                                    |
| A26 | Penghapusan hak akses                             | Penghapusan hak akses yang dimiliki karyawan yang tidak lagi bekerja pada <i>server</i> , perangkat lunak dan perangkat jaringan. Selain itu dilakukan juga                                                                                                                                                                                                                               |

|     |                                            |                                                                                                                                                                                                                                                                  |
|-----|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                            | penghapusan hak akses dari perangkat <i>fingerprint</i> dan pengembalian kunci pintu <i>analog</i> yang dipegang oleh karyawan (A.9.2.2 dan A.9.2.6).                                                                                                            |
| A27 | Prosedur <i>reset password</i>             | Proses penggantian <i>password</i> baru akun <i>email</i> yang bisa dilakukan secara <i>online</i> ataupun melalui Subdit Pelayanan (A.9.2.4).                                                                                                                   |
| A28 | Peninjauan hak akses                       | Peninjauan hak akses yang dimiliki pengguna pada aset tertentu, apakah akun sudah dihapus bagi yang sudah pindah/keluar. Untuk hak akses fisik dilakukan juga peninjauan pada rekaman <i>CCTV</i> (A.9.2.5).                                                     |
| A29 | Saran penggunaan <i>password</i> yang aman | Saran penggunaan <i>password</i> yang aman didokumentasikan di halaman Webmail ITS dan Integra ITS, seperti <i>password</i> harus yang sulit ditebak, menggunakan kombinasi huruf kapital-kecil, dan lainnya (A.9.3.1).                                          |
| A30 | Kebijakan bekerja di pusat data            | Peraturan yang melarang penggunaan alat perekam gambar seperti kamera dan <i>handphone</i> dan aktifitas makan-minum dan merokok didalam ruang pusat data (A.11.1.5).                                                                                            |
| A31 | Pengujian kabel                            | Pengujian pada kabel yang dilakukan untuk memeriksa apakah terdapat kerusakan pada kabel secara berkala (A.11.2.3).                                                                                                                                              |
| A32 | Prosedur pemeliharaan perlengkapan         | Proses perawatan secara fisik dilakukan pada perangkat (seperti <i>switch</i> , <i>router</i> ) dan peralatan pendukungnya (seperti <i>AC</i> , <i>UPS</i> , <i>diesel generator</i> , <i>grounding</i> ) secara berkala (A.11.2.4).                             |
| A33 | Perizinan peminjaman atau permintaan aset  | Setiap peminjaman perangkat atau peralatan, dan permintaan data/informasi yang dimiliki oleh DPTSI-ITS harus melalui proses perizinan terlebih dahulu. Peminjam diharuskan mengisi berita acara untuk perangkat dan surat permohonan untuk informasi (A.11.2.5). |
| A34 | Pembuangan media elektronik                | Semua perangkat dengan media penyimpanan yang rusak dan tidak bisa diperbaiki oleh vendor karena sudah melewati masa garansi dikirimkan ke BAUK-ITS untuk dirusak secara fisik (A.11.2.7).                                                                       |

|     |                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A35 | ISO 9000                                      | Dokumen yang berisikan berbagai dokumen, prosedur, instruksi kerja, dan formulir untuk menjalankan aktifitas bisnis di DPTSI-ITS (A.12.1.1).                                                                                                                                                                                                                                                                                            |
| A36 | Prosedur manajemen perubahan                  | Proses perubahan yang dilakukan di DPTSI-ITS mulai dari identifikasi dan perekaman, perencanaan dan pengujian, verifikasi kebutuhan keamanan informasi, persetujuan formal dan komunikasi perubahan (A.12.1.1). Selain itu dilakukan penggantian <i>password default</i> dari vendor pada perangkat (A.9.2.4).                                                                                                                          |
| A37 | Identifikasi kebutuhan kapasitas sumberdaya   | Identifikasi kebutuhan minimum sumberdaya yang dibutuhkan. Untuk sistem dan jaringan, DPTSI-ITS memiliki standar spesifikasi sistem (contohnya spesifikasi <i>processor</i> , <i>memory</i> , <i>hardisk</i> , dan lainnya yang diperlukan) dan standar konfigurasi pemasangan jaringan. Sedangkan untuk SDM, Direktorat SDM dan Organisasi menggunakan metode analisis struktur organisasi dan proses bisnis di organisasi (A.12.1.3). |
| A38 | Prosedur <i>backup</i>                        | Proses <i>backup</i> data yang dilakukan sesuai dengan jadwal (harian atau mingguan) dan <i>backup</i> konfigurasi yang dilakukan setiap ada perubahan (A.12.3.1).                                                                                                                                                                                                                                                                      |
| A39 | Pemasangan perangkat lunak                    | Pemasangan perangkat lunak kedalam sistem operasi yang diikuti dengan pengujian pemasangan, pengembalian keadaan semula jika terjadi masalah, dan penyimpanan perangkat lunak sebelumnya (A.12.5.1). Selain itu dilakukan penggantian <i>password default</i> dari vendor pada perangkat (A.9.2.4).                                                                                                                                     |
| A40 | Pemasangan <i>patch</i>                       | Pemasangan <i>patch</i> terbaru yang sebelumnya diujicoba apakah terdapat efek samping yang mengganggu. Jika pemasangan bermasalah maka akan tetap menggunakan versi yang lama (A.12.6.1).                                                                                                                                                                                                                                              |
| A41 | Prosedur pengawasan jaringan                  | Proses pengawasan jaringan untuk memastikan <i>internet</i> , <i>intranet</i> dan sistem informasi terpadu dilingkungan ITS berjalan secara normal (A.13.1.1).                                                                                                                                                                                                                                                                          |
| A42 | <i>Non-disclosure agreement</i> bagi karyawan | Perjanjian menjaga kerahasiaan bagi karyawan PNS yang baru masuk dan Subdit Pengembangan yang diberikan akses ke sistem informasi (A.13.2.4).                                                                                                                                                                                                                                                                                           |

|     |                                                         |                                                                                                                                                                                                                                                                                                                                                                      |
|-----|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A43 | Identifikasi spesifikasi persyaratan keamanan informasi | Sebelum aktifitas pengembangan atau pemutakhiran sistem informasi dimulai, dilakukan identifikasi persyaratan keamanan, proses bisnis dan fungsionalitas dari sistem yang dibutuhkan melalui mematuhi kebijakan atau hukum yang berlaku, peninjauan insiden yang pernah terjadi, kerentanan yang ditemukan atau dicurigai, dan wawancara dengan pengguna (A.14.1.1). |
| A44 | <i>Developer Guide</i>                                  | Buku panduan bagi Subdit Pengembang yang berisikan penjelasan <i>source code</i> dan <i>database</i> dengan penggambaran diagramnya yang membantu <i>programmer</i> selanjutnya dalam pengembangan sistem (A.14.2.2).                                                                                                                                                |
| A45 | <i>User Guide</i>                                       | Buku panduan bagi pengguna yang berisikan penjelasan penggunaan perangkat lunak yang digunakan di DPTSI-ITS (A.14.2.2).                                                                                                                                                                                                                                              |
| A46 | Prosedur kontrol perubahan sistem                       | Proses pengembangan atau pembaharuan sistem informasi yang dikembangkan oleh DPTSI-ITS mulai dari identifikasi persyaratan sampai sosialisasi pelatihan sistem (A.14.2.2).                                                                                                                                                                                           |
| A47 | Peninjauan teknis aplikasi setelah perubahan            | Peninjauan untuk melihat apakah sistem informasi dapat berjalan normal setelah dilakukan perubahan pada sistem informasi tersebut atau <i>platform</i> -nya ( <i>DBMS</i> , sistem operasi dan lainnya) (A.14.2.3).                                                                                                                                                  |
| A48 | Pengujian keamanan sistem                               | Pengujian sistem didalam proses pengembangan sistem, seperti menyesuaikan apakah <i>input</i> data dan hasil yang diharapkan pada kondisi tertentu (A.14.2.8).                                                                                                                                                                                                       |
| A49 | Prosedur pengujian penerimaan sistem                    | Proses pengujian sistem baru atau pembaharuan yang dikembangkan yang mencakup pengujian fungsi, <i>accessability</i> , manajemen pengguna (hak akses) dan <i>usability</i> dari sistem sebelum diterima oleh pengguna dan dimasukkan kedalam <i>server live</i> (A.14.2.9).                                                                                          |
| A50 | <i>Non-disclosure agreement</i> bagi vendor             | Perjanjian menjaga kerahasiaan bagi vendor yang dapat mengakses aset yang dimiliki oleh DPTSI-ITS (A.15.1.2).                                                                                                                                                                                                                                                        |



|     |                                      |                                                                                                                                                                                         |
|-----|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A51 | Peninjauan layanan vendor            | Peninjauan untuk melihat apakah layanan yang diberikan vendor sesuai dengan perjanjian didalam kontraknya dengan bantuan <i>file log</i> dan jumlah laporan keluhannya (A.15.2.1).      |
| A52 | Pengaturan perubahan layanan vendor  | Pengaturan perubahan layanan vendor jika berdasarkan hasil peninjauan layanan vendor sudah tidak sesuai kondisi kontraknya (A.15.2.2).                                                  |
| A53 | Prosedur penanganan insiden          | Proses penanganan insiden terkait TIK yang ada di lingkungan ITS yang mencakup perbaikan komponen rusak dan instalasi jaringan rusak (A.16.1.1).                                        |
| A54 | <i>Service desk</i>                  | Layanan pelaporan keluhan yang terkait TIK di lingkungan ITS melalui datang langsung ke Subdit Pelayanan, telepon, <i>email</i> ataupun sistem E-Tiket (A.16.1.1 dan A.16.1.2).         |
| A55 | Penilaian dan keputusan dari insiden | Penilaian mana laporan kejadian yang dikerjakan terlebih dahulu berdasarkan waktu laporan masuk atau jabatan pelapor (A.16.1.4).                                                        |
| A56 | Pembelajaran dari insiden            | Penggunaan setiap penyelesaian keluhan untuk mengurangi kemungkinan dan dampaknya kedepan melalui program kesadaran keamanan ataupun peningkatan/penerapan kontrol keamanan (A.16.1.6). |
| A57 | Pengumpulan bukti                    | Pengumpulan dan pemeliharaan bukti dari berbagai sumber (seperti <i>log</i> pada <i>server</i> dan perangkat jaringan) untuk alat bantu hukum dan pemberian sangsi (A.16.1.7).          |
| A58 | Daftar Dokumen Eksternal             | Dokumen didalam ISO 9000 yang berisi undang-undang/peraturan yang berlaku dan diikuti oleh DPTSI-ITS (A.18.1.1).                                                                        |
| A59 | Audit keamanan informasi             | Peninjauan keamanan informasi yang dilakukan oleh mahasiswa melalui peneilitian yang memperlihatkan kondisi keamanan saat ini dan saran perbaikannya (A.18.2.1).                        |
| A60 | Peninjauan kepatuhan teknis          | Peninjauan sistem yang mencakup pengujian pemindaian kerentanan dan <i>stress test</i> yang dilakukan tidak secara berkala atau ketika terdapat masalah saja (A.18.2.3).                |

| <i>Physical</i> |                                       |                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| P1              | Pintu                                 | Setiap ruangan memiliki pintu yang memiliki kunci <i>analog</i> dan biasanya akan dikunci jika tidak ada orang didalam atau sudah tidak digunakan lagi (A.11.1.1).                                                                                                                                                                                                                             |
| P2              | Pintu dengan kunci <i>fingerprint</i> | Lorong-lorong menuju ruangan Subdit Infrastruktur dan Subdit Pengembangan dikunci dan harus memasukkan sidik jari karyawan. Pengunjung yang ingin lewat harus meminta izin ke dan didampingi oleh Subdit Pelayanan dengan menyatakan maksud kedatangannya. Selain itu ruang pusat data juga dikunci dan hanya Subdit Infrastruktur dan Direktur DPTSI-ITS saja yang bisa mengakses (A.11.1.1). |
| P3              | Pintu kebakaran                       | Pintu yang tersedia disetiap lantai untuk jalur evakuasi jika terjadi bencana kebakaran (A.11.1.1).                                                                                                                                                                                                                                                                                            |
| P4              | Area penerimaan tamu                  | Area yang digunakan untuk mengontrol akses fisik pengunjung untuk pergi ke ruangan lain yang hanya dapat diakses karyawan dan yang diizinkan saja (A.11.1.1).                                                                                                                                                                                                                                  |
| P5              | <i>CCTV</i>                           | Dibeberapa sudut ruangan didalam gedung ITS Research Center dipasang <i>CCTV</i> . Selain itu didalam ruangan pusat data juga memiliki <i>CCTV</i> yang dikelola DPTSI-ITS (A.11.1.2).                                                                                                                                                                                                         |
| P6              | Pusat data                            | Ruangan yang menempatkan <i>server</i> dan perangkat jaringan (seperti <i>firewall</i> , <i>router</i> , <i>switch</i> ) agar dijauhi dari akses publik (A.11.1.3)                                                                                                                                                                                                                             |
| P7              | Pengamanan penempatan pada ruangan    | Menempatkan setiap meja kerja karyawan agar layar komputer/laptop tidak menghadap keluar agar tidak dapat mudah dilihat oleh pengunjung. Selain itu terdapat nomor ruangan pada pintu yang tidak mengindikasikan maksud dari ruangan tersebut (A.11.1.3).                                                                                                                                      |
| P8              | Karyawan <i>shift</i> malam           | DPTSI-ITS memiliki karyawan yang menginap dan berjaga didalam kantor di malam hari. Karyawan tersebut bisa melakukan <i>troubleshooting</i> jika terdapat masalah ringan yang tidak kritis (A.11.1.4).                                                                                                                                                                                         |

|     |                            |                                                                                                                                                                                                                                                                                               |
|-----|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| P9  | Satpam                     | Terdapat petugas yang menjaga disekitar gedung ITS Research Center 24 jam (A.11.1.4).                                                                                                                                                                                                         |
| P10 | Lemari                     | Terdapat beberapa lemari yang memiliki kunci <i>analog</i> yang biasanya digunakan untuk menyimpan dokumen yang tidak boleh diakses tanpa izin (A.11.1.4).                                                                                                                                    |
| P11 | <i>Hydrant</i>             | Perangkat yang dipasang didinding yang berfungsi sebagai sumber air untuk memadamkan api (A.11.1.4).                                                                                                                                                                                          |
| P12 | Perangkat pendeteksi asap  | Perangkat yang dipasang didinding atau dilangit-langit sebagai pendeteksi asap yang akan berbunyi ( <i>alarm</i> ) jika terdapat indikasi asap (A.11.1.4).                                                                                                                                    |
| P13 | Perangkat pemadam otomatis | Perangkat yang dipasang dilangit-langit yang berfungsi mengeluarkan material yang dapat memadamkan api secara otomatis (A.11.1.4).                                                                                                                                                            |
| P14 | APAR                       | APAR (Alat Pemadam Api Ringan) yang berfungsi sebagai perangkat pemadam api <i>mobile</i> yang dipasang didalam ruangan pusat data maupun di beberapa tempat didalam kantor. Tata cara penggunaan APAR umumnya sudah ditempel pada perangkat (A.11.1.4).                                      |
| P15 | <i>Grounding</i>           | Perangkat yang menciptakan sebuah jalur yang <i>low-impedance</i> (tahanan rendah) terhadap permukaan bumi yang melindungi perangkat elektronik dari lonjakan listrik, petir dan lainnya (A.11.2.1).                                                                                          |
| P16 | <i>Circuit Breaker</i>     | Pengaman yang ada di kotak panel listrik atau stop kontak yang melindungi arus listrik dari beban berlebih dan hubungan singkat. Jika terjadi penyimpangan pada arus listrik, maka perangkat akan memutuskan aliran listrik secara otomatis (A.11.2.1).                                       |
| P17 | <i>Air conditioner</i>     | Perangkat pendingin ruangan secara <i>default</i> dipasang disetiap ruang kantor. Sedangkan untuk ruang pusat data, DPTSI-ITS menyediakan lebih dari satu perangkat pendingin ruangan yang mengatur kelembaban dan suhu, dan memiliki <i>remote</i> yang dapat memantau dari jauh (A.11.2.1). |
| P18 | <i>Diesel generator</i>    | Perangkat daya cadangan yang berfungsi untuk menangani kehilangan pasokan listrik yang berjalan                                                                                                                                                                                               |

|           |                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|           |                                           | secara otomatis ketika terjadi mati listrik. Namun waktu respon perangkat tidak bisa langsung tanpa jeda memasok listrik ketika terjadi mati listrik. Ruang lingkup pasokan listrik yang dicakup hanya pusat data saja (A.11.2.2).                                                                                                                                                                                                               |
| P19       | UPS                                       | Perangkat pelindung untuk kehilangan pasokan listrik yang membantu jeda waktu perangkat <i>diesel generator</i> untuk aktif dalam memasok listrik. Perangkat ini bekerja secara terus menerus ( <i>standby-online</i> ). Ruang lingkup pasokan listrik yang dicakup hanya pusat data saja. Selain itu terdapat UPS yang memiliki daya rendah untuk komputer dan hanya mampu digunakan beberapa menit untuk menyimpan hasil pekerjaan (A.11.2.2). |
| P20       | Sumber penerangan dan komunikasi cadangan | Perangkat senter untuk sumber penerangan cadangan dan <i>walkie-talkie</i> untuk komunikasi cadangan jika terjadi keadaan darurat (A.11.2.2).                                                                                                                                                                                                                                                                                                    |
| P21       | Pemasangan kabel yang aman                | Kabel listrik dan jaringan sudah dipisah untuk mencegah interferensi satu sama lain. Selain itu kabel dilindungi dengan pipa pelindung kabel dan saluran beton bertulang berbentuk penampang huruf U ( <i>U-Ditch</i> ) didalam tanah (A.11.2.3).                                                                                                                                                                                                |
| P22       | Patok penanda kabel                       | Penanda ditanah yang menandakan bahwa terdapat jalur kabel didalam tanah (contohnya "FO" untuk kabel <i>fiber optic</i> dan "2.0 VA" untuk kabel listrik) (A.11.2.3).                                                                                                                                                                                                                                                                            |
| P23       | Perangkat pemasangan dan pengecekan kabel | Perangkat pemasangan kabel <i>UTP</i> dan listrik seperti <i>crimping tool</i> , <i>cable tester</i> , kabel cadangan, <i>jack</i> , panel dan lainnya. Sedangkan untuk kabel <i>fiber optic</i> hanya ada <i>cable tester</i> saja (A.11.2.3).                                                                                                                                                                                                  |
| P24       | Perangkat absen <i>finger print</i>       | Perangkat yang tersedia disetiap unit/jurusan yang berfungsi untuk absensi karyawan dan dosen dengan sidik jari (A.12.1.3).                                                                                                                                                                                                                                                                                                                      |
| Technical |                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

|    |                                            |                                                                                                                                                                                                                                                                                                                                              |
|----|--------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| T1 | Autentikasi pengguna                       | Jaringan <i>intranet</i> dan <i>internet</i> , Webmail ITS, sistem informasi, perangkat jaringan, dan <i>server</i> diatur agar melakukan autentikasi terlebih dahulu sebelum dapat mengakses (A.9.1.2).                                                                                                                                     |
| T2 | <i>Single Sign-On</i>                      | Autentikasi yang dilakukan satu kali dengan akun Integra ITS untuk dapat mengakses beberapa sistem informasi terpadu dan layanan <i>internet</i> didalam lingkungan ITS (A.9.3.1).                                                                                                                                                           |
| T3 | Prosedur <i>login</i> yang aman            | Webmail ITS diatur agar tidak menampilkan pesan <i>error</i> yang memberitahukan fungsi atau data sistem, melindungi dari <i>bruteforce</i> , menampilkan <i>password</i> dalam format <i>asterisk</i> , pembatasan <i>session</i> , dan lainnya (A.9.4.2).                                                                                  |
| T4 | Sistem manajemen <i>password</i> yang aman | <ul style="list-style-type: none"> <li>• Sistem Webmail ITS diatur agar panjang <i>password</i> 8 karakter dan mencegah penggunaan <i>password</i> yang sama.</li> <li>• <i>Server</i> diatur agar panjang <i>password</i> 8 karakter, penggunaan kombinasi karakter dan mencegah penggunaan <i>password</i> yang sama (A.9.4.3).</li> </ul> |
| T5 | Git ITS                                    | Sistem informasi terpusat untuk manajemen <i>source code</i> mulai dari pembuatan, kolaborasi antar tim, penyimpanan, pengujian, dan dokumentasi (A.9.4.5).                                                                                                                                                                                  |
| T6 | Protokol <i>TLS</i>                        | Protokol yang melindungi koneksi antara pengguna dengan semua sistem informasi terpadu yang disediakan, ataupun <i>administrator</i> dengan perangkat jaringan yang dikelola. Penyedia layanan <i>TLS</i> yang digunakan adalah DigiCert Inc. (A.10.1.1 dan A.13.2.3).                                                                       |
| T7 | <i>VPN</i>                                 | Jalur koneksi aman yang khusus dan wajib digunakan oleh <i>administrator</i> untuk melakukan koneksi <i>remote</i> ke <i>server</i> . Jika tidak maka akses akan ditolak oleh <i>firewall</i> (A.10.1.1).                                                                                                                                    |
| T8 | Enkripsi <i>database password</i>          | Setiap <i>field</i> untuk <i>password</i> akun untuk sistem informasi yang dibangun sudah disimpan dalam bentuk terenkripsi didalam <i>database</i> (A.10.1.1).                                                                                                                                                                              |

|     |                                             |                                                                                                                                                                                                                                                                                                        |
|-----|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| T9  | <i>Logout otomatis/<br/>session timeout</i> | Webmail ITS, perangkat jaringan dan <i>server</i> sudah diatur agar melakukan <i>log-out</i> secara otomatis dan memerlukan <i>login</i> ulang (A.11.2.8).                                                                                                                                             |
| T10 | Cacti                                       | Perangkat lunak yang memonitor kondisi ataupun beban trafik pada <i>backbone</i> antar jaringan, masing-masing <i>server</i> atau perangkat lainnya yang memiliki <i>IP address</i> . Selain itu juga Cacti digunakan untuk mengawasi banyaknya pengguna dan sisa kapasitas <i>hardisk</i> (A.12.1.3). |
| T11 | Windows Defender                            | Perangkat lunak <i>default</i> dari Microsoft Windows yang dipasang disetiap komputer karyawan untuk mencegah beragam <i>virus</i> , <i>malware</i> dan <i>spyware</i> (A.12.2.1).                                                                                                                     |
| T12 | ClamAV                                      | Perangkat lunak berlisensi <i>open source</i> yang dipasang pada <i>server</i> untuk mencegah beragam <i>trojan horse</i> , <i>virus</i> , <i>malware</i> dan kode berbahaya lainnya (A.12.2.1).                                                                                                       |
| T13 | <i>Server backup</i>                        | <i>Server</i> yang digunakan untuk <i>backup</i> secara terpusat yang memiliki dua jenis, yaitu bersifat otomatis dan sinkronisasi untuk <i>backup</i> data <i>server</i> , dan bersifat manual untuk <i>backup</i> konfigurasi atau <i>log</i> perangkat jaringan (A.12.3.1).                         |
| T14 | <i>Backup file secara online</i>            | <i>File</i> pekerjaan tertentu yang dimiliki karyawan biasanya dilakukan <i>backup</i> ke media penyimpanan <i>online</i> seperti Google Drive, Office 365 dan lainnya (A.12.3.1).                                                                                                                     |
| T15 | SIEM AlienVault                             | <i>Server</i> yang mengumpulkan <i>file log</i> tentang aktifitas baik operasional dan keamanan yang terjadi pada <i>server</i> , lalu menganalisa dan melaporkannya secara ringkas melalui <i>dashboard</i> (A.12.4.1).                                                                               |
| T16 | DNS (BIND)                                  | <i>Server</i> yang digunakan untuk pencarian nama domain yang ada didalam jaringan ITS. Selain itu <i>server</i> ini juga digunakan untuk referensi sinkronisasi jam yang sama bagi <i>server</i> dan perangkat jaringan lainnya (A.12.4.4).                                                           |

|     |                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-----|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| T17 | Cisco ASA Firewall                 | Perangkat jaringan yang memiliki kemampuan <i>firewall</i> yang diatur agar membatasi hanya memperbolehkan <i>port</i> tertentu saja dan mengalokasikan domain pada infrastruktur jaringan (A.13.1.1).                                                                                                                                                                                                                                                            |
| T18 | Honeypot Dionaea                   | <i>Server</i> milik KEMENKOMINFO yang berfungsi sebagai <i>decoy</i> untuk mencegah dan mengkarantina <i>malware</i> yang mengeksploitasi melalui jaringan ITS (A.13.1.1).                                                                                                                                                                                                                                                                                        |
| T19 | Tsubame                            | <i>Server</i> milik KEMENKOMINFO yang berfungsi sebagai sensor untuk pengawasan ancaman <i>internet</i> (contohnya infeksi <i>worm</i> ataupun investigasi kerentanan sistem), serta saling berbagi informasi dan analisisnya (A.13.1.1).                                                                                                                                                                                                                         |
| T20 | Sangfor Internet Access Management | Perangkat jaringan untuk mengatur dan melaporkan penggunaan <i>bandwith</i> yang digunakan, seperti mengurangi <i>bandwith</i> media sosial dan media <i>streaming</i> , dan memblokir <i>website</i> yang berbahaya atau melanggar hukum (A.13.1.1).                                                                                                                                                                                                             |
| T21 | Proxy ITS (Squid)                  | <i>Server</i> yang berfungsi sebagai perantara jaringan ITS dengan koneksi luar, penyimpanan <i>cache</i> riwayat halaman <i>website</i> dan alat autentikasi untuk akses <i>internet</i> diarea kampus (A.13.1.1).                                                                                                                                                                                                                                               |
| T22 | Nagios                             | Perangkat lunak untuk <i>server</i> Linux yang berfungsi mengawasi keseluruhan kondisi operasional perangkat jaringan pada infrastruktur jaringan di ITS. Nagios menyediakan laporan analisa tentang kondisi koneksi jaringan secara <i>realtime</i> , seperti apakah terdapat <i>switch</i> dan perangkat <i>fingerprint</i> yang tidak terhubung atau bermasalah. Hasil laporan ditampilkan menggunakan TV LCD didalam ruangan Subdit Infrastruktur (A.13.1.1). |
| T23 | ITS Web Monitoring System          | <i>Website</i> yang dibangun untuk memantau kondisi <i>down</i> atau <i>running</i> -nya semua <i>server</i> yang dikelola oleh DPTSI-ITS secara <i>realtime</i> . Hasil laporan ditampilkan menggunakan TV LCD didalam ruangan Subdit Pelayanan (A.13.1.1).                                                                                                                                                                                                      |

|     |                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-----|----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| T24 | Layanan keamanan <i>ISP</i>            | Layanan keamanan yang disediakan <i>ISP</i> PT. Telkom adalah <i>anti-virus</i> , <i>anti-spam</i> , <i>anti-DDoS</i> yang mem- <i>filter</i> ancaman yang masuk ke jaringan ITS. Untuk <i>availability</i> layanan <i>internet</i> sendiri diharuskan <i>up</i> sebesar 99.75%. Selain itu terdapat <i>VPN</i> untuk jalur koneksi aman dan InternetPositif untuk pemblokiran <i>internet</i> berbahaya dan melanggar hukum (A.13.1.2).                                                                                                             |
| T25 | Jalur <i>ISP</i> yang redundan         | <i>ISP</i> yang digunakan memiliki dua jalur, yaitu IP transit yang utama dan Astine sebagai <i>backup</i> jika yang utama gagal (A.13.1.2).                                                                                                                                                                                                                                                                                                                                                                                                         |
| T26 | Pemisahan jaringan <i>logic</i>        | Pemisahan jaringan secara <i>logic</i> kedalam domain-domain tertentu yang memiliki pengaturan keamanan dan pembatasan yang saling berbeda. Selain itu terdapat domain <i>DMZ</i> yang digunakan untuk melindungi dari akses dari luar melalui <i>server</i> publik kedalam jaringan internal ITS (A.13.1.3).                                                                                                                                                                                                                                        |
| T27 | Pemisahan jaringan fisik               | Pemisahan jaringan secara fisik menggunakan topologi STAR dan RING agar memiliki beberapa titik untuk <i>me-routing</i> jika satu jalur komunikasi terdapat masalah (A.13.1.3).                                                                                                                                                                                                                                                                                                                                                                      |
| T28 | Standar keamanan Google dan Office 365 | Layanan <i>email</i> yang bekerjasama dengan Google akan dilindungi standar keamanan yang disediakan oleh Google, seperti manajemen <i>password</i> , <i>backup</i> data, protokol <i>TLS</i> , <i>anti-spam</i> , <i>anti-virus</i> dan lainnya Sedangkan layanan <i>email</i> yang bekerjasama dengan Microsoft akan dilindungi standar keamanan yang disediakan oleh Microsoft, seperti halaman <i>login</i> , manajemen <i>password</i> , <i>backup</i> data, protokol <i>TLS</i> , <i>anti-spam</i> , <i>anti-virus</i> dan lainnya (A.13.2.3). |
| T29 | Fortigate Anti-Spam                    | Perangkat jaringan yang memiliki kemampuan menyaring semua <i>email</i> masuk yang dicurigai <i>spam</i> dan juga berbahaya (A.13.2.3).                                                                                                                                                                                                                                                                                                                                                                                                              |
| T30 | Lingkungan pengembangan yang aman      | DPTSI-ITS membagi lingkungan pengembangan sistem kedalam tiga tempat, seperti pembuatan di komputer/laptop <i>programmer</i> , pengujian di <i>server development</i> , dan operasional di <i>server live</i> (A.14.2.6 dan A.12.1.4).                                                                                                                                                                                                                                                                                                               |



|     |                                       |                                                                                                                                                                                                                                                                                          |
|-----|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| T31 | Umpan Balik (E-Tiket)                 | <i>Website</i> yang digunakan untuk pelaporan masalah dan insiden yang terkait TIK di ITS. Sistem memiliki fasilitas penggolongan prioritas laporan dan pengiriman <i>screenshoot</i> masalah pada sistem (A.16.1.2).                                                                    |
| T32 | <i>Disaster Recovery Center (DRC)</i> | DPTSI-ITS memasang <i>server co-location</i> di Telkom Gubeng yang melakukan <i>backup</i> data dari <i>server</i> Webmail ITS setiap hari (A.17.1.1).                                                                                                                                   |
| T33 | <i>Server</i> redundan                | <i>Server</i> redundan yang berfungsi jika suatu <i>server</i> operasional gagal berfungsi atau mengalami gangguan maka layanan akan dialihkan ke <i>server</i> redundan (A.17.2.1).                                                                                                     |
| T34 | Komponen redundan                     | Setiap <i>server</i> fisik menggunakan konfigurasi <i>RAID</i> pada <i>hardisk</i> dan konfigurasi <i>multi-channel</i> pada <i>memory</i> (A.17.2.1).                                                                                                                                   |
| T35 | Cadangan komponen atau perangkat      | DPTSI-ITS memiliki cadangan komponen (seperti <i>hardisk</i> ) maupun perangkat (seperti <i>access point</i> , <i>access switch</i> atau <i>distribution switch</i> ) yang dapat digunakan jika terjadi masalah atau kegagalan operasional (A.17.2.1).                                   |
| T36 | Portal perangkat lunak legal          | DPTSI-ITS menyediakan portal untuk mengunduh perangkat lunak berlisensi <i>full version</i> di <a href="http://unduh.its.ac.id">unduh.its.ac.id</a> dan berlisensi <i>open source</i> di <a href="http://boyoy.its.ac.id">boyoy.its.ac.id</a> beserta prosedur pemasangannya (A.18.1.2). |

Tabel I.6 Daftar Kerentanan

| Kode | Kerentanan                                                   | Keterangan                                                                                                                                                                                            |
|------|--------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V1   | Kebijakan masih dalam bentuk <i>draft</i> dan belum ditinjau | Beberapa kebijakan tentang keamanan informasi masih dalam pembuatan dan belum disahkan oleh DPTSI-ITS untuk digunakan (A.5.1.1). Selain itu peninjauan kebijakannya masih belum terlaksana (A.5.1.2). |
| V2   | Kurangnya dokumentasi tugas dan tanggung jawab               | Dokumen Uraian Tugas tidak mencatat semua tugas dan area tanggung jawab yang diemban karyawan                                                                                                         |

|     |                                                        |                                                                                                                                                                                                                                                           |
|-----|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                                        | DPTSI-ITS, terutama yang terkait dengan keamanan informasi (A.6.1.1 dan A.6.1.2).                                                                                                                                                                         |
| V3  | Kurangnya pengelolaan kontak dukungan                  | Tidak adanya dokumentasi prosedur untuk kontak dukungan dengan vendor atau organisasi lain, dan eskalasi masalah yang terjadi (A.6.1.3).                                                                                                                  |
| V4  | Kurangnya pengelolaan <i>forum</i> yang dikunjungi     | Tidak adanya pengelolaan <i>forum</i> apa saja yang diikuti karyawan dan aturan untuk tata cara bertukar informasi didalam forum (A.6.1.4).                                                                                                               |
| V5  | Tidak adanya proses manajemen resiko                   | Tidak adanya perencanaan dan penerapan kontrol keamanan berdasarkan manajemen resiko. Selain itu beberapa mitigasi/penanganan biasanya dilakukan setelah insiden/gangguan terjadi (A.6.1.5).                                                              |
| V6  | Tidak adanya aturan penggunaan perangkat <i>mobile</i> | Tidak adanya dokumentasi kebijakan penggunaan perangkat <i>mobile</i> milik karyawan yang berisikan bagaimana konfigurasi dan kontrol keamanan yang harus dipasang, seperti <i>anti-virus</i> , enkripsi, aplikasi <i>tracking</i> dan lainnya (A.6.2.1). |
| V7  | Tidak adanya aturan penggunaan komputer/laptop         | Tidak adanya dokumentasi kebijakan penggunaan komputer/laptop milik karyawan atau DPTSI-ITS yang berisikan bagaimana konfigurasi dan kontrol keamanan yang harus dipasang, seperti <i>anti-virus</i> , enkripsi, <i>firewall</i> dan lainnya (A.6.2.2).   |
| V8  | Kurangnya pengarahan keamanan sebelum diberikan akses  | Kurangnya pengarahan keamanan informasi sebelum diberikan akses ke sistem informasi yang berisikan apa saja yang harus dilakukan untuk menjaga keamanan informasi (A.7.2.1).                                                                              |
| V9  | Tidak adanya panduan ekspektasi keamanan informasi     | Tidak adanya panduan yang menyatakan ekspektasi keamanan informasi pada peran karyawan didalam organisasi (A.7.2.1).                                                                                                                                      |
| V10 | Tidak adanya pelaporan <i>anonym</i>                   | Tidak adanya sistem pelaporan <i>anonym</i> untuk karyawan yang melanggar kebijakan dan prosedur (A.7.2.1).                                                                                                                                               |
| V11 | Kurangnya kualifikasi yang dimiliki karyawan           | Tidak semua karyawan berkualifikasi untuk melaksanakan tugasnya (contohnya karyawan DPTSI-ITS kurang memiliki sertifikasi Ms.SQL                                                                                                                          |

|     |                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----|--------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                                                                | Server dan pemasangan <i>fiber optic</i> ) (A.7.2.2 dan A.11.2.3). Selain itu pelatihan yang diberikan ke karyawan tidaklah merata dan terkadang hanya 1-2 orang saja yang diberikan/mengikuti pelatihan. Bahkan dokumen Matriks Kebutuhan Pelatihan SDM tidak terbaharui secara berkala.                                                                                                                             |
| V12 | Kurang terencana dan terukurnya program kesadaran keamanan                     | Tidak adanya matriks untuk program kesadaran keamanan yang berisikan perencanaan program seperti dalam Matriks Kebutuhan Pelatihan SDM. Selain itu tidak adanya pengujian tingkat keefektifan program kesadaran keamanan yang dilakukan (A.7.2.2).                                                                                                                                                                    |
| V13 | Tidak adanya pemberitahuan tanggung jawab setelah keluar/mutasi kerja karyawan | Tidak ada penjelasan tanggung jawab karyawan setelah diberhentikan, contohnya perjanjian ataupun pemberitahuan ulang kepada karyawan bahwa informasi/rahasia organisasi harus dijaga meski karyawan sudah keluar (A.7.3.1).                                                                                                                                                                                           |
| V14 | Kurang terincinya Daftar Rekaman Mutu                                          | Daftar dokumentasi aset informasi tidak merinci secara lengkap data dan informasi baik yang <i>softcopy/hardcopy</i> yang tersebar dimasing-masing Subdit (A.8.1.1).                                                                                                                                                                                                                                                  |
| V15 | Kurangnya dokumentasi pemilik aset                                             | Kurangnya pendokumentasian pemilik aset yang bertanggung jawab terhadap aset, yang ada hanya aset sistem informasi terpadu yang dikembangkan oleh Subdit Pengembangan (A.8.1.2).                                                                                                                                                                                                                                      |
| V16 | Kurang lengkapnya aturan penggunaan perangkat yang ada                         | Tidak adanya kebijakan penggunaan komputer dan laptop dinas, <i>internet/intranet</i> dan media sosial, perangkat lunak, dan perangkat lainnya (A.8.1.3).                                                                                                                                                                                                                                                             |
| V17 | Kesalahan pembuatan dan kurang jelasnya instruksi kerja di ISO 9000            | <ul style="list-style-type: none"> <li>• Terdapat kesalahan dalam pembuatan instruksi kerja seperti instruksi Penggunaan <i>Server</i>, <i>Crimping Tools</i> dan lainnya. Instruksi kerja seharusnya menjelaskan secara rinci langkah dan merujuk aktifitas didalam dokumen prosedur saja.</li> <li>• Didalam instruksi kerja penggunaan <i>server</i> dituliskan “Apabila terjadi <i>trouble</i> lakukan</li> </ul> |

|     |                                                                    |                                                                                                                                                                                                                    |
|-----|--------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                                                    | analisa”, namun tidak menjelaskan bagaimana cara menganalisanya (A.8.1.3).                                                                                                                                         |
| V18 | Kurangnya proses pengembalian aset                                 | Tidak adanya dokumentasi prosedur pengembalian aset yang dipinjam karyawan yang berhenti atau mutasi kerja (A.8.1.4).                                                                                              |
| V19 | Tidak adanya penyerapan ilmu yang dimiliki karyawan                | Tidak adanya penerapan <i>knowledge management</i> untuk mendokumentasikan ilmu-ilmu baru yang dimiliki karyawan selama bekerja (A.8.1.4).                                                                         |
| V20 | Tidak ada dokumentasi klasifikasi informasi                        | Klasifikasi kerahasiaan informasi sudah pernah ditetapkan, namun klasifikasi tidak terdokumentasi dan masih berada dalam pikiran masing-masing pihak yang bisa terdapat perbedaan antara satu sama lain (A.8.2.1). |
| V21 | Tidak ada pemberian <i>label</i> berdasarkan klasifikasi informasi | Tidak ada pemberian <i>label</i> pada aset informasi berdasarkan klasifikasi informasi yang ada (A.8.2.2).                                                                                                         |
| V22 | Kurangnya proses penanganan aset                                   | Tidak ada panduan yang lengkap menjelaskan penanganan aset informasi tertentu secara aman, seperti bagaimana cara menyimpan, mengirim dan menghapus/memusnahkannya (A.8.2.3).                                      |
| V23 | Tidak adanya prosedur tentang <i>removable media</i>               | Tidak adanya prosedur khusus yang mengatur bagaimana penggunaan <i>removable media</i> seperti <i>flashdisk</i> , <i>hardisk</i> eksternal, <i>memory card</i> dan penyimpan eksternal lainnya (A.8.3.1).          |
| V24 | Kurangnya aktifitas penyediaan hak akses                           | Kurangnya dokumentasi prosedur dan rekaman untuk setiap aktifitas penyediaan hak akses pengguna (A.9.2.2).                                                                                                         |
| V25 | Kurangnya aktifitas penghapusan hak akses                          | Kurangnya dokumentasi prosedur dan rekaman untuk setiap aktifitas penghapusan hak akses pengguna (A.9.2.2 dan A.9.2.6).                                                                                            |
| V26 | Kurangnya rekaman hak akses yang diberikan                         | Tidak adanya perekaman hak akses yang dimiliki oleh karyawan kedalam <i>server</i> , perangkat lunak, perangkat jaringan dan komputer/laptop dinas (A.9.2.2).                                                      |

|     |                                                                              |                                                                                                                                                                                                                                                                                                                                                                                        |
|-----|------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V27 | Kurangnya penerapan <i>least privilege</i>                                   | Kurangnya pemberian hak akses yang bertingkat pada <i>server</i> dan tidak adanya pembatasan hak akses pada komputer dan laptop dinas karena semua hak akses bersifat <i>administrator</i> (A.9.2.3).                                                                                                                                                                                  |
| V28 | Tidak adanya pengelolaan hak akses                                           | Tidak adanya identifikasi hak akses yang dimiliki oleh sistem, tidak tersedianya hak akses tertentu yang memiliki jangka waktu berlaku, dan tidak adanya pemisahan penggunaan hak akses <i>administrator</i> dengan penggunaan biasa (A.9.2.3).                                                                                                                                        |
| V29 | Tidak adanya pengelolaan <i>sharing password</i> dan <i>password default</i> | Tidak adanya dokumentasi prosedur untuk pengecekan <i>password default</i> pada perangkat, dan prosedur pengelolaan <i>password</i> yang dibagikan kepada karyawan (A.9.2.3)                                                                                                                                                                                                           |
| V30 | Kurang amannya <i>password</i> sementara yang diberikan                      | <i>Password</i> sementara akun <i>email</i> yang diberikan saat <i>reset password</i> oleh Subdit Pelayanan tidaklah unik dan mudah ditebak, dilakukan pengiriman <i>password</i> sementara melalui <i>email</i> , serta tidak ada pemaksaan penggantian <i>password</i> sementara pada Webmail ITS (A.9.2.4).                                                                         |
| V31 | Kurangnya aktifitas <i>reset password</i>                                    | Tidak adanya dokumentasi prosedur dan rekaman untuk setiap aktifitas <i>reset password</i> untuk sistem informasi selain Webmail ITS, <i>server</i> , perangkat jaringan atau komputer/laptop dinas (A.9.2.4). Selain itu ketika pengguna meminta untuk merubah <i>password</i> , tidak ada perekaman apakah memang dikarenakan lupa atau dicurigai akun dibuka orang lain tanpa izin. |
| V32 | Kurangnya aktifitas peninjauan hak akses                                     | Tidak adanya dokumentasi prosedur dan rekaman untuk setiap aktifitas peninjauan hak akses pengguna pada <i>server</i> , perangkat lunak dan perangkat jaringan. Selain itu tidak dilakukan peninjauan untuk akun <i>email</i> Webmail ITS dan kontrol fisik (perangkat <i>fingerprint</i> dan kunci pintu <i>analog</i> ) (A.9.2.5).                                                   |
| V33 | Kurangnya aktifitas penghapusan hak akses fisik                              | Tidak adanya dokumentasi prosedur untuk penghapusan atau pencabutan hak akses fisik yang ada (A.9.2.6).                                                                                                                                                                                                                                                                                |

|     |                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V34 | Kurangnya prosedur <i>login</i> yang aman pada Webmail ITS | Webmail ITS tidak memiliki laporan setiao percobaan <i>login</i> yang berhasil/gagal, tidak menonaktifkan pesan bantuan untuk lupa <i>password</i> , dan lainnya (A.9.4.2).                                                                                                                                                                                                                                                                                                                |
| V35 | Kurangnya sistem manajemen <i>password</i> yang aman       | <ul style="list-style-type: none"> <li>• Webmail ITS tidak memaksa agar pengguna menggunakan kombinasi huruf besar-kecil, angka dan simbol, dan merubah <i>password</i> secara berkala ataupun saat <i>password</i> di-reset.</li> <li>• <i>Server</i> tidak memaksa agar pengguna merubah <i>password</i> secara berkala.</li> <li>• Perangkat komputer dan laptop dinas milik DPTSI-ITS tidak memaksa pengguna untuk menggunakan standar <i>password</i> yang aman (A.9.4.3).</li> </ul> |
| V36 | Tidak adanya pembatasan aplikasi utilitas                  | Tidak adanya batasan penggunaan aplikasi utilitas atau fungsi tertentu yang mampu merubah sistem (CMD, terminal dan lainnya) pada <i>server</i> dan komputer/laptop dinas (A.9.4.4)                                                                                                                                                                                                                                                                                                        |
| V37 | Kurangnya pengelolaan <i>source code</i>                   | Tidak adanya dokumentasi prosedur pengelolaan <i>source code</i> yang berisikan langkah-langkah dalam pembuatan <i>source code</i> dari awal berikut penempatannya, sampai <i>source code</i> selesai dan dipasang kedalam <i>server</i> (A.9.4.5).                                                                                                                                                                                                                                        |
| V38 | Tidak terlindunginya media penyimpanan                     | Perlindungan enkripsi tidak mencakup <i>hardisk</i> dan media penyimpanan lainnya, hanya mencakup jalur komunikasi dan <i>password</i> di <i>database</i> (A.10.1.1).                                                                                                                                                                                                                                                                                                                      |
| V39 | Tidak adanya aturan enkripsi dan manajemen kunci           | Tidak adanya dokumentasi apa saja yang dienkripsi, yang menerapkan kebijakan dan manajemen kunci, aturan penggunaan enkripsi, dan lainnya (A.10.1.1).Selain itu tidak adanya dokumentasi terkait daur hidup kunci enkripsi baik dalam pembuatan, pendistribusian, penyimpanan dan penghapusan (A.10.1.2).                                                                                                                                                                                  |
| V40 | Protokol <i>TSL</i> versi lama                             | Terdapat halaman <i>login</i> pada <i>website</i> yang protokol <i>TSL</i> -nya menggunakan versi lama yaitu versi 1.0,                                                                                                                                                                                                                                                                                                                                                                    |

|     |                                                             |                                                                                                                                                                                                                                           |
|-----|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |                                                             | pada Webmail ITS. Hal ini dapat dilihat pada Gambar F.67, Gambar F.68, dan Gambar F.70.                                                                                                                                                   |
| V41 | Tidak adanya pendeteksi pencurian                           | Tidak adanya pendeteksi aksi percobaan pencurian seperti <i>alarm</i> yang dipasang disetiap pintu keluar atau jendela yang dapat diakses pada ruangan pusat data atau ruangan lainnya (A.11.1.1).                                        |
| V42 | Tidak adanya aturan kontrol akses fisik                     | Tidak adanya dokumentasi kebijakan kontrol akses fisik yang menjelaskan aturan keluar masuk kantor dan yang harus dilakukan karyawan untuk menangani pengunjung (A.11.1.2).                                                               |
| V43 | Kurangnya pengelolaan pengunjung                            | Tidak adanya aktifitas autentikasi identitas pengunjung yang datang, tidak adanya daftar tamu, dan tidak dilakukannya pengelolaan dan peninjauan rekaman akses keluar-masuk (A.11.1.2).                                                   |
| V44 | Tidak adanya tanda pengenalan dikawasan kantor              | Tidak adanya tanda pengenalan atau identitas lainnya bagi pengunjung dan karyawan untuk digunakan didalam kantor (A.11.1.2).                                                                                                              |
| V45 | Mudahnya mengidentifikasi maksud ruangan                    | Ruangan pusat data ada didalam ruangan Subdit Infrastruktur, dimana ruangan pusat data memiliki pintu dan jendela kaca yang memudahkan untuk mengawasi dari luar. Serta ruangan Subdit Infrastruktur juga memiliki pintu kaca (A.11.1.3). |
| V46 | Tidak adanya pengelolaan dan peninjauan akses ke pusat data | Tidak adanya dokumentasi prosedur pengelolaan setiap akses yang dilakukan kedalam ruangan pusat data baik untuk karyawan Subdit Infrastruktur dan bukan (A.11.1.5).                                                                       |
| V47 | Tidak adanya pemeriksaan kiriman berbahaya                  | Tidak adanya prosedur dan perangkat pemeriksaan kiriman dari bahan peledak, benda tajam, kimia/beracun, pemalsuan, dan lainnya kedalam kantor (A.11.1.6).                                                                                 |
| V48 | Tidak adanya ruangan khusus bongkar muat                    | Tidak ada ruangan yang khusus untuk aktifitas bongkar-muat barang dan pemeriksaannya (A.11.1.6).                                                                                                                                          |
| V49 | Tidak adanya alat pengecekan interferensi <i>WiFi</i>       | Tidak adanya perangkat untuk mengecek interferensi antar sinyal yang dipancarkan dengan frekuensi yang sama (A.11.2.1).                                                                                                                   |

|     |                                                          |                                                                                                                                                                                                                                                           |
|-----|----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V50 | Kurangnya perlindungan kegagalan daya                    | Perlindungan untuk pemadaman listrik tidak melindungi semua perangkat (seperti <i>access switch</i> ), dan hanya melindungi sebagian komputer dengan <i>UPS</i> (A.11.2.2).                                                                               |
| V51 | Tidak adanya redundansi <i>ISP</i>                       | <i>ISP</i> yang digunakan hanya ada satu yaitu PT. Telkom dan tidak redundan (A.11.2.2 dan A.13.1.2).                                                                                                                                                     |
| V52 | Kurangnya alat bantu untuk kabel <i>fiber optic</i>      | Kurangnya perangkat serta panduan untuk pemasangan dan perbaikan kabel <i>fiber optic</i> . Pemasangan dan perbaikannya hanya bisa dilakukan oleh vendor (A.11.2.3).                                                                                      |
| V53 | Kurangnya pemeliharaan perlengkapan                      | Perawatan yang dilakukan tidak mencakup komputer ataupun laptop dinas secara khusus. Selain itu terdapat perangkat yang tidak memiliki dokumentasi prosedurnya seperti <i>server</i> (A.11.2.4).                                                          |
| V54 | Kurangnya penjadwalan dan pencatatan perawatan perangkat | Perawatan perangkat secara fisik dilakukan, namun tidak ada catatan apa saja yang sudah dirawat dan aktifitas tidak terjadwal secara berkala. Selain itu tidak adanya rekaman perbaikan perangkat (A.11.2.4).                                             |
| V55 | Kurangnya pengecekan <i>BIOS</i> perangkat               | Setiap perangkat keras dan jaringan yang diterima setelah diperbaiki ataupun baru dibeli dari vendor tidak diperiksa apakah perangkat dirubah tanpa izin melalui pengecekan kode pada <i>BIOS</i> dengan yang ada di <i>website</i> perangkat (A.11.2.4). |
| V56 | Tidak ada pengecekan barang bawaan                       | Tidak adanya pengecekan barang bawaan karyawan ataupun pengunjung untuk memeriksa apakah terdapat barang curian, berbahaya atau lainnya (A.11.2.5).                                                                                                       |
| V57 | Kurangnya pengelolaan media yang dibuang                 | Tidak adanya dokumentasi prosedur pembuangan secara aman media penyimpanan elektronik. Selain itu tidak ada penanganan khusus untuk <i>CD/DVD</i> (A.11.2.7).                                                                                             |
| V58 | Tidak adanya <i>screensaver</i> dengan <i>password</i>   | Perangkat komputer dan laptop dinas milik DPTSI-ITS tidak diatur agar menjalankan <i>screensaver</i> yang diberi <i>password</i> ketika tidak digunakan atau ditinggal (A.11.2.8).                                                                        |



|     |                                                    |                                                                                                                                                                                                                                                     |
|-----|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V59 | Tidak adanya aturan <i>clear desk and screen</i>   | Tidak adanya dokumentasi kebijakan terkait kerapian meja kerja dan membersihkan layar monitor komputer/laptop dinas (A.11.2.9).                                                                                                                     |
| V60 | Kurangnya dokumentasi prosedur yang ada            | Beberapa prosedur yang ada didalam dokumen ISO 9000 kurang lengkap karena beberapa prosedur belum terdokumentasikan dan masih dalam bentuk <i>draft</i> (A.12.1.1).                                                                                 |
| V61 | Kurangnya pembaharuan dokumen ISO 9000             | Dokumen ISO 9000 yang dimiliki DPTSI-ITS belum diperbaharui selama 3 tahun untuk menyesuaikan dengan pembaharuan yang telah dilakukan (contohnya struktur organisasi, nama organisasi, uraian tugas, aturan baru, dan dokumen lainnya).             |
| V62 | Kurangnya aturan dan prosedur manajemen perubahan  | Kurangnya dokumentasi kebijakan dan prosedur untuk mengelola perubahan yang terjadi di organisasi secara lengkap, hanya ada prosedur yang berhubungan dengan sistem informasi yang dikembangkan DPTSI-ITS dan konfigurasi jaringan saja (A.12.1.2). |
| V63 | Kurangnya rencana manajemen kapasitas              | Tidak adanya dokumentasi terkait perencanaan manajemen kapasitas untuk memenuhi kebutuhan kedepan baik sumber daya yang terkait sistem/jaringan dan karyawan (A.12.1.3).                                                                            |
| V64 | Kurangnya aturan pemisahan lingkungan              | Tidak adanya dokumentasi kebijakan terkait pemindahan perangkat lunak yang dikembangkan didalam lingkungan pengembangan (A.12.1.4).                                                                                                                 |
| V65 | Kurangnya penanganan <i>malware</i> yang dilakukan | Tidak adanya dokumentasi kebijakan dan prosedur terkait <i>malware</i> yang memberikan peringatan dan penanganan jika terjadi serangan <i>malware</i> pada sistem (A.12.2.1).                                                                       |
| V66 | Tidak adanya aturan <i>backup</i>                  | Tidak adanya dokumentasi kebijakan terkait <i>backup</i> yang dilakukan dan pengelolaannya (A.12.3.1).                                                                                                                                              |
| V67 | Hasil <i>backup</i> tidak berganda                 | <i>Backup</i> tidak disimpan secara berganda untuk mencegah <i>corrupt</i> pada satu hasil <i>backup</i> . Untuk data <i>server</i> dilakukan sinkronisasi dimana penimpanan <i>file backup</i> yang lama (A.12.3.1).                               |

|     |                                                                      |                                                                                                                                                                                                                                            |
|-----|----------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V68 | Tidak ada pengujian hasil <i>backup</i>                              | <i>Backup</i> yang dilakukan tidak diuji secara berkala pada waktu tertentu, apakah data yang disimpan tidak terdapat masalah dan bisa digunakan untuk melakukan <i>restore</i> (A.12.3.1).                                                |
| V69 | Perangkat <i>backup</i> dan yang di <i>backup</i> dilokasi yang sama | <i>Server backup</i> ditempatkan di ruangan pusat data, tidak ditaruh di gedung/lokasi lain untuk mencegah jika terjadi bencana alam (A.12.3.1).                                                                                           |
| V70 | Kurangnya cakupan <i>SIEM</i> AlienVault                             | Tidak semua perangkat yang disimpan <i>file log</i> -nya oleh <i>SIEM</i> seperti komputer/laptop dinas dan <i>server development</i> (A.12.4.1).                                                                                          |
| V71 | Tidak adanya perlindungan <i>log administrator</i>                   | Tidak adanya perlindungan <i>log</i> dari aktifitas yang dilakukan <i>administrator</i> pada Webmail ITS, <i>server</i> dan perangkat jaringan (A.12.4.3).                                                                                 |
| V72 | Kurangnya pengaturan sinkronisasi jam                                | Tidak semua perangkat dilakukan sinkronisasi jam, seperti <i>server development</i> dan komputer/laptop dinas (A.12.4.4).                                                                                                                  |
| V73 | Tidak adanya aturan pemasangan perangkat lunak                       | Tidak adanya dokumentasi kebijakan dan prosedur pemasangan perangkat lunak yang tidak dikembangkan di komputer dan <i>server</i> , selain itu tidak adanya sistem manajemen konfigurasi yang digunakan pengaturan konfigurasi (A.12.5.1).  |
| V74 | Kurangnya manajemen kerentanan teknis                                | Pemasangan <i>patch</i> dilakukan oleh masing-masing karyawan yang bertanggung jawab tanpa adanya kebijakan dan prosedur bakunya. Selain itu tidak ada rekaman perangkat mana yang sudah ter- <i>patch</i> dan mana yang belum (A.12.6.1). |
| V75 | Tidak adanya pembatasan pemasangan perangkat lunak                   | Tidak adanya pembatasan perangkat lunak yang boleh dan tidak boleh dipasang di komputer atau laptop dinas yang digunakan oleh karyawan (A.12.6.2).                                                                                         |
| V76 | Tidak adanya audit sistem informasi                                  | Tidak adanya aktifitas audit/evaluasi terhadap sistem informasi yang dimiliki serta dokumentasi prosedurnya (A.12.7.1).                                                                                                                    |
| V77 | Tidak adanya aturan pertukaran informasi                             | Tidak adanya dokumentasi kebijakan dan prosedur pertukaran informasi secara aman (A.13.2.1).                                                                                                                                               |

|     |                                                                           |                                                                                                                                                                                                                                                                                                 |
|-----|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V78 | Tidak adanya perjanjian pertukaran informasi dengan pihak ketiga          | Tidak adanya perjanjian khusus yang berkaitan dengan pertukaran yang aman informasi bisnis antara DPTSI-ITS dengan pihak ketiga (A.13.2.2).                                                                                                                                                     |
| V79 | Kurangnya kontrol untuk <i>email spam</i>                                 | Kurangnya kontrol keamanan dari sisi aplikasi untuk mencegah <i>email spam</i> yang masuk, seperti <i>filter</i> otomatis atau tombol penanda <i>email spam</i> yang dapat memasukkan <i>email</i> kedalam <i>folder</i> khusus <i>spam</i> dan memberitahukan <i>administrator</i> (A.13.2.3). |
| V80 | Tidak adanya kontrol tambahan untuk <i>email</i>                          | Tidak adanya aturan penggunaan media sosial, dan autentikasi tambahan untuk mengontrol akses dari koneksi jaringan publik (A.13.2.3).                                                                                                                                                           |
| V81 | <i>Email</i> ITS dikenali sebagai <i>spam</i>                             | <i>Email</i> ITS yang dikirim ke penyedia layanan <i>email</i> lain dikenali sebagai <i>spam</i> dan masuk kedalam <i>folder spam</i> .                                                                                                                                                         |
| V82 | Kurangnya perjanjian menjaga kerahasiaan bagi karyawan                    | Perjanjian menjaga kerahasiaan yang ada hanyalah sumpah PNS bagi karyawan PNS dan kesepakatan bersama menjaga kerahasiaan bagi Subdit Pengembangan. Tidak ada perjanjian secara formal untuk karyawan lainnya (A.13.2.4).                                                                       |
| V83 | Tidak adanya acuan identifikasi persyaratan pengembangan sistem informasi | Tidak adanya penggunaan standar atau metode tertentu untuk mengidentifikasi persyaratan keamanan minimum didalam proyek pengembangan sistem informasi (A.14.1.1) ataupun ketika pengujian sistemnya (A.14.2.9).                                                                                 |
| V84 | Kurangnya pengelolaan perubahan paket perangkat lunak                     | Setiap modifikasi paket perangkat lunak yang dilakukan oleh petugas ketika pemasangan tidak diatur, diuji dan didokumentasikan secara formal (A.14.2.4).                                                                                                                                        |
| V85 | Tidak adanya standar dalam pemrograman                                    | Tidak adanya standar teknis dan <i>source code</i> yang digunakan untuk pemrograman yang aman untuk bahasa pemrograman <i>PHP</i> dan <i>My SQL Server</i> (A.14.2.5).                                                                                                                          |
| V86 | Tidak adanya prosedur di                                                  | Tidak adanya dokumentasi prosedur untuk proses pengembangan untuk SIM tertentu maupun aktifitas                                                                                                                                                                                                 |

|     |                                                           |                                                                                                                                                                                                                                                             |
|-----|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | lingkungan pengembangan                                   | manajemen resikonya didalam lingkungan pengembangan sistem (A.14.2.6).                                                                                                                                                                                      |
| V87 | Tidak adanya metode peninjauan <i>source code</i>         | Tidak adanya metode yang meninjau apakah didalam <i>source code</i> terdapat kode berbahaya atau kerentanan baik yang dimasukkan <i>programmer</i> secara sengaja atau tidak (A.14.2.9).                                                                    |
| V88 | Tidak adanya alat bantu dalam pengujian penerimaan sistem | Tidak adanya penggunaan standar, alat ukur, ataupun perangkat uji sistem apapun yang dapat membantu ketika pengujian penerimaan sistem (A.14.2.9).                                                                                                          |
| V89 | Tidak adanya prosedur peninjauan layanan                  | Tidak adanya dokumentasi prosedur untuk peninjauan kesesuaian layanan TIK dengan yang dijanjikan didalam kontrak (A.15.2.1).                                                                                                                                |
| V90 | Tidak adanya prosedur perubahan ketentuan layanan         | Tidak adanya dokumentasi prosedur perubahan ketentuan layanan TIK jika vendor merubah ketentuan dari yang telah dijanjikan didalam kontrak (A.15.2.2).                                                                                                      |
| V91 | Kurangnya prosedur dan panduan penanganan insiden         | Kurangnya dokumentasi prosedur yang digunakan sebagai acuan petugas untuk menangani insiden tertentu seperti <i>troubleshooting</i> untuk perangkat keras/lunak tertentu, pemulihan data/konfigurasi yang hilang/rusak dan lainnya (A.16.1.1 dan A.16.1.5). |
| V92 | Tidak adanya keharusan pelaporan kerentanan               | Tidak adanya sosialisasi dan pemberitahuan apapun agar pengguna sistem atau layanan dapat mengidentifikasi dan melaporkan jika ditemukan kerentanan (A.16.1.3).                                                                                             |
| V93 | Kurangnya penilaian dan keputusan dalam insiden           | Tidak adanya penilaian serta keputusan mana keluhan dan insiden yang akan dikerjakan terlebih dahulu menggunakan metode tertentu yang terdokumentasi (A.16.1.4).                                                                                            |
| V94 | Tidak adanya prosedur eskalasi dan komunikasi insiden     | Tidak adanya dokumentasi prosedur untuk penanganan insiden dan pengkomunikasiannya ke pemangku kepentingan terkait agar mengurangi kemungkinan dan dampak insiden (A.16.1.6).                                                                               |

|      |                                                                  |                                                                                                                                                                                                                                                                                                                             |
|------|------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V95  | Kurangnya penanganan bukti forensik                              | Tidak adanya peran/tanggung jawab khusus, sertifikasi/kualifikasi, dan dokumentasi prosedur untuk penanganan bukti forensik yang akan dijadikan bukti hukum (A.16.1.7).                                                                                                                                                     |
| V96  | Tidak adanya dokumen <i>BCP</i> atau <i>DRP</i>                  | Tidak adanya dokumentasi prosedur dan penggunaan kerangka kerja apapun terkait <i>BCP</i> atau <i>DRP</i> (A.17.1.2).                                                                                                                                                                                                       |
| V97  | Tidak adanya penanggung jawab <i>BCP</i> atau <i>DRP</i>         | Tidak adanya pembuatan struktur manajemen ataupun penunjukan khusus untuk karyawan yang melakukan aktifitas <i>BCP</i> atau <i>DRP</i> (A.17.1.2).                                                                                                                                                                          |
| V98  | Tidak adanya pengujian <i>BCP</i> dan <i>DRP</i>                 | Karena <i>BCP</i> dan <i>DRP</i> belum didokumentasikan dan direncanakan, tidak adanya pengujian secara formal <i>BCP</i> dan <i>DRP</i> yang diterapkan (A.17.1.3).                                                                                                                                                        |
| V99  | Kurangnya cadangan komponen dan perangkat                        | Tidak tersedianya cadangan komponen perangkat (seperti <i>processor</i> atau <i>memory</i> ) dan perangkat (seperti <i>firewall</i> , <i>core switch</i> , atau perangkat lainnya yang mahal) jika terjadi masalah atau kegagalan operasional (A.17.2.1).                                                                   |
| V100 | Kurangnya perlindungan dari pelanggaran hak kekayaan intelektual | Tidak adanya kebijakan, prosedur, program kesadaran keamanan ataupun penerapan kontrol untuk memastikan semua perangkat lunak yang dipasang di komputer berlisensi <i>full version</i> , <i>freeware</i> atau <i>open source</i> , dan tidak melanggar hak kekayaan intelektual didalam ruang lingkup DPTSI-ITS (A.18.1.2). |
| V101 | Kurangnya audit keamanan informasi                               | Kurangnya aktifitas audit tentang keamanan informasi formal baik secara internal maupun eksternal karena masih belum mengadopsi standar apapun (A.18.2.1).                                                                                                                                                                  |
| V102 | Tidak adanya tinjauan pihak manajemen                            | Tidak adanya tinjauan kebijakan, prosedur, standar dan persyaratan keamanan lainnya oleh pihak manajemen untuk melihat <i>non-conformity</i> karena masih belum mengadopsi standar keamanan informasi apapun (A.18.2.2).                                                                                                    |
| V103 | Kurangnya peninjauan                                             | Kurangnya aktifitas tes penetrasi dan pemindaian kerentanan berikut dokumentasi prosedurnya untuk menguji keamanan sistem informasi terpadu dan                                                                                                                                                                             |

|      |                                                      |                                                                                                                                                                                                                                                       |
|------|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | kepatuhan teknis pada sistem                         | infrastruktur jaringan saat pengembangan atau operasional (A.18.2.3 dan A.14.2.9).                                                                                                                                                                    |
| V104 | Kurangnya penggunaan Git ITS                         | Tidak semua <i>source code</i> dimasukkan kedalam Git ITS, dimana sistem informasi yang baru saja yang dimasukkan.                                                                                                                                    |
| V105 | Pasokan listrik tidak selalu stabil                  | Pasokan listrik yang disediakan oleh PLN tidak selalu berjalan stabil, dimana terkadang terjadi mati lampu pada waktu tertentu tanpa pemberitahuan atau pada saat turun hujan.                                                                        |
| V106 | Tegangan listrik tidak selalu stabil                 | Pasokan listrik yang disediakan oleh PLN tidak selalu mengalirkan tegangan listrik yang stabil dan aman, contohnya dari tegangan tinggi dan lonjakan.                                                                                                 |
| V107 | Mudahnya terjadinya interfensi pada sinyal dan kabel | Sambungan non-kabel ( <i>WiFi</i> ) atau kabel jaringan mudah terkena interfensi jika terdapat sinyal <i>WiFi</i> pada gelombang yang sama atau pemasangan kabel listrik yang didekatkan dengan kabel jaringan.                                       |
| V108 | Layanan <i>ISP</i> tidak selalu stabil               | Koneksi <i>internet</i> yang disediakan oleh <i>ISP</i> tidak selamanya berjalan stabil, dimana terkadang terjadi kegagalan koneksi pada waktu tertentu tanpa pemberitahuan.                                                                          |
| V109 | Tidak ada jaminan dukungan vendor selamanya          | Tidak ada layanan dan dukungan produk yang disediakan oleh vendor bisa dijamin berjalan selamanya dikarenakan vendor bangkrut, menghentikan dukungan pada layanan/produk, atau merubah ketentuan pada layanan.                                        |
| V110 | Tidak ada jaminan kepatuhan perjanjian dan ketentuan | Tidak ada jaminan bahwa perjanjian dan kepatuhan yang dibuat dan harus dipatuhi pengguna sistem, karyawan dan vendor selalu dipatuhi.                                                                                                                 |
| V111 | Koneksi jaringan <i>intranet &amp; internet</i>      | Koneksi <i>intranet</i> dan <i>internet</i> dapat digunakan sebagai jalur beberapa potensi ancaman pada keamanan informasi seperti <i>denial of service</i> , penyebaran <i>malware</i> , <i>eavesdropping</i> , <i>website deface</i> , dan lainnya. |
| V112 | Kurangnya pengetahuan tentang                        | Kurangnya pengetahuan tentang perbaikan perangkat yang dibeli secara detail, karena jika terjadi masalah serius pada perangkat maka                                                                                                                   |

|      |                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | perbaikan perangkat secara detail                                 | tindakan yang dilakukan adalah menghubungi vendornya.                                                                                                                                                                                                                                                                                                                                                                                      |
| V113 | Telatnya rilis <i>patch</i> pada perangkat                        | Telat rilisnya <i>patch</i> terbaru untuk perangkat keras, perangkat lunak atau perangkat jaringan untuk menangani masalah keamanan dan operasional yang ada.                                                                                                                                                                                                                                                                              |
| V114 | Perangkat telah melewati batas umur garansi                       | Terdapat beberapa perangkat keras/jaringan (seperti <i>server</i> , <i>router</i> , <i>firewall</i> ) dan perangkat pelengkap (seperti <i>AC</i> , <i>UPS</i> , <i>diesel generator</i> ) yang sudah berumur dan melewati masa garansi.                                                                                                                                                                                                    |
| V115 | Perangkat beroperasi tanpa henti                                  | Beberapa perangkat keras/jaringan (seperti <i>server</i> , <i>router</i> , <i>firewall</i> ) dan perangkat pelengkap (seperti <i>AC</i> , <i>UPS</i> , <i>diesel generator</i> ) beroperasi tanpa henti 24 jam x 7 hari.                                                                                                                                                                                                                   |
| V116 | Temperatur perangkat saat beroperasi                              | Setiap perangkat keras/jaringan seperti <i>server</i> , komputer, <i>switch</i> , <i>router</i> dan lainnya mengeluarkan panas saat beroperasi dan bersifat merusak, apalagi jika penggunaannya melebihi kapasitas.                                                                                                                                                                                                                        |
| V117 | Banyaknya jumlah pengguna                                         | Banyaknya jumlah pemangku kepentingan di ITS yang menggunakan layanan TIK, seperti dosen berjumlah 970 orang, karyawan berjumlah 1.135 orang dan mahasiswa berjumlah 17.625 orang.                                                                                                                                                                                                                                                         |
| V118 | Rusaknya patok penanda kabel                                      | Penanda kabel yang dipasang untuk menandakan lokasi kabel terdapat kerusakan atau hilang. Hal ini dapat dilihat pada Gambar F.100. Bahkan beberapa penanda tidak menggunakan standar aslinya, malah menggunakan batu bata merah sebagai penggantinya.                                                                                                                                                                                      |
| V119 | Kurangnya praktik keamanan informasi yang dilakukan oleh karyawan | Karyawan (atau kontraktor) tidak atau kurang melakukan praktik keamanan informasi (bisa dikarenakan lupa), seperti tidak melakukan <i>log-out</i> , meninggalkan perangkat laptop/mobile ditempat umum, tidak melihat sekitar ketika memasukkan <i>password</i> , lupa mengunci pintu, lupa menaruh dokumen, kurangnya pengawasan saat proyek pembangunan, kurangnya pengawasan hasil dari aktifitas yang dilakukan karyawan, dan lainnya. |

|      |                           |                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| V120 | Kurangnya jumlah karyawan | Jumlah karyawan yang bekerja di DPTSI-ITS tidaklah cukup, dimana terdapat karyawan mengerjakan tugas diluar tanggung jawabnya dan perangkapan peran. Misalnya terdapat diluar Subdit Pengembangan yang melakukan didalam pengembangan sistem informasi, atau perangkapan peran karyawan (contohnya analis sistem dirangkap menjadi <i>programmer</i> atau bahkan satu karyawan merangkap dari analis sistem sampai penguji sistem). |
|------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



Tabel I.7 Lembar Kerja Penilaian Resiko Direktur DPTSI-ITS

| Nomor Resiko | Aset | Ancaman | Kontrol Keamanan                                  | Kerentanan                                                                                            | Aspek CIA | Dampak | Probabilitas | Level Resiko |
|--------------|------|---------|---------------------------------------------------|-------------------------------------------------------------------------------------------------------|-----------|--------|--------------|--------------|
| D1           | AS50 | AN16    | A2, A5-A9, A13, A14, A35, A53, A56, A57, A59      | V4, V11, V19, V91, V92, V94, V95, V112                                                                | I         | 2      | 2            | 4            |
| D2           |      | AN19    | A7, A8, A12-A14, A17, A18, A22, A35, A45          | V1, V6-V9, V11, V16, V17, V19, V22, V23, V36, V39, V60, V61, V70, V73, V75, V76                       | CI        | 1      | 2            | 2            |
| D3           |      | AN28    | A4, A15, A37, P24                                 | V5, V11, V63, V120                                                                                    | A         | 3      | 2            | 6            |
| D4           |      | AN40    | A4, A7, A10, A15, A24, A26, A28, A33, A42, A57    | V1, V2, V10, V13, V15, V22, V24-V28, V31, V32, V36, V38, V70, V71, V73, V77, V78, V82, V95 V101, V102 | IA        | 3      | 1            | 3            |
| D5           |      | AN46    | A11, A29                                          | V1, V8, V9, V12, V16, V22, V23, V32, V39, V60, V61, V73, V77, V78, V80, V94, V101, V102, V110, V119   | C         | 3      | 2            | 6            |
| D6           | AS51 | AN17    | A2, A7-A9, A13, A14, A35, A55, A56, A58, A59, T31 | V3, V4, V11, V19, V92-V94                                                                             | I         | 2      | 1            | 2            |
| D7           |      | AN19    | A7, A8, A12-A14, A17, A18, A22, A35, A45          | V1, V6-V9, V11, V16-V19, V22, V23, V36, V39, V60, V61, V70, V73, V75, V76                             | CI        | 1      | 3            | 3            |

|     |                 |      |                                                                |                                                                                                                  |    |   |   |   |
|-----|-----------------|------|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|----|---|---|---|
| D8  | AS51<br>(lanj.) | AN28 | A4, A15, A37, P24                                              | V5, V11, V63, V120                                                                                               | A  | 3 | 2 | 6 |
| D9  |                 | AN40 | A4, A7, A10, A15,<br>A24, A26, A28,<br>A33, A42, A57           | V1, V2, V10, V13, V15, V22, V24-<br>V28, V31, V32, V36, V38, V70, V71,<br>V73, V77, V78, V82, V95, V101,<br>V102 | IA | 3 | 1 | 3 |
| D10 |                 | AN46 | A11, A29                                                       | V1, V8, V9, V12, V16, V22, V23,<br>V32, V39, V60, V61, V73, V77, V78,<br>V80, V94, V101, V102, V110, V119        | C  | 3 | 3 | 9 |
| D11 | AS52            | AN18 | A2, A5-A9, A13,<br>A14, A35, A43-<br>A49, A56, A59, T5,<br>T30 | V4, V11, V19, V37, V83, V85-V88,<br>V92, V94                                                                     | I  | 2 | 2 | 4 |
| D12 |                 | AN19 | A7, A8, A12-A14,<br>A17, A18, A22,<br>A35, A45                 | V1, V6-V9, V11, V16, V17, V19,<br>V22, V23, V36, V39, V60, V61, V70,<br>V73, V75, V76                            | CI | 1 | 2 | 2 |
| D13 |                 | AN28 | A4, A15, A37, P24                                              | V5, V11, V63, V120                                                                                               | A  | 3 | 2 | 6 |
| D14 |                 | AN40 | A4, A7, A10, A15,<br>A24, A26, A28,<br>A33, A42, A57           | V1, V2, V10, V13, V15, V22, V24-<br>V28, V31, V32, V36, V38, V70, V71,<br>V73, V77, V78, V82, V95, V101,<br>V102 | IA | 3 | 1 | 3 |
| D15 |                 | AN46 | A11, A29                                                       | V1, V8, V9, V12, V16, V22, V23,<br>V32, V39, V60, V61, V73, V77, V78,<br>V80, V94, V101, V102, V110, V119        | C  | 3 | 2 | 6 |

Tabel I.8 Lembar Kerja Penilaian Resiko Kasubdit Infrastruktur

| Nomor Resiko | Aset | Ancaman | Kontrol Keamanan                                       | Kerentanan                                                     | Aspek CIA | Dampak   | Probabilitas | Level Resiko |
|--------------|------|---------|--------------------------------------------------------|----------------------------------------------------------------|-----------|----------|--------------|--------------|
| IK1          | AS1  | AN21    | A1, A2, A5, A7, A8, A13, A14                           | V1, V11, V66, V119                                             | I         | 2        | 1            | 2            |
| IK2          |      | AN24    | A1, A16, T14                                           | V1, V14, V22, V66, V119                                        | IA        | 1        | 1            | 1            |
| IK3          |      | AN25    | A1, A21, A34, A42                                      | V1, V6, V7, V9, V20-V23, V38, V57, V119                        | C         | 1        | 1            | 1            |
| IK4          |      | AN34    | A1, A4, A7, A10, A15, A16, P1, P2, P5, P8-P10, T1, T14 | V1, V5-V7, V20-V28, V31-V33, V35, V38, V41-V45, V58, V66, V119 | CA        | 2        | 1            | 2            |
| IK5          | AS2  | AN21    | A1, A2, A5, A7, A8, A13, A14                           | V1, V11, V66, V119                                             | I         | 2        | 1            | 2            |
| IK6          |      | AN24    | A1, T14                                                | V1, V14, V22, V66, V119                                        | IA        | 2        | 1            | 2            |
| IK7          |      | AN25    | A1, A21, A34, A42                                      | V1, V6, V7, V9, V20-V23, V38, V57, V119                        | C         | 2        | 1            | 2            |
| IK8          |      | AN34    | A1, A4, A7, A10, A15, P1, P2, P5, P8, P9, T1, T14      | V1, V5-V7, V20-V28, V31-V33, V35, V38, V41-V45, V58, V66, V119 | CA        | 2        | 1            | 2            |
| IK9          | AS3  | AN24    | A1, T13, T15                                           | V1, V14, V22, V66-V72, V119                                    | IA        | <b>3</b> | <b>2</b>     | <b>6</b>     |
| IK10         |      | AN26    | A1, T15, T16                                           | V71, V72                                                       | I         | 2        | 1            | 2            |

|      |                |      |                                                                               |                                                                                             |     |   |   |   |
|------|----------------|------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|-----|---|---|---|
| IK11 | AS3<br>(lanj.) | AN29 | A1, A25, A26,<br>A28, T1, T4, T7,<br>T9, T15, T17, T19                        | V1, V6-V9, V24-V26, V29, V31,<br>V32, V58-V60, V71, V74, V91, V95,<br>V101-V103, V111, V113 | CIA | 2 | 1 | 2 |
| IK12 |                | AN39 | A1, A38, T1, T4,<br>T13, T15                                                  | V70, V71                                                                                    | IA  | 3 | 1 | 3 |
| IK13 | AS4            | AN24 | A1, T14                                                                       | V14, V119                                                                                   | IA  | 1 | 1 | 1 |
| IK14 |                | AN25 | A1, A34, A42                                                                  | V1, V6, V7, V9, V20-V23, V38,<br>V57, V119                                                  | C   | 1 | 1 | 1 |
| IK15 |                | AN34 | A1, A4, A7, A10,<br>A15, P1, P2, P5,<br>P8, P9, T1                            | V1, V5-V7, V20-V28, V31-V33,<br>V35, V38, V39, V41-V45, V58,<br>V119                        | CA  | 1 | 1 | 1 |
| IK16 | AS5            | AN24 | A1, T14                                                                       | V1, V14, V66, V119                                                                          | IA  | 1 | 1 | 1 |
| IK17 |                | AN25 | A1, A34, A42                                                                  | V1, V6, V7, V9, V20-V23, V38,<br>V57, V119                                                  | C   | 1 | 1 | 1 |
| IK18 |                | AN34 | A1, A4, A7, A10,<br>A15, P1, P2, P5,<br>P8, P9, T1                            | V1, V5-V7, V20-V28, V31-V33,<br>V35, V38, V39, V41-V45, V58, V66,<br>V119                   | CA  | 1 | 1 | 1 |
| IK19 | AS14           | AN10 | A1-A5, A18, A32,<br>A36, A40, A41,<br>A53, P16, P17,<br>T10, T23, T32-<br>T35 | V1, V36, V53, V54, V74, V91, V99,<br>V105, V106, V109, V112-V116                            | A   | 3 | 3 | 9 |
| IK20 |                | AN14 | A1, A3, A4, A38,<br>T13, T32-T35                                              | V1, V53, V54, V63, V66-V68, V114-<br>V116, V119                                             | A   | 3 | 3 | 9 |

|      |                 |      |                                                                                                     |                                                                                                |     |   |   |   |
|------|-----------------|------|-----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----|---|---|---|
| IK21 | AS14<br>(lanj.) | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13                                                       | V4, V11, V19, V61                                                                              | CIA | 2 | 2 | 4 |
| IK22 |                 | AN23 | A1, A5, A40, A41,<br>A47-A49, A54,<br>T33                                                           | V1, V36, V62, V73-V76, V83-V88,<br>V91, V92, V101-V103, V113, V119                             | IA  | 2 | 3 | 6 |
| IK23 |                 | AN27 | A1, A3, A4, A37,<br>A41, T10, T21,<br>T23, T32-T35                                                  | V63, V101, V116, V117                                                                          | A   | 3 | 2 | 6 |
| IK24 |                 | AN29 | A1, A5, A25, A26,<br>A28, A40, A60,<br>P7, T1, T4, T6, T7,<br>T9                                    | V1, V6-V9, V24-V29, V31-V33,<br>V35, V58-V60, V71, V74, V91, V95,<br>V101-V103, V111, V113     | CIA | 2 | 2 | 4 |
| IK25 |                 | AN31 | A1, A3, A5, A18,<br>A30, A40, A41,<br>A51, A52, A54,<br>T10, T15, T17,<br>T19, T21-T24,<br>T32, T33 | V1, V4, V62, V63, V74, V89, V92,<br>V101-V103, V108, V110, V111,<br>V113, V117                 | A   | 3 | 2 | 6 |
| IK26 |                 | AN36 | A1, A4, A7, A10,<br>A15, A16, P1, P2,<br>P4-P6, P8, P9                                              | V1, V5, V24, V26, V32, V33, V41-<br>V46                                                        | CA  | 3 | 1 | 3 |
| IK27 |                 | AN41 | A1, A5, A11, A31-<br>A40, T12, T18,<br>T19, T24                                                     | V1, V8, V9, V12, V16, V23,<br>V55, V62, V65-V68, V73-V75, V91,<br>V101, V102, V111, V113, V119 | CIA | 1 | 2 | 2 |

|      |                 |      |                                                                               |                                                                                            |     |   |   |   |
|------|-----------------|------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-----|---|---|---|
| IK28 | AS14<br>(lanj.) | AN43 | A1, A5, A38, A40,<br>A41, T13, T15                                            | V1, V36, V62, V66, V71, V74, V91,<br>V111, V113                                            | I   | 1 | 2 | 2 |
| IK29 | AS15            | AN6  | A1, A38, T34                                                                  | V1, V66-V69, V96-V98                                                                       | A   | 2 | 2 | 4 |
| IK30 |                 | AN10 | A1-A5, A18, A32,<br>A36, A40, A41,<br>A53, P16, P17,<br>T10, T23, T34,<br>T35 | V1, V36, V53, V54, V74, V91, V99,<br>V105, V106, V109, V112-V116                           | A   | 2 | 2 | 4 |
| IK31 |                 | AN14 | A1, A3, A4, A38,<br>T13, T32-T35                                              | V1, V53, V54, V63, V66-V68, V114-<br>V116, V119                                            | A   | 2 | 2 | 4 |
| IK32 |                 | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13                                 | V4, V11, V19, V61                                                                          | CIA | 2 | 2 | 4 |
| IK33 |                 | AN23 | A1, A5, A40, A41,<br>A47-A49, T33                                             | V1, V36, V62, V73-V76, V83-V88,<br>V91, V92, V101-V103, V113, V119                         | IA  | 2 | 2 | 4 |
| IK34 |                 | AN27 | A1, A3, A4, A37,<br>A41, T10, T23,<br>T34, T35                                | V63, V101, V116                                                                            | A   | 2 | 1 | 2 |
| IK35 |                 | AN29 | A1, A5, A25, A26,<br>A28, A40, P7, T1,<br>T4, T6, T7, T9                      | V1, V6-V9, V24-V29, V31-V33,<br>V35, V58-V60, V71, V74, V91, V95,<br>V101-V103, V111, V113 | CIA | 2 | 2 | 4 |
| IK36 |                 | AN36 | A1, A4, A7, A10,<br>A15, A16, P1, P2,<br>P4-P6, P8, P9                        | V1, V5, V24, V26, V32, V33, V41-<br>V46                                                    | CA  | 3 | 1 | 3 |

|      |                 |      |                                                         |                                                                                            |     |   |   |   |
|------|-----------------|------|---------------------------------------------------------|--------------------------------------------------------------------------------------------|-----|---|---|---|
| IK37 | AS15<br>(lanj.) | AN41 | A1, A5, A11, A31-A40, T12, T18, T19, T24                | V1, V8, V9, V12, V16, V23, V55, V62, V65-V68, V73-V75, V91, V101, V102, V111, V113, V119   | CIA | 1 | 2 | 2 |
| IK38 |                 | AN43 | A1, A5, A38, A40, A41, T13, T15                         | V1, V36, V62, V66, V71, V74, V91, V111, V113                                               | I   | 1 | 2 | 2 |
| IK39 | AS16            | AN9  | A1-A5, A18, A32, A36, A40, A41, A53, A54, P16, P17, T10 | V1, V54, V74, V91, V99, V105, V106, V109, V112-V115                                        | A   | 3 | 3 | 9 |
| IK40 |                 | AN20 | A1, A5, A7, A8, A13, A14, A36, A38, T13                 | V4, V11, V19, V61                                                                          | CIA | 2 | 2 | 4 |
| IK41 |                 | AN27 | A1, A3, A4, A37, A41, T10                               | V63, V101, V116, V117                                                                      | A   | 2 | 3 | 6 |
| IK42 |                 | AN29 | A1, A5, A25, A26, A28, A36, A40, P7, T1, T9             | V1, V6-V9, V24-V26, V29, V31, V32, V55, V58-V60, V71, V74, V91, V95, V101-V103, V111, V113 | CIA | 1 | 1 | 1 |
| IK43 |                 | AN35 | A1, A4, A7, A10, A15, A16, P1, P2, P4-P6, P8, P9        | V1, V5, V24, V26, V32, V33, V41-V46, V56                                                   | A   | 3 | 1 | 3 |
| IK44 |                 | AN43 | A1, A5, A38, A40, A41, T13                              | V1, V62, V66, V71, V74, V91, V111, V113                                                    | I   | 2 | 1 | 2 |

|      |      |      |                                                              |                                                                                            |     |   |   |   |
|------|------|------|--------------------------------------------------------------|--------------------------------------------------------------------------------------------|-----|---|---|---|
| IK45 | AS17 | AN9  | A1-A5, A18, A32, A36, A40, A41, A53, A54, P16, P17, T10      | V1, V54, V74, V91, V99, V105, V106, V109, V112-V115                                        | A   | 3 | 3 | 9 |
| IK46 |      | AN20 | A1, A5, A7, A8, A13, A14, A36, A38, T13                      | V4, V11, V19, V61                                                                          | CIA | 3 | 3 | 9 |
| IK47 |      | AN27 | A1, A3, A4, A37, A41, T10                                    | V63, V101, V116, V117                                                                      | A   | 2 | 2 | 4 |
| IK48 |      | AN29 | A1, A5, A25, A26, A28, A36, A40, P7, T1, T9                  | V1, V6-V9, V24-V26, V29, V31, V32, V55, V58-V60, V71, V74, V91, V95, V101-V103, V111, V113 | CIA | 1 | 1 | 1 |
| IK49 |      | AN35 | A1, A4, A7, A10, A15, A16, P1, P2, P4-P6, P8, P9             | V1, V5, V24, V26, V32, V33, V41-V46, V56                                                   | A   | 3 | 1 | 3 |
| IK50 |      | AN43 | A1, A5, A38, A40, A41,, T13                                  | V1, V62, V66, V71, V74, V91, V111, V113                                                    | I   | 1 | 1 | 1 |
| IK51 | AS18 | AN9  | A1-A5, A18, A32, A36, A40, A41, A53, A54, P16, P17, T10, T22 | V1, V54, V74, V91, V99, V105, V106, V109, V112-V115                                        | A   | 3 | 3 | 9 |
| IK52 |      | AN20 | A1, A5, A7, A8, A13, A14, A36, A38, T13                      | V4, V11, V19, V61                                                                          | CIA | 3 | 3 | 9 |



|      |                 |      |                                                                               |                                                                                                  |     |   |   |   |
|------|-----------------|------|-------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----|---|---|---|
| IK53 | AS18<br>(lanj.) | AN27 | A1, A3, A4, A37,<br>A41, T10, T22                                             | V63, V101, V116, V117                                                                            | A   | 2 | 3 | 6 |
| IK54 |                 | AN29 | A1, A5, A25, A26,<br>A28, A36, A40,<br>P7, T1, T9                             | V1, V6-V9, V24-V26, V29, V31,<br>V32, V55, V58-V60, V71, V74, V91,<br>V95, V101-V103, V111, V113 | CIA | 1 | 1 | 1 |
| IK55 |                 | AN35 | A1, A4, A7, A10,<br>A15, A16, P1, P2,<br>P4-P6, P8, P9                        | V1, V5, V24, V26, V32, V33, V41-<br>V46, V56                                                     | A   | 3 | 1 | 3 |
| IK56 |                 | AN43 | A1, A5, A38, A40,<br>A41, T13                                                 | V1, V62, V66, V71, V74, V91, V111,<br>V113                                                       | I   | 1 | 1 | 1 |
| IK57 | AS19            | AN9  | A1-A5, A18, A32,<br>A36, A40, A41,<br>A53, A54, P16,<br>P17, T10, T22,<br>T35 | V54, V91, V105, V106, V109, V112-<br>V115                                                        | A   | 3 | 3 | 9 |
| IK58 |                 | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13                                 | V4, V11, V19, V61                                                                                | CIA | 3 | 3 | 9 |
| IK59 |                 | AN27 | A1, A3, A4, A37,<br>A41, T10, T22                                             | V63, V101, V116, V117                                                                            | A   | 2 | 2 | 4 |
| IK60 |                 | AN29 | A1, A5, A25, A26,<br>A28, A36, A40,<br>P7, T1, T9                             | V1, V6-V9, V24-V26, V29, V31,<br>V32, V55, V58-V60, V71, V74, V91,<br>V95, V101-V103, V111, V113 | CIA | 1 | 1 | 1 |

|      |                 |      |                                                                                   |                                                                                                  |     |   |   |   |
|------|-----------------|------|-----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----|---|---|---|
| IK61 | AS19<br>(lanj.) | AN35 | A1, A4, A7, A10,<br>A15, A16, P1, P2,<br>P4-P6, P8, P9                            | V1, V5, V24, V26, V32, V33, V41-<br>V46, V56                                                     | A   | 3 | 1 | 3 |
| IK62 |                 | AN43 | A1, A5, A38, A40,<br>A41, T13                                                     | V1, V62, V66, V71, V74, V91, V111,<br>V113                                                       | I   | 1 | 1 | 1 |
| IK63 | AS20            | AN9  | A1-A5, A18, A32,<br>A36, A40, A41,<br>A53, A54, A1,<br>P16, P17, T10,<br>T22, T35 | V1, V54, V74, V91, V105, V106,<br>V109, V112-V115                                                | A   | 2 | 3 | 6 |
| IK64 |                 | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13                                     | V4, V11, V19, V61                                                                                | CIA | 2 | 3 | 6 |
| IK65 |                 | AN27 | A1, A3, A4, A37,<br>A41, T10, T22                                                 | V63, V101, V116, V117                                                                            | A   | 1 | 2 | 2 |
| IK66 |                 | AN29 | A1, A5, A25, A26,<br>A28, A36, A40,<br>P7, T1, T9                                 | V1, V6-V9, V24-V26, V29, V31,<br>V32, V55, V58-V60, V71, V74, V91,<br>V95, V101-V103, V111, V113 | CIA | 1 | 1 | 1 |
| IK67 |                 | AN35 | A1, A4, A7, A10,<br>A15, A16, P1, P2,<br>P4-P6, P8, P9                            | V1, V5, V24, V26, V32, V33, V41-<br>V46, V56                                                     | A   | 2 | 1 | 2 |
| IK68 |                 | AN43 | A1, A5, A38, A40,<br>A41, T13                                                     | V1, V62, V66, V71, V74, V91, V111,<br>V113                                                       | I   | 1 | 1 | 1 |
| IK69 | AS21            | AN4  | A1, A4                                                                            | V49, V116, V107                                                                                  | A   | 2 | 1 | 2 |

|      |                 |      |                                                                  |                                                                                                  |     |   |   |   |
|------|-----------------|------|------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----|---|---|---|
| IK70 | AS21<br>(lanj.) | AN9  | A1-A5, A18, A32,<br>A36, A40, A53,<br>A54, P16, P17,<br>T10, T35 | V1, V50, V54, V74, V91, V105,<br>V106, V109, V112-V115                                           | A   | 1 | 2 | 2 |
| IK71 |                 | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13                    | V4, V11, V19, V61                                                                                | CIA | 1 | 2 | 2 |
| IK72 |                 | AN27 | A1, A3, A4, A37                                                  | V63, V101, V116                                                                                  | A   | 1 | 1 | 1 |
| IK73 |                 | AN29 | A1, A5, A25, A26,<br>A28, A36, A40,<br>P7, T1, T9                | V1, V6-V9, V24-V26, V29, V31,<br>V32, V55, V58-V60, V71, V74, V91,<br>V95, V101-V103, V111, V113 | CIA | 1 | 1 | 1 |
| IK74 |                 | AN35 | A1, A4, A7, A10,<br>A15, A16, P1, P2,<br>P5, P8, P9              | V1, V5, V24, V26, V32, V33, V41-<br>V45, V56                                                     | A   | 1 | 1 | 1 |
| IK75 |                 | AN43 | A1, A5, A36, A38,<br>A40, T13                                    | V1, V62, V66, V71, V74, V91, V111,<br>V113                                                       | I   | 1 | 1 | 1 |
| IK76 | AS22            | AN9  | A1-A5, A18, A32,<br>A36, A40, A41,<br>A53, P16, P17,<br>T10      | V1, V54, V74, V91, V99, V105,<br>V106, V109, V112-V115                                           | A   | 3 | 3 | 9 |
| IK77 |                 | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13                    | V4, V11, V19, V61                                                                                | CIA | 3 | 3 | 9 |
| IK78 |                 | AN27 | A1, A3, A4, A37,<br>A41, T10                                     | V63, V101, V116, V117                                                                            | A   | 2 | 3 | 6 |

|      |                 |      |                                                             |                                                                                                  |     |   |   |   |
|------|-----------------|------|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-----|---|---|---|
| IK79 | AS22<br>(lanj.) | AN29 | A1, A5, A25, A26,<br>A28, A36, A40,<br>P7, T1, T9           | V1, V6-V9, V24-V26, V29, V31,<br>V32, V55, V58-V60, V71, V74, V91,<br>V95, V101-V103, V111, V113 | CIA | 1 | 1 | 1 |
| IK80 |                 | AN35 | A1, A4, A7, A10,<br>A15, A16, P1, P2,<br>P4-P6, P8, P9      | V1, V5, V24, V26, V32, V33, V41-<br>V46, V56                                                     | A   | 3 | 1 | 3 |
| IK81 |                 | AN43 | A1, A5, A38, A40,<br>A41, T13                               | V1, V62, V66, V71, V74, V91, V111,<br>V113                                                       | I   | 1 | 1 | 1 |
| IK82 | AS23            | AN9  | A1-A5, A18, A32,<br>A36, A40, A41,<br>A53, P16, P17,<br>T10 | V1, V54, V74, V91, V99, V105,<br>V106, V109, V112-V115                                           | A   | 3 | 1 | 3 |
| IK83 |                 | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13               | V4, V11, V19, V61                                                                                | CIA | 3 | 1 | 3 |
| IK84 |                 | AN27 | A1, A3, A4, A37,<br>A41, T10                                | V63, V101, V116, V117                                                                            | A   | 2 | 1 | 2 |
| IK85 |                 | AN29 | A1, A5, A25, A26,<br>A28, A36, A40,<br>P7, T1, T9           | V1, V6-V9, V24-V26, V29, V31,<br>V32, V55, V58-V60, V71, V74, V91,<br>V95, V101-V103, V111, V113 | CIA | 1 | 1 | 1 |
| IK86 |                 | AN35 | A1, A4, A7, A10,<br>A15, A16, P1, P2,<br>P4-P6, P8, P9      | V1, V5, V24, V26, V32, V33, V41-<br>V46, V56                                                     | A   | 3 | 1 | 3 |
| IK87 |                 | AN43 | A1, A5, A38, A40,<br>A41, T13                               | V1, V62, V66, V71, V74, V91, V111,<br>V113                                                       | I   | 1 | 1 | 1 |

|      |                 |      |                                               |                                                                                                |     |   |   |   |
|------|-----------------|------|-----------------------------------------------|------------------------------------------------------------------------------------------------|-----|---|---|---|
| IK88 | AS24            | AN10 | A1-A5, P16, P17, T35                          | V1, V7, V36, V50, V53, V54, V74, V91, V99, V105, V106, V109, V113, V114, V116                  | A   | 1 | 2 | 2 |
| IK89 |                 | AN23 | A1, A3, A5, A40                               | V1, V16, V36, V62, V73-V75, V84, V91, V92, V101-V103, V113, V119                               | IA  | 1 | 2 | 2 |
| IK90 |                 | AN29 | A1, A5, A40, T1, T26                          | V1, V7-V9, V12, V24-V28, V31-V33, V35, V58-V60, V70, V71, V74, V91, V95, V101-V103, V111, V113 | CIA | 1 | 2 | 2 |
| IK91 | AS24<br>(lanj.) | AN36 | A1, A4, A7, A10, A15, A16, P1, P2, P5, P8, P9 | V1, V5, V24, V26, V32, V33, V41-V45, V56                                                       | CA  | 2 | 1 | 2 |
| IK92 |                 | AN38 | A1, T36                                       | V1, V9, V75, V100                                                                              | CIA | 1 | 2 | 2 |
| IK93 |                 | AN41 | A1, A5, A11, A40, T11, T18, T24, T26          | V1, V7-V9, V12, V16, V23, V55, V62, V65, V66, V73-V75, V91, V101, V102, V111, V113, V119       | CIA | 1 | 2 | 2 |
| IK94 |                 | AN43 | A1, A4                                        | V1, V16, V36, V62, V66, V70, V71, V73-V75, V91, V111, V113                                     | I   | 1 | 2 | 2 |
| IK95 | AS27            | AN10 | A1-A5, P16, P17, T35                          | V1, V6, V36, V53, V54, V74, V91, V99, V105, V106, V109, V113, V114, V116                       | A   | 1 | 2 | 2 |
| IK96 |                 | AN23 | A1, A3, A5, A40                               | V1, V16, V36, V62, V73-V75, V84, V91, V92, V101-V103, V113, V119                               | IA  | 1 | 2 | 2 |

|       |                 |      |                                                          |                                                                                                              |     |   |   |   |
|-------|-----------------|------|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|-----|---|---|---|
| IK97  | AS27<br>(lanj.) | AN29 | A1, A5, A40, T1,<br>T26                                  | V1, V6, V8, V9, V12, V24-V28,<br>V31-V33, V35, V58-V60, V70, V71,<br>V74, V91, V95, V101-V103, V111,<br>V113 | CIA | 1 | 1 | 1 |
| IK98  |                 | AN36 | A1, A4, A7, A10,<br>A15, A16, A19,<br>P1, P2, P5, P8, P9 | V1, V5, V18, V24, V26, V32, V33,<br>V41-V45, V56                                                             | CA  | 2 | 1 | 2 |
| IK99  |                 | AN38 | A1, T36                                                  | V1, V9, V75, V100                                                                                            | CIA | 1 | 2 | 2 |
| IK100 |                 | AN41 | A1, A5, A11, A40,<br>T11, T18, T24,<br>T26               | V1, V6, V8, V9, V12, V16, V23,<br>V55, V62, V65, V66, V73-V75, V91,<br>V101, V102, V111, V113, V119          | CIA | 1 | 2 | 2 |
| IK101 |                 | AN43 | A1, A4                                                   | V1, V16, V36, V62, V66, V70, V71,<br>V73-V75, V91, V111, V113                                                | I   | 1 | 2 | 2 |
| IK102 | AS30            | AN11 | A1, A5, A36, A38-<br>A41, A47, T33                       | V1, V62, V73-V76, V83-V88, V91,<br>V92, V101-V103, V113, V119                                                | A   | 2 | 2 | 4 |
| IK103 |                 | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13            | V4, V11, V19, V61                                                                                            | CIA | 2 | 1 | 2 |
| IK104 |                 | AN29 | A1, A5, A25, A26,<br>A28, A40, P7, T1,<br>T7, T9         | V1, V6-V9, V24-V26, V29, V31,<br>V32, V58-V60, V74, V91, V95,<br>V101-V103, V111, V113                       | CIA | 2 | 1 | 2 |
| IK105 |                 | AN43 | A1, A5, A38, A40,<br>A41, T13                            | V1, V62, V66, V71, V74, V91, V111,<br>V113                                                                   | I   | 2 | 1 | 2 |
| IK106 | AS31            | AN11 | A1, A5, A36, A39-<br>A41, A47, T33                       | V1, V62, V73-V76, V83-V88, V91,<br>V92, V101-V103, V113, V119                                                | A   | 2 | 2 | 4 |

|       |                 |      |                                                            |                                                                                        |     |   |   |   |
|-------|-----------------|------|------------------------------------------------------------|----------------------------------------------------------------------------------------|-----|---|---|---|
| IK107 | AS31<br>(lanj.) | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13              | V4, V11, V19, V61                                                                      | CIA | 2 | 1 | 2 |
| IK108 |                 | AN29 | A1, A5, A25, A26,<br>A28, A40, P7, T1,<br>T7, T9           | V1, V6-V9, V24-V26, V29, V31,<br>V32, V58-V60, V74, V91, V95,<br>V101-V103, V111, V113 | CIA | 2 | 1 | 2 |
| IK109 |                 | AN43 | A1, A5, A40, A41,<br>T13                                   | V1, V62, V66, V71, V74, V91, V111,<br>V113                                             | I   | 2 | 1 | 2 |
| IK110 | AS32            | AN11 | A1, A5, A36, A39-<br>A41, A47, T33                         | V1, V62, V73-V76, V83-V88, V91,<br>V92, V101-V103, V113, V119                          | A   | 2 | 1 | 2 |
| IK111 |                 | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13              | V4, V11, V19, V61                                                                      | CIA | 2 | 1 | 2 |
| IK112 |                 | AN29 | A1, A5, A25, A26,<br>A28, A40, P7, T1,<br>T7, T9, T15, T26 | V1, V6-V9, V24-V26, V31-V33,<br>V35, V58-V60, V74, V91, V95,<br>V101-V103, V111, V113  | CIA | 2 | 1 | 2 |
| IK113 |                 | AN43 | A1, A5, A40, A41,<br>T13                                   | V1, V62, V66, V71, V74, V91, V111,<br>V113                                             | I   | 2 | 1 | 2 |
| IK114 | AS33            | AN11 | A1, A5, A36, A39-<br>A41, A47, T33                         | V1, V62, V73-V76, V83-V88, V91,<br>V92, V101-V103, V113, V119                          | A   | 1 | 2 | 2 |
| IK115 |                 | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13              | V4, V11, V19, V61                                                                      | CIA | 1 | 1 | 1 |

|       |                 |      |                                                       |                                                                                        |     |          |          |          |
|-------|-----------------|------|-------------------------------------------------------|----------------------------------------------------------------------------------------|-----|----------|----------|----------|
| IK116 | AS33<br>(lanj.) | AN29 | A1, A5, A25, A26,<br>A28, A40, P7, T1,<br>T7, T9, T15 | V1, V6-V9, V24-V26, V29, V31,<br>V32, V58-V60, V74, V91, V95,<br>V101-V103, V111, V113 | CIA | 1        | 1        | 1        |
| IK117 |                 | AN43 | A1, A5, A40, A41,<br>T13                              | V1, V62, V66, V71, V74, V91, V111,<br>V113                                             | I   | 1        | 1        | 1        |
| IK118 | AS34            | AN11 | A1, A5, A36, A38-<br>A41, A47, T33                    | V1, V62, V73-V76, V83-V88, V91,<br>V92, V101-V103, V113, V119                          | A   | 1        | 2        | 2        |
| IK119 |                 | AN20 | A1, A5, A7, A8,<br>A13, A14, A36,<br>A38, T13         | V4, V11, V19, V61                                                                      | CIA | 2        | 1        | 2        |
| IK120 |                 | AN29 | A1, A5, A25, A26,<br>A28, A40, P7, T1,<br>T7, T9      | V1, V6-V9, V24-V26, V29, V31,<br>V32, V58-V60, V74, V91, V95,<br>V101-V103, V111, V113 | CIA | 1        | 1        | 1        |
| IK121 |                 | AN43 | A1, A5, A38, A40,<br>A41, T13                         | V1, V62, V66, V71, V74, V91, V111,<br>V113                                             | I   | 1        | 1        | 1        |
| IK122 | AS38            | AN8  | A1, A3, A51, A52,<br>A54, T10, T15,<br>T24, T25, T27  | V89, V90, V108-V110                                                                    | A   | <b>2</b> | <b>2</b> | <b>4</b> |
| IK123 |                 | AN13 | A1, A3, A5, A54,<br>T10, T20, T21                     | V89, V90, V108, V110, V117                                                             | A   | 1        | 2        | 2        |
| IK124 | AS39            | AN29 | A1, A5, A23-A27,<br>T2, T15, T17, T20,<br>T21, T26    | V111, V119                                                                             | CIA | 1        | 2        | 2        |
| IK125 |                 | AN30 | A1, A5, T15, T18.<br>T19, T24                         | V1, V62, V65, V111                                                                     | CIA | <b>3</b> | <b>2</b> | <b>6</b> |



|       |                 |      |                                                                  |                           |     |          |          |          |
|-------|-----------------|------|------------------------------------------------------------------|---------------------------|-----|----------|----------|----------|
| IK126 | AS39<br>(lanj.) | AN44 | A1, A5, T6, T7                                                   | V111, V117                | C   | 1        | 2        | 2        |
| IK127 | AS40            | AN6  | A1, A3, A51, A52                                                 | V89, V90, V96-V98, V110   | A   | 1        | 1        | 1        |
| IK128 |                 | AN32 | A1, A3, A50                                                      | V89, V90, V96, V109, V110 | CI  | 1        | 1        | 1        |
| IK129 | AS41            | AN1  | A1, A3, A4, A18,<br>A30-A32, P3, P8,<br>P9, P11-P16, P20,<br>T32 | V46-V48, V56, V106, V116  | A   | 3        | 1        | 3        |
| IK130 |                 | AN15 | A1, P17                                                          | V116                      | A   | 2        | 1        | 2        |
| IK131 |                 | AN29 | A1, P1, P2, P4, P5,<br>P7-P9                                     | V1, V41-V46               | CIA | 1        | 1        | 1        |
| IK132 | AS42            | AN12 | A1, A3, A5, A30,<br>A41, A54, P20-<br>P23, T27                   | V52, V118, V119           | A   | <b>3</b> | <b>2</b> | <b>6</b> |
| IK133 | AS43            | AN5  | A1, A4, A5, A30-<br>A32, P15, P16                                | V106                      | A   | 3        | 1        | 3        |
| IK134 |                 | AN12 | A1, A4, A5, A30,<br>P20-P23                                      | V118, V119                | A   | <b>3</b> | <b>2</b> | <b>6</b> |
| IK135 | AS44            | AN3  | A1, P21                                                          | V107                      | A   | 2        | 1        | 2        |
| IK136 |                 | AN12 | A1, A3, A5, A18,<br>A30, A31, A41,<br>A54, P20-P23,<br>T27       | V118, V119                | A   | <b>2</b> | <b>2</b> | <b>4</b> |
| IK137 | AS45            | AN10 | A1-A5, A32                                                       | V99, V112, V114-V116      | A   | 3        | 1        | 3        |

|       |                 |      |                                                                       |                                         |   |   |   |   |
|-------|-----------------|------|-----------------------------------------------------------------------|-----------------------------------------|---|---|---|---|
| IK138 | AS45<br>(lanj.) | AN37 | A1, A4, A7, A10,<br>A15, A16, A25,<br>A26, A28, P1, P9                | V5, V24, V26, V32, V33, V41             | A | 3 | 1 | 3 |
| IK139 | AS46            | AN10 | A1-A5, A32                                                            | V99, V112, V114-V116                    | A | 3 | 1 | 3 |
| IK140 |                 | AN37 | A1, A4, A7, A10,<br>A15, A16, A25,<br>A26, A28, P1, P9                | V5, V24, V26, V32, V33, V41             | A | 3 | 1 | 3 |
| IK141 | AS47            | AN2  | A1, A32, P15, P16                                                     | V106                                    | A | 3 | 1 | 3 |
| IK142 |                 | AN7  | A1, A3, A4, P18-<br>P20                                               | V50, V105                               | A | 1 | 3 | 3 |
| IK143 | AS48            | AN10 | A1-A5, A32, P16                                                       | V112, V114-V116                         | A | 1 | 2 | 2 |
| IK144 |                 | AN37 | A1, A4, A7, A10,<br>A15, A16, A25,<br>A26, A28, P1, P2,<br>P5, P8, P9 | V1, V5, V24, V26, V32, V33, V41-<br>V46 | A | 3 | 1 | 3 |

Tabel I.9 Lembar Kerja Penilaian Resiko Kasubdit Pelayanan

| Nomor Resiko | Aset | Ancaman | Kontrol Keamanan                                                  | Kerentanan                                                                            | Aspek CIA | Dampak | Probabilitas | Level Resiko |
|--------------|------|---------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------|-----------|--------|--------------|--------------|
| PT1          | AS6  | AN24    | A1, T13, T32                                                      | V1, V22, V66-V69, V119                                                                | IA        | 2      | 1            | 2            |
| PT2          |      | AN29    | A1, A20, A23-A28,<br>A35, A40, T1, T4,<br>T7-T9, T15, T17,<br>T19 | V1, V24-V26, V28, V30-V35, V58-<br>V60, V71, V74, V91, V95, V101-<br>V103, V111, V113 | CIA       | 2      | 1            | 2            |

|      |                |      |                                                      |                                                                                                      |     |          |          |          |
|------|----------------|------|------------------------------------------------------|------------------------------------------------------------------------------------------------------|-----|----------|----------|----------|
| PT3  | AS6<br>(lanj.) | AN42 | A1, A2, A7, A23-<br>A28, A35, A38                    | V1, V66-V69, V119                                                                                    | I   | 2        | 1        | 2        |
| PT4  | AS7            | AN21 | A1-A3, A5, A7,<br>A8, A13, A14                       | V1, V11, V66, V119                                                                                   | I   | 2        | 1        | 2        |
| PT5  |                | AN24 | A1, T14                                              | V1, V14, V22, V66, V119                                                                              | IA  | 3        | 1        | 3        |
| PT6  |                | AN25 | A1, A21, A34, A42                                    | V1, V6, V7, V9, V20-V23, V38, V57,<br>V119                                                           | C   | 1        | 1        | 1        |
| PT7  |                | AN34 | A1, A4, A7, A10,<br>A15, P1, P5, P8-<br>P10, T1, T14 | V1, V5-V7, V20-V28, V31-V33, V35,<br>V38, V41-V45, V58, V66, V119                                    | CA  | 1        | 1        | 1        |
| PT8  | AS8            | AN21 | A1-A3, A5, A7,<br>A8, A13, A14                       | V1, V11, V66, V119                                                                                   | I   | 2        | 1        | 2        |
| PT9  |                | AN24 | A1, T14                                              | V1, V14, V22, V66, V119                                                                              | IA  | 2        | 1        | 2        |
| PT10 | AS25           | AN10 | A1-A5, P16, P17,<br>T35                              | V1, V7, V36, V50, V53, V54, V74,<br>V91, V99, V105, V106, V109, V113,<br>V114, V116                  | A   | 3        | 1        | 3        |
| PT11 |                | AN23 | A1, A3, A5, A40                                      | V1, V16, V36, V62, V73-V75, V84,<br>V91, V92, V101-V103, V113, V119                                  | IA  | 2        | 1        | 2        |
| PT12 |                | AN29 | A1, A5, A40, P7,<br>T1, T26                          | V1, V7-V9, V12, V24-V28, V31-V33,<br>V35, V58-V60, V70, V71, V74, V91,<br>V95, V101-V103, V111, V113 | CIA | <b>2</b> | <b>2</b> | <b>4</b> |

|      |                 |      |                                                      |                                                                                                            |     |   |   |   |
|------|-----------------|------|------------------------------------------------------|------------------------------------------------------------------------------------------------------------|-----|---|---|---|
| PT13 | AS25<br>(lanj.) | AN36 | A1, A4, A7, A10,<br>A15, A16, P1, P5,<br>P8, P9      | V1, V5, V24, V26, V32, V33, V41-<br>V45, V56                                                               | CA  | 3 | 1 | 3 |
| PT14 |                 | AN38 | A1, T36                                              | V1, V9, V75, V100                                                                                          | CIA | 2 | 1 | 2 |
| PT15 |                 | AN41 | A1, A5, A11, A40,<br>T11, T18, T24, T26              | V1, V7-V9, V12, V16, V23, V55,<br>V62, V65, V66, V73-V75, V91, V101,<br>V102, V111, V113, V119             | CIA | 2 | 2 | 4 |
| PT16 |                 | AN43 | A1, A4                                               | V1, V16, V36, V62, V66, V70, V71,<br>V73-V75, V91, V111, V113                                              | I   | 2 | 1 | 2 |
| PT17 | AS28            | AN10 | A1-A5, P16, P17,<br>T35                              | V1, V6, V36, V53, V54, V74, V91,<br>V99, V105, V106, V109, V113, V114,<br>V116                             | A   | 3 | 1 | 3 |
| PT18 |                 | AN23 | A1, A3, A5, A40                                      | V1, V16, V36, V62, V73-V75, V84,<br>V91, V92, V101-V103, V113, V119                                        | IA  | 2 | 1 | 2 |
| PT19 |                 | AN29 | A1, A5, A40, P7,<br>T1, T26                          | V1, V6, V8, V9, V12, V24-V28, V31-<br>V33, V35, V58-V60, V70, V71, V74,<br>V91, V95, V101-V103, V111, V113 | CIA | 2 | 1 | 2 |
| PT20 |                 | AN36 | A1, A4, A7, A10,<br>A15, A16, A19, P1,<br>P5, P8, P9 | V1, V5, V18, V24, V26, V32, V33,<br>V41-V45, V56                                                           | CA  | 3 | 1 | 3 |
| PT21 |                 | AN38 | A1, T36                                              | V1, V9, V75, V100                                                                                          | CIA | 2 | 1 | 2 |
| PT22 |                 | AN41 | A1, A5, A11, A40,<br>T11, T18, T24, T26              | V1, V6, V8, V9, V12, V16, V23, V55,<br>V62, V65, V66, V73-V75, V91, V101,<br>V102, V111, V113, V119        | CIA | 2 | 2 | 4 |

|      |                 |      |                                                                                             |                                                                                                 |     |   |   |   |
|------|-----------------|------|---------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|-----|---|---|---|
| PT23 | AS28<br>(lanj.) | AN43 | A1, A4                                                                                      | V1, V16, V36, V62, V66, V70, V71,<br>V73-V75, V91, V111, V113                                   | I   | 2 | 1 | 2 |
| PT24 | AS35            | AN11 | A1, A5, A36, A39-<br>A41, A46-A49,<br>A53, T13                                              | V1, V63, V66-V69, V74, V76, V83,<br>V91, V113                                                   | A   | 1 | 2 | 2 |
| PT25 |                 | AN43 | A1, A5, A40, A41,<br>T13                                                                    | V1, V62, V66, V71, V74, V91, V111,<br>V113                                                      | I   | 1 | 1 | 1 |
| PT26 | AS36            | AN11 | A1, A5, A36, A38-<br>A41, A46-A49,<br>T33                                                   | V1, V62, V73-V76, V83-V88, V91,<br>V92, V101-V103, V113, V119                                   | A   | 2 | 1 | 2 |
| PT27 |                 | AN29 | A1, A5, A20, A23-<br>A29, A40, A54, P7,<br>T1, T3, T4, T6, T8,<br>T9, T15, T17, T19,<br>T28 | V1, V6-V9, V24-V26, V28-V35, V40,<br>V58-V60, V71, V74, V80, V91, V95,<br>V101-V103, V111, V113 | CIA | 2 | 2 | 4 |
| PT28 |                 | AN43 | A1, A5, A38, A40,<br>A41, T13                                                               | V1, V62, V66, V71, V74, V91, V111,<br>V113                                                      | I   | 1 | 1 | 1 |
| PT29 |                 | AN45 | A1, A17, T24, T28,<br>T29                                                                   | V79, V81                                                                                        | A   | 3 | 2 | 6 |
| PT30 |                 | AN19 | A12, A17, A22,<br>A23, A45                                                                  | V16, V76                                                                                        | CI  | 1 | 1 | 1 |
| PT32 | AS49            | AN40 | A4, A10, A15,<br>A24, A57                                                                   | V1, V16, V32, V94, V95, V100,<br>V101, V102                                                     | IA  | 1 | 3 | 3 |

|      |                 |      |          |                                                                              |   |   |   |   |
|------|-----------------|------|----------|------------------------------------------------------------------------------|---|---|---|---|
| PT33 | AS49<br>(lanj.) | AN46 | A11, A29 | V1, V12, V16, V30, V31, V34, V35,<br>V77, V79, V94, V95, V101, V102,<br>V119 | C | 3 | 3 | 9 |
|------|-----------------|------|----------|------------------------------------------------------------------------------|---|---|---|---|

Tabel I.10 Lembar Kerja Penilaian Resiko Kasubdit Pengembangan

| Nomor Resiko | Aset | Ancaman | Kontrol Keamanan                                  | Kerentanan                                                     | Aspek CIA | Dampak | Proabilitas | Level Resiko |
|--------------|------|---------|---------------------------------------------------|----------------------------------------------------------------|-----------|--------|-------------|--------------|
| PS1          | AS9  | AN21    | A1, A2, A5, A7, A8, A13, A14                      | V1, V11, V19, V66, V119                                        | I         | 1      | 1           | 1            |
| PS2          |      | AN24    | A1, T14                                           | V1, V14, V22, V66, V119                                        | IA        | 1      | 1           | 1            |
| PS3          |      | AN25    | A1, A21, A34, A42                                 | V1, V6, V7, V9, V20-V23, V38, V57, V119                        | C         | 2      | 1           | 2            |
| PS4          |      | AN34    | A1, A4, A7, A10, A15, P1, P2, P5, P8, P9, T1, T14 | V1, V5-V7, V20-V28, V31-V33, V35, V38, V41-V45, V58, V66, V119 | CA        | 2      | 1           | 2            |
| PS5          | AS10 | AN21    | A1, A2, A5, A7, A8, A13, A14                      | V1, V11, V19, V66, V119                                        | I         | 2      | 2           | 4            |
| PS6          |      | AN24    | A1, T14                                           | V1, V14, V22, V66, V119                                        | IA        | 2      | 1           | 2            |
| PS7          |      | AN25    | A1, A21, A34, A42                                 | V1, V6, V7, V9, V20-V23, V38, V57, V119                        | C         | 1      | 1           | 1            |
| PS8          |      | AN34    | A1, A4, A7, A10, A15, P1, P2, P5, P8-P10, T1, T14 | V1, V5-V7, V20-V28, V31-V33, V35, V38, V41-V45, V58, V66, V119 | CA        | 2      | 1           | 2            |

|      |      |      |                                                           |                                                                |     |   |   |   |
|------|------|------|-----------------------------------------------------------|----------------------------------------------------------------|-----|---|---|---|
| PS9  | AS11 | AN21 | A1, A2, A5, A7, A8, A13, A14                              | V1, V11, V19, V66, V119                                        | I   | 2 | 2 | 4 |
| PS10 |      | AN24 | A1, T14                                                   | V1, V14, V22, V66, V119                                        | IA  | 1 | 1 | 1 |
| PS11 | AS12 | AN21 | A1, A2, A5, A7, A8, A13, A14                              | V1, V11, V19, V66, V119                                        | I   | 2 | 2 | 4 |
| PS12 |      | AN24 | A1, T14                                                   | V1, V14, V22, V66, V119                                        | IA  | 1 | 2 | 2 |
| PS13 |      | AN25 | A1, A21, A34, A42                                         | V1, V6, V7, V9, V20-V23, V38, V57, V119                        | C   | 1 | 1 | 1 |
| PS14 |      | AN34 | A1, A4, A7, A10, A15, P1, P2, P5, P8-P10, T1, T14         | V1, V5-V7, V20-V28, V31-V33, V35, V38, V41-V45, V58, V66, V119 | CA  | 2 | 1 | 2 |
| PS15 | AS13 | AN22 | A1, A2, A5-A8, A13, A14, A43, A44, A46, A48, A49, T5, T30 | V5, V11, V19, V83, V85-V88, V119                               | CIA | 2 | 2 | 4 |
| PS16 |      | AN24 | A1, T5, T14                                               | V1, V5, V14, V22, V37, V64, V66, V104, V119                    | IA  | 1 | 2 | 2 |
| PS17 |      | AN25 | A1, A21, A34, A42                                         | V1, V5-V7, V9, V20-V23, V37, V38, V57, V64, V119               | C   | 1 | 1 | 1 |
| PS18 |      | AN33 | A1, A2, A4, A5, A7, A8, A10, A13-A15, A46, A48, T5, T30   | V5, V11, V19, V37, V64, V87, V88, V119                         | CI  | 3 | 1 | 3 |

|      |                 |      |                                                                |                                                                                                      |     |          |          |          |
|------|-----------------|------|----------------------------------------------------------------|------------------------------------------------------------------------------------------------------|-----|----------|----------|----------|
| PS19 | AS13<br>(lanj.) | AN34 | A1, A4, A7, A10,<br>A15, P1, P2, P5,<br>P8-P10, T1, T5,<br>T14 | V1, V5-V7, V20-V28, V31-V33, V35,<br>V37, V38, V41-V45, V58, V64, V66,<br>V104, V119                 | CA  | 3        | 1        | 3        |
| PS20 | AS26            | AN10 | A1-A5, P16, P17,<br>T35                                        | V1, V7, V36, V50, V53, V54, V74,<br>V91, V99, V105, V106, V109, V113,<br>V114, V116                  | A   | 3        | 1        | 3        |
| PS21 |                 | AN23 | A1, A3, A5, A40                                                | V1, V16, V36, V62, V73-V75, V84,<br>V91, V92, V101-V103, V113, V119                                  | IA  | 2        | 1        | 2        |
| PS22 |                 | AN29 | A1, A5, A40, P7,<br>T1, T26                                    | V1, V7-V9, V12, V24-V28, V31-V33,<br>V35, V58-V60, V70, V71, V74, V91,<br>V95, V101-V103, V111, V113 | CIA | <b>2</b> | <b>2</b> | <b>4</b> |
| PS23 |                 | AN36 | A1, A4, A7, A10,<br>A15, A16, P1, P2,<br>P5, P8, P9            | V1, V5, V24, V26, V32, V33, V41-<br>V45, V56                                                         | CA  | 3        | 1        | 3        |
| PS24 |                 | AN38 | A1, T36                                                        | V1, V9, V75, V100                                                                                    | CIA | 2        | 1        | 2        |
| PS25 |                 | AN41 | A1, A5, A11, A40,<br>T11, T18, T24, T26                        | V1, V7-V9, V12, V16, V23, V55,<br>V62, V65, V66, V73-V75, V91, V101,<br>V102, V111, V113, V119       | CIA | <b>2</b> | <b>2</b> | <b>4</b> |
| PS26 |                 | AN43 | A1, A4                                                         | V1, V16, V36, V62, V66, V70, V71,<br>V73-V75, V91, V111, V113                                        | I   | 2        | 1        | 2        |
| PS27 | AS29            | AN10 | A1-A5, P16, P17,<br>T35                                        | V1, V6, V36, V53, V54, V74, V91,<br>V99, V105, V106, V109, V113, V114,<br>V116                       | A   | 3        | 1        | 3        |



|      |                 |      |                                                    |                                                                                                     |     |   |   |   |
|------|-----------------|------|----------------------------------------------------|-----------------------------------------------------------------------------------------------------|-----|---|---|---|
| PS28 | AS29<br>(lanj.) | AN23 | A1, A3, A5, A40                                    | V1, V16, V36, V62, V73-V75, V84, V91, V92, V101-V103, V113, V119                                    | IA  | 2 | 1 | 2 |
| PS29 |                 | AN29 | A1, A5, A40, P7, T1, T26                           | V1, V6, V8, V9, V12, V24-V28, V31-V33, V35, V58-V60, V70, V71, V74, V91, V95, V101-V103, V111, V113 | CIA | 2 | 1 | 2 |
| PS30 |                 | AN36 | A1, A4, A7, A10, A15, A16, A19, P1, P2, P5, P8, P9 | V1, V5, V18, V24, V26, V32, V33, V41-V45, V56                                                       | CA  | 3 | 1 | 3 |
| PS31 |                 | AN38 | A1, T36                                            | V1, V9, V75, V100                                                                                   | CIA | 2 | 1 | 2 |
| PS32 |                 | AN41 | A1, A5, A11, A40, T11, T18, T24, T26               | V1, V6, V8, V9, V12, V16, V23, V55, V62, V65, V66, V73-V75, V91, V101, V102, V111, V113, V119       | CIA | 2 | 2 | 4 |
| PS33 |                 | AN43 | A1, A4                                             | V1, V16, V36, V62, V66, V70, V71, V73-V75, V91, V111, V113                                          | I   | 2 | 1 | 2 |
| PS34 | AS37            | AN11 | A1, A5, A36, A40, A41, A47, T33                    | V1, V62, V73-V76, V83-V88, V91, V92, V101-V103, V113, V119                                          | A   | 1 | 2 | 1 |
| PS35 |                 | AN20 | A1, A5, A7, A8, A13, A14, A36, A38, T13            | V4, V11, V19, V61                                                                                   | CIA | 2 | 1 | 2 |
| PS36 |                 | AN29 | A1, A5, A25, A26, A28, A40, P7, T1, T7, T9         | V1, V6-V9, V24-V26, V29, V31, V32, V58-V60, V74, V91, V95, V101-V103, V111, V113                    | CIA | 2 | 1 | 2 |
| PS37 |                 | AN43 | A1, A5, A38, A40, A41, T13                         | V1, V62, V66, V71, V74, V91, V111, V113                                                             | I   | 2 | 1 | 2 |

Tabel I.11 Evaluasi Resiko

| Prioritas | Nomor Resiko                 | Resiko                                               | Level Resiko |        | Keputusan      |
|-----------|------------------------------|------------------------------------------------------|--------------|--------|----------------|
| 1         | IK39, IK45, IK51, IK57, IK76 | Kegagalan perangkat jaringan                         | 9            | High   | Tidak diterima |
| 2         | IK46, IK52, IK58, IK77       | Kesalahan konfigurasi                                | 9            | High   | Tidak diterima |
| 3         | D10, PT33                    | Terkena aktifitas <i>social engineering</i>          | 9            | High   | Tidak diterima |
| 4         | IK19                         | Kegagalan perangkat keras                            | 9            | High   | Tidak diterima |
| 5         | IK20                         | Penurunan kondisi media penyimpanan                  | 9            | High   | Tidak diterima |
| 6         | IK23, IK41, IK53, IK78       | Kegagalan akibat penggunaan melebihi batas kapasitas | 6            | Medium | Tidak diterima |
| 7         | D3, D8, D13                  | Absensi karyawan                                     | 6            | Medium | Tidak diterima |
| 8         | D5, D15                      | Terkena aktifitas <i>social engineering</i>          | 6            | Medium | Tidak diterima |
| 9         | IK132, IK134                 | Kerusakan kabel                                      | 6            | Medium | Tidak diterima |
| 10        | IK9                          | Kerusakan/kehilangan data                            | 6            | Medium | Tidak diterima |

|    |                                    |                                                      |   |        |                |
|----|------------------------------------|------------------------------------------------------|---|--------|----------------|
| 11 | IK22                               | Kesalahan/bug pada perangkat lunak                   | 6 | Medium | Tidak diterima |
| 12 | IK25                               | <i>Denial of service</i>                             | 6 | Medium | Tidak diterima |
| 13 | IK63                               | Kegagalan perangkat jaringan                         | 6 | Medium | Tidak diterima |
| 14 | IK64                               | Kesalahan konfigurasi                                | 6 | Medium | Tidak diterima |
| 15 | IK125                              | Aktifitas <i>worm</i>                                | 6 | Medium | Tidak diterima |
| 16 | PT29                               | <i>Spam</i>                                          | 6 | Medium | Tidak diterima |
| 17 | IK24, IK35, PS22, PS29, PT12, PT27 | Akses tanpa izin                                     | 4 | Medium | Tidak diterima |
| 18 | PS25, PS32, PT15, PT22             | Penyebaran <i>malware</i>                            | 4 | Medium | Tidak diterima |
| 19 | IK21, IK32, IK40                   | Kesalahan konfigurasi                                | 4 | Medium | Tidak diterima |
| 20 | PS5, PS9, PS11                     | Kesalahan pembuatan data                             | 4 | Medium | Tidak diterima |
| 21 | IK47, IK59                         | Kegagalan akibat penggunaan melebihi batas kapasitas | 4 | Medium | Tidak diterima |
| 22 | IK102, IK106                       | Kegagalan perangkat lunak                            | 4 | Medium | Tidak diterima |

|    |                                      |                                                       |   |        |                |
|----|--------------------------------------|-------------------------------------------------------|---|--------|----------------|
| 23 | D1                                   | Kurang kualifikasi dalam mengkonfigurasi perangkat    | 4 | Medium | Tidak diterima |
| 24 | D11                                  | Kesalahan dalam membuat sistem informasi              | 4 | Medium | Tidak diterima |
| 25 | IK29                                 | Kegagalan dalam memulihkan data                       | 4 | Medium | Tidak diterima |
| 26 | IK30                                 | Kegagalan perangkat keras                             | 4 | Medium | Tidak diterima |
| 27 | IK31                                 | Penurunan kondisi media penyimpanan                   | 4 | Medium | Tidak diterima |
| 28 | IK33                                 | Kesalahan/bug pada perangkat lunak                    | 4 | Medium | Tidak diterima |
| 29 | IK122                                | Kegagalan koneksi                                     | 4 | Medium | Tidak diterima |
| 30 | IK136                                | Kerusakan kabel                                       | 4 | Medium | Tidak diterima |
| 31 | PS15                                 | Kesalahan pembuatan yang menyebabkan <i>bug/error</i> | 4 | Medium | Tidak diterima |
| 32 | IK26, IK36, PS23, PS30, PT13, PT20   | Pencurian perangkat keras                             | 3 | Low    | Diterima       |
| 33 | IK43, IK49, IK55, IK61, IK80, IK86   | Pencurian perangkat jaringan                          | 3 | Low    | Diterima       |
| 34 | IK137, IK139, PS20, PS27, PT10, PT17 | Kegagalan perangkat keras                             | 3 | Low    | Diterima       |

|    |                     |                                                      |   |            |          |
|----|---------------------|------------------------------------------------------|---|------------|----------|
| 35 | D4, D9, D14, PT32   | Penyalahgunaan hak akses dan tindakan ilegal lainnya | 3 | <i>Low</i> | Diterima |
| 36 | IK82                | Kegagalan perangkat jaringan                         | 3 | <i>Low</i> | Diterima |
| 37 | IK138, IK140, IK144 | Pencurian perangkat pelengkap                        | 3 | <i>Low</i> | Diterima |
| 38 | D7                  | Kesalahan dalam menggunakan perangkat TIK            | 3 | <i>Low</i> | Diterima |
| 39 | IK12                | Penghapusan <i>log</i> tanpa izin                    | 3 | <i>Low</i> | Diterima |
| 40 | IK83                | Kesalahan konfigurasi                                | 3 | <i>Low</i> | Diterima |
| 41 | IK129               | Kebakaran                                            | 3 | <i>Low</i> | Diterima |
| 42 | IK133               | Hubungan arus pendek                                 | 3 | <i>Low</i> | Diterima |
| 43 | IK141               | Petir                                                | 3 | <i>Low</i> | Diterima |
| 44 | IK142               | Kegagalan daya listrik                               | 3 | <i>Low</i> | Diterima |
| 45 | PS18                | Kode berbahaya pada <i>source code</i>               | 3 | <i>Low</i> | Diterima |
| 46 | PS19                | Pencurian dokumen/media penyimpanan                  | 3 | <i>Low</i> | Diterima |

|    |                                                                                  |                                     |   |            |          |
|----|----------------------------------------------------------------------------------|-------------------------------------|---|------------|----------|
| 47 | PT5                                                                              | Kerusakan/kehilangan data           | 3 | <i>Low</i> | Diterima |
| 48 | IK28, IK38, IK44, IK94, IK101, IK105, IK109, IK113, PS26, PS33, PS37, PT16, PT23 | Perubahan konfigurasi tanpa izin    | 2 | <i>Low</i> | Diterima |
| 49 | IK11, IK90, IK104, IK108, IK112, IK124, PS36, PT2, PT19                          | Akses tanpa izin                    | 2 | <i>Low</i> | Diterima |
| 50 | IK71, IK103, IK107, IK111, IK119, PS35                                           | Kesalahan Konfigurasi               | 2 | <i>Low</i> | Diterima |
| 51 | IK110, IK114, IK118, PS34, PT24, PT26                                            | Kegagalan perangkat lunak           | 2 | <i>Low</i> | Diterima |
| 52 | IK89, IK96, PS21, PS28, PT11, PT18                                               | Kesalahan/bug pada perangkat lunak  | 2 | <i>Low</i> | Diterima |
| 53 | IK92, IK99, PS24, PS31, PT14, PT21                                               | Penggunaan perangkat lunak ilegal   | 2 | <i>Low</i> | Diterima |
| 54 | IK6, PS6, PS12, PS16, PT1, PT9                                                   | Kerusakan/kehilangan data           | 2 | <i>Low</i> | Diterima |
| 55 | IK4, IK8, PS4, PS8, PS14                                                         | Pencurian dokumen/media penyimpanan | 2 | <i>Low</i> | Diterima |
| 56 | IK1, IK5, PT4, PT8                                                               | Kesalahan pembuatan data            | 2 | <i>Low</i> | Diterima |
| 57 | IK27, IK37, IK93, IK100                                                          | Penyebaran <i>malware</i>           | 2 | <i>Low</i> | Diterima |

|    |                   |                                                      |   |            |          |
|----|-------------------|------------------------------------------------------|---|------------|----------|
| 58 | IK34, IK65, IK84  | Kegagalan akibat penggunaan melebihi batas kapasitas | 2 | <i>Low</i> | Diterima |
| 59 | IK88, IK95, IK143 | Kegagalan perangkat keras                            | 2 | <i>Low</i> | Diterima |
| 60 | D2, D12           | Kesalahan dalam menggunakan perangkat TIK            | 2 | <i>Low</i> | Diterima |
| 61 | IK7, PS3          | Penyingkapan informasi                               | 2 | <i>Low</i> | Diterima |
| 62 | IK91, IK98        | Pencurian perangkat keras                            | 2 | <i>Low</i> | Diterima |
| 63 | D6                | Kesalahan dalam melayani pelanggan                   | 2 | <i>Low</i> | Diterima |
| 64 | IK10              | Waktu <i>log</i> tidak sama                          | 2 | <i>Low</i> | Diterima |
| 65 | IK67              | Pencurian perangkat jaringan                         | 2 | <i>Low</i> | Diterima |
| 66 | IK69              | Gangguan sinyal dari perangkat lain                  | 2 | <i>Low</i> | Diterima |
| 67 | IK70              | Kegagalan perangkat jaringan                         | 2 | <i>Low</i> | Diterima |
| 68 | IK123             | Lambatnya koneksi jaringan                           | 2 | <i>Low</i> | Diterima |
| 69 | IK126             | <i>Sniffing</i>                                      | 2 | <i>Low</i> | Diterima |

|    |                                                                           |                                                      |   |            |          |
|----|---------------------------------------------------------------------------|------------------------------------------------------|---|------------|----------|
| 70 | IK130                                                                     | Tidak sesuainya kondisi temperatur                   | 2 | <i>Low</i> | Diterima |
| 71 | IK135                                                                     | Gangguan elektromagnetik                             | 2 | <i>Low</i> | Diterima |
| 72 | IK42, IK48, IK54, IK60, IK66, IK73, IK79, IK85, IK97, IK116, IK120, IK131 | Akses tanpa izin                                     | 1 | <i>Low</i> | Diterima |
| 73 | IK50, IK56, IK62, IK68, IK75, IK81, IK87, IK117, IK121, PT25, PT28        | Perubahan konfigurasi tanpa izin                     | 1 | <i>Low</i> | Diterima |
| 74 | IK3, IK14, IK17, PS7, PS13, PS17, PT6                                     | Penyingkapan informasi                               | 1 | <i>Low</i> | Diterima |
| 75 | IK3, IK13, IK16, PS2, PS10                                                | Kerusakan/kehilangan data                            | 1 | <i>Low</i> | Diterima |
| 76 | IK15, IK18, PT7                                                           | Pencurian dokumen/media penyimpanan                  | 1 | <i>Low</i> | Diterima |
| 77 | IK72                                                                      | Kegagalan akibat penggunaan melebihi batas kapasitas | 1 | <i>Low</i> | Diterima |
| 78 | IK74                                                                      | Pencurian perangkat jaringan                         | 1 | <i>Low</i> | Diterima |
| 79 | IK115                                                                     | Kesalahan Konfigurasi                                | 1 | <i>Low</i> | Diterima |
| 80 | IK127                                                                     | Kegagalan dalam memulihkan data                      | 1 | <i>Low</i> | Diterima |



|    |       |                                              |   |            |          |
|----|-------|----------------------------------------------|---|------------|----------|
| 81 | IK128 | Gangguan ke sistem oleh vendor               | 1 | <i>Low</i> | Diterima |
| 82 | PS1   | Kesalahan pembuatan data                     | 1 | <i>Low</i> | Diterima |
| 83 | PT2   | Penyimpangan data yang dimasukkan            | 1 | <i>Low</i> | Diterima |
| 84 | PT30  | Kesalahan dalam menggunakan perangkat<br>TIK | 1 | <i>Low</i> | Diterima |

## **6. Kebijakan/Dokumen Terkait**

Kebijakan atau dokumen yang terkait dengan dokumen ini adalah sebagai berikut:

1. Daftar wawancara untuk penilaian resiko dapat dilihat pada Lampiran A.
2. Dokumen [Kebijakan SMKI] dapat dilihat pada Lampiran H.
3. Dokumen standar SNI ISO/IEC 27005:2013.
4. Dokumen standar SNI ISO/IEC 27001:2013.

*Halaman ini sengaja dikosongkan*

Direktorat Pengembangan Teknologi Sistem Informasi ITS

# PROSES PENANGANAN RESIKO

|                |                                  |
|----------------|----------------------------------|
| Nama Dokumen:  | Laporan Proses Penanganan Risiko |
| Versi          | 1                                |
| Tanggal        | 28/10/2017                       |
| Dibuat oleh    | Furqon Mauladani                 |
| Disetujui oleh |                                  |

## 1. Pendahuluan

Tujuan dari dokumen ini adalah mendefinisikan metodologi untuk penanganan risiko keamanan informasi dan menetapkan kontrol keamanan berdasarkan dokumen standar SNI ISO/IEC 27001:2013. Dokumen ini juga melaporkan hasil dari proses penanganan risiko.

## 2. Tahapan Penanganan Risiko

Beberapa tahapan dalam penanganan risiko adalah sebagai berikut:

1. Dapatkan hasil dari laporan [Proses Penilaian Risiko].
2. Pilih risiko yang tidak diterima oleh DPTSI-ITS.
3. Pemilihan penanganan risiko dengan kontrol-kontrol keamanan pada *Annex A* didalam dokumen standar SNI ISO/IEC 27001:2013 yang sesuai dengan sasaran kontrol keamanan dan deskripsi kontrol keamanan tersebut, atau merencanakan aktifitas menghindari risiko, membagi risiko atau menerima risiko.
4. Berdasarkan kontrol keamanan yang dipilih, selanjutnya dilakukan pemilihan apakah beberapa kontrol keamanan yang ada dapat diterapkan atau tidak. Contoh rincian dari penerapan kontrol keamanan terkait dapat dilihat pada dokumen standar SNI ISO/IEC 27002:2013 pada nomor atau kontrol keamanan yang sama. Rincian penerapan kontrol keamanan tidak diharuskan dari dokumen standar SNI ISO/IEC 27002:2013, namun bisa menggunakan standar lain atau praktek terbaik lainnya asal penanganan risiko sesuai dengan sasaran kontrol keamanan dan deskripsi kontrol keamanan tersebut.
5. Bila kontrol keamanan tersebut dapat diterapkan dan disetujui, maka pilih siapa yang akan bertanggung jawab dalam pelaksanaan kontrol keamanan tersebut.
6. Bila pemilihan kontrol keamanan pada sasaran kontrol keamanan sudah selesai, selanjutnya rancang [*Statement of Applicability*] yang berisi keseluruhan kontrol keamanan pada dokumen standar SNI ISO/IEC 27001:2013 dengan informasi tambahan seperti:

- Apa saja kontrol keamanan yang sudah diterapkan dan direncanakan untuk diterapkan.
- Siapa yang bertanggung jawab dalam pelaksanaan dan penerapan kontrol keamanan tersebut.

### **3. Komunikasi dan Konsultasi**

Laporan [Proses Penanganan Resiko] dan [*Statement of Applicability*] harus didokumentasikan dan dilaporkan ke pemangku kepentingan yang tepat, serta dijaga oleh tim pemimpin SMKI selaku yang bertanggung jawab dalam pengelolaan dokumen terkait SMKI.

### **4. Pengawasan dan Peninjauan**

Pimpinan bersama dengan komite pengendali SMKI harus melakukan peninjauan terhadap penanganan resiko yang ada saat ini dan memperbarui dokumen [Proses Penanganan Resiko] dan [*Statement of Applicability*] dengan kontrol-kontrol keamanan yang baru jika kurang efektif dalam menangani resiko. Peninjauan dapat dilakukan setahun sekali, atau lebih cepat bilamana ada kontrol keamanan yang ingin dievaluasi keefektifannya dalam jangka waktu kurang dari 1 tahun.

### **5. Laporan Proses Penanganan Resiko**

Hasil dari proses penilaian resiko dapat dilihat pada halaman dibawah ini.

Tabel J.1 Pemilihan Penanganan Resiko

| No Resiko                    | Resiko                                                                                                                                                                                                                                                                                                                                                                                              | Pemilihan Penanganan     |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| IK39, IK45, IK51, IK57, IK76 | Kegagalan perangkat jaringan                                                                                                                                                                                                                                                                                                                                                                        | <i>Risk Modification</i> |
|                              | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.8.1.1. Inventaris aset.</li> <li>• A.8.1.2. Kepemilikan aset.</li> <li>• A.11.2.4. Pemeliharaan perlengkapan.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.1.2. Manajemen perubahan.</li> <li>• A.17.2.1. Ketersediaan dari fasilitas pemrosesan informasi.</li> </ul> |                          |
| IK46, IK52, IK58, IK77       | Kesalahan konfigurasi                                                                                                                                                                                                                                                                                                                                                                               | <i>Risk Modification</i> |
|                              | <ul style="list-style-type: none"> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.8.1.4. Pengembalian aset.</li> </ul>                                                                                                                                                                                                                                        |                          |
| D10, PT33                    | Terkena aktifitas <i>social engineering</i>                                                                                                                                                                                                                                                                                                                                                         | <i>Risk Modification</i> |
|                              | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> </ul>                                                                                                                                                                                                                                                                                                          |                          |

|                   |                                                                                                                                                                                                                                                                                                                                                                                                     |                          |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
|                   | <ul style="list-style-type: none"> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.8.2.1. Klasifikasi informasi.</li> </ul>                                                                                                                                                                                                                                    |                          |
| IK19              | Kegagalan perangkat keras                                                                                                                                                                                                                                                                                                                                                                           | <i>Risk Modification</i> |
|                   | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.8.1.1. Inventaris aset.</li> <li>• A.8.1.2. Kepemilikan aset.</li> <li>• A.11.2.4. Pemeliharaan perlengkapan.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.1.2. Manajemen perubahan.</li> <li>• A.17.2.1. Ketersediaan dari fasilitas pemrosesan informasi.</li> </ul> |                          |
| IK20              | Penurunan kondisi media penyimpanan                                                                                                                                                                                                                                                                                                                                                                 | <i>Risk Modification</i> |
|                   | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.8.1.1. Inventaris aset.</li> <li>• A.8.1.2. Kepemilikan aset.</li> <li>• A.17.2.1. Ketersediaan dari fasilitas pemrosesan informasi.</li> </ul>                                                                                                                                                        |                          |
| IK23, IK41, IK53, | Kegagalan akibat penggunaan melebihi batas kapasitas                                                                                                                                                                                                                                                                                                                                                | <i>Risk Modification</i> |

|              |                                                                                                                                                                                                                    |                          |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| IK78         | <ul style="list-style-type: none"> <li>• A.12.1.3. Manajemen kapasitas.</li> </ul>                                                                                                                                 |                          |
| D3, D8, D13  | Absensi karyawan                                                                                                                                                                                                   | <i>Risk Modification</i> |
|              | <ul style="list-style-type: none"> <li>• A.12.1.3. Manajemen kapasitas.</li> </ul>                                                                                                                                 |                          |
| D5, D15      | Terkena aktifitas <i>social engineering</i>                                                                                                                                                                        | <i>Risk Modification</i> |
|              | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.8.2.1. Klasifikasi informasi.</li> </ul> |                          |
| IK132, IK134 | Kerusakan kabel                                                                                                                                                                                                    | <i>Risk Modification</i> |
|              | <ul style="list-style-type: none"> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.8.1.4. Pengembalian aset.</li> <li>• A.11.2.3. Keamanan pemasangan kabel.</li> </ul>       |                          |
| IK9          | Kerusakan/kehilangan data                                                                                                                                                                                          | <i>Risk Modification</i> |
|              | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.3.1. <i>Backup</i> informasi.</li> </ul>              |                          |



|      |                                                                                                                                                                                                                                                                                                                                                                                                     |                          |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| IK22 | Kesalahan/ <i>bug</i> pada perangkat lunak                                                                                                                                                                                                                                                                                                                                                          | <i>Risk Modification</i> |
|      | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.6.1. Manajemen kerentanan teknis.</li> <li>• A.14.2.4. Pembatasan pada perubahan paket perangkat lunak.</li> </ul>                                                                                                                     |                          |
| IK25 | <i>Denial of service</i>                                                                                                                                                                                                                                                                                                                                                                            | <i>Risk Sharing</i>      |
|      | <ul style="list-style-type: none"> <li>• Menyewa jasa pihak ketiga yang ahli dalam penanganan <i>denial of service</i>.</li> </ul>                                                                                                                                                                                                                                                                  |                          |
| IK63 | Kegagalan perangkat jaringan                                                                                                                                                                                                                                                                                                                                                                        | <i>Risk Modification</i> |
|      | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.8.1.1. Inventaris aset.</li> <li>• A.8.1.2. Kepemilikan aset.</li> <li>• A.11.2.4. Pemeliharaan perlengkapan.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.1.2. Manajemen perubahan.</li> <li>• A.17.2.1. Ketersediaan dari fasilitas pemrosesan informasi.</li> </ul> |                          |
| IK64 | Kesalahan konfigurasi                                                                                                                                                                                                                                                                                                                                                                               | <i>Risk Modification</i> |

|                                    |                                                                                                                                                                                                                                                                                                                                                  |                          |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
|                                    | <ul style="list-style-type: none"> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.8.1.4. Pengembalian aset.</li> </ul>                                                                                                                                                                                     |                          |
| IK125                              | Aktifitas <i>worm</i>                                                                                                                                                                                                                                                                                                                            | <i>Risk Modification</i> |
|                                    | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.1.2. Manajemen perubahan.</li> <li>• A.12.2.1. Kontrol terhadap <i>malware</i>.</li> <li>• A.12.6.1. Manajemen kerentanan teknis.</li> <li>• A.13.1.1. Kontrol jaringan.</li> </ul> |                          |
| PT29                               | <i>Spam</i>                                                                                                                                                                                                                                                                                                                                      | <i>Risk Avoidance</i>    |
|                                    | <ul style="list-style-type: none"> <li>• Tidak menggunakan layanan <i>email</i> mandiri. Secara umum untuk karyawan (non-pimpinan), dosen dan mahasiswa menggunakan layanan <i>email</i> google.</li> </ul>                                                                                                                                      |                          |
| IK24, IK35, PS22, PS29, PT12, PT27 | Akses tanpa izin                                                                                                                                                                                                                                                                                                                                 | <i>Risk Modification</i> |
|                                    | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.9.2.2. Penyediaan akses pengguna.</li> <li>• A.9.2.3. Manajemen hak akses <i>administrator</i>.</li> </ul>                                                                                                                                          |                          |

|                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                          |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
|                           | <ul style="list-style-type: none"> <li>• A.9.2.4. Manajemen informasi autentikasi rahasia dari pengguna.</li> <li>• A.9.2.5. Meninjau hak akses pengguna.</li> <li>• A.9.4.3. Sistem manajemen <i>password</i>.</li> <li>• A.11.2.8. Peralatan pengguna yang tidak diawasi.</li> <li>• A.11.2.9. Kebijakan merapihkan meja dan membersihkan layar.</li> </ul>                                                                                                                                                                                                           |                          |
| PS25, PS32, PT15,<br>PT22 | Penyebaran <i>malware</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <i>Risk Modification</i> |
|                           | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.11.2.4. Pemeliharaan perlengkapan.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.1.2. Manajemen perubahan.</li> <li>• A.12.2.1. Kontrol terhadap <i>malware</i>.</li> <li>• A.12.5.1. Pemasangan perangkat lunak pada sistem operasi.</li> <li>• A.12.6.1. Manajemen kerentanan teknis.</li> <li>• A.12.6.2. Pembatasan pemasangan perangkat lunak.</li> </ul> |                          |
| IK21, IK32, IK40          | Kesalahan konfigurasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <i>Risk Modification</i> |

|                |                                                                                                                                                                                                                                                                                 |                          |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
|                | <ul style="list-style-type: none"> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.8.1.4. Pengembalian aset.</li> </ul>                                                                                                                    |                          |
| PS5, PS9, PS11 | Kesalahan pembuatan data                                                                                                                                                                                                                                                        | <i>Risk Modification</i> |
|                | <ul style="list-style-type: none"> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.8.1.4. Pengembalian aset.</li> </ul>                                                                                                                    |                          |
| IK47, IK59     | Kegagalan akibat penggunaan melebihi batas kapasitas                                                                                                                                                                                                                            | <i>Risk Modification</i> |
|                | A.12.1.3. Manajemen kapasitas.                                                                                                                                                                                                                                                  |                          |
| IK102, IK106   | Kegagalan perangkat lunak                                                                                                                                                                                                                                                       | <i>Risk Modification</i> |
|                | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.6.1. Manajemen kerentanan teknis.</li> <li>• A.14.2.4. Pembatasan pada perubahan paket perangkat lunak.</li> </ul> |                          |
| D1             | Kurang kualifikasi dalam mengkonfigurasi perangkat                                                                                                                                                                                                                              | <i>Risk Modification</i> |
|                | <ul style="list-style-type: none"> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.8.1.4. Pengembalian aset.</li> </ul>                                                                                                                    |                          |

|      |                                                                                                                                                                                                                                                                                                                                                                                                     |                          |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| D11  | Kesalahan dalam membuat sistem informasi                                                                                                                                                                                                                                                                                                                                                            | <i>Risk Modification</i> |
|      | <ul style="list-style-type: none"> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.8.1.4. Pengembalian aset.</li> <li>• A.14.2.5. Prinsip keahlian teknis yang aman.</li> </ul>                                                                                                                                                                                |                          |
| IK29 | Kegagalan dalam memulihkan data                                                                                                                                                                                                                                                                                                                                                                     | <i>Risk Modification</i> |
|      | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.3.1. <i>Backup</i> informasi.</li> </ul>                                                                                                                                                                                               |                          |
| IK30 | Kegagalan perangkat keras                                                                                                                                                                                                                                                                                                                                                                           | <i>Risk Modification</i> |
|      | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.8.1.1. Inventaris aset.</li> <li>• A.8.1.2. Kepemilikan aset.</li> <li>• A.11.2.4. Pemeliharaan perlengkapan.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.1.2. Manajemen perubahan.</li> <li>• A.17.2.1. Ketersediaan dari fasilitas pemrosesan informasi.</li> </ul> |                          |

|       |                                                                                                                                                                                                                                                                                 |                          |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| IK31  | Penurunan kondisi media penyimpanan                                                                                                                                                                                                                                             | <i>Risk Modification</i> |
|       | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.8.1.1. Inventaris aset.</li> <li>• A.8.1.2. Kepemilikan aset.</li> <li>• A.17.2.1. Ketersediaan dari fasilitas pemrosesan informasi.</li> </ul>                                    |                          |
| IK33  | Kesalahan/ <i>bug</i> pada perangkat lunak                                                                                                                                                                                                                                      | <i>Risk Modification</i> |
|       | <ul style="list-style-type: none"> <li>• A.5.1.1. Kebijakan keamanan informasi.</li> <li>• A.12.1.1. Mendokumentasikan prosedur operasional.</li> <li>• A.12.6.1. Manajemen kerentanan teknis.</li> <li>• A.14.2.4. Pembatasan pada perubahan paket perangkat lunak.</li> </ul> |                          |
| IK122 | Kegagalan koneksi                                                                                                                                                                                                                                                               | <i>Risk Modification</i> |
|       | <ul style="list-style-type: none"> <li>• A.11.2.2. Utilitas pendukung.</li> </ul>                                                                                                                                                                                               |                          |
| IK136 | Kerusakan kabel                                                                                                                                                                                                                                                                 | <i>Risk Modification</i> |
|       | <ul style="list-style-type: none"> <li>• A.11.2.3. Keamanan pemasangan kabel.</li> </ul>                                                                                                                                                                                        |                          |
| PS15  | Kesalahan pembuatan yang menyebabkan <i>bug/error</i>                                                                                                                                                                                                                           | <i>Risk Modification</i> |

|                                      |                                                                                                                                                                                                                      |                       |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                                      | <ul style="list-style-type: none"> <li>• A.7.2.2. Kepedulian, pendidikan dan pelatihan keamanan informasi.</li> <li>• A.8.1.4. Pengembalian aset.</li> <li>• A.14.2.5. Prinsip keahlian teknis yang aman.</li> </ul> |                       |
| IK26, IK36, PS23, PS30, PT13, PT20   | Pencurian perangkat keras                                                                                                                                                                                            | <i>Risk Retention</i> |
| IK43, IK49, IK55, IK61, IK80, IK86   | Pencurian perangkat jaringan                                                                                                                                                                                         | <i>Risk Retention</i> |
| IK137, IK139, PS20, PS27, PT10, PT17 | Kegagalan perangkat keras                                                                                                                                                                                            | <i>Risk Retention</i> |
| D4, D9, D14, PT32                    | Penyalahgunaan hak akses dan tindakan ilegal lainnya                                                                                                                                                                 | <i>Risk Retention</i> |
| IK82                                 | Kegagalan perangkat jaringan                                                                                                                                                                                         | <i>Risk Retention</i> |
| IK138, IK140, IK144                  | Pencurian perangkat pelengkap                                                                                                                                                                                        | <i>Risk Retention</i> |
| D7                                   | Kesalahan dalam menggunakan perangkat TIK                                                                                                                                                                            | <i>Risk Retention</i> |
| IK12                                 | Penghapusan <i>log</i> tanpa izin                                                                                                                                                                                    | <i>Risk Retention</i> |

|                                                                                                 |                                        |                       |
|-------------------------------------------------------------------------------------------------|----------------------------------------|-----------------------|
| IK83                                                                                            | Kesalahan konfigurasi                  | <i>Risk Retention</i> |
| IK129                                                                                           | Kebakaran                              | <i>Risk Retention</i> |
| IK133                                                                                           | Hubungan arus pendek                   | <i>Risk Retention</i> |
| IK141                                                                                           | Petir                                  | <i>Risk Retention</i> |
| IK142                                                                                           | Kegagalan daya listrik                 | <i>Risk Retention</i> |
| PS18                                                                                            | Kode berbahaya pada <i>source code</i> | <i>Risk Retention</i> |
| PS19                                                                                            | Pencurian dokumen/media penyimpanan    | <i>Risk Retention</i> |
| PT5                                                                                             | Kerusakan/kehilangan data              | <i>Risk Retention</i> |
| IK28, IK38, IK44,<br>IK94, IK101,<br>IK105, IK109,<br>IK113, PS26,<br>PS33, PS37, PT16,<br>PT23 | Perubahan konfigurasi tanpa izin       | <i>Risk Retention</i> |
| IK11, IK90,<br>IK104, IK108,<br>IK112, IK124,<br>PS36, PT2, PT19                                | Akses tanpa izin                       | <i>Risk Retention</i> |



|                                              |                                                      |                       |
|----------------------------------------------|------------------------------------------------------|-----------------------|
| IK71, IK103,<br>IK107, IK111,<br>IK119, PS35 | Kesalahan Konfigurasi                                | <i>Risk Retention</i> |
| IK110, IK114,<br>IK118, PS34,<br>PT24, PT26  | Kegagalan perangkat lunak                            | <i>Risk Retention</i> |
| IK89, IK96, PS21,<br>PS28, PT11, PT18        | Kesalahan/bug pada perangkat lunak                   | <i>Risk Retention</i> |
| IK92, IK99, PS24,<br>PS31, PT14, PT21        | Penggunaan perangkat lunak ilegal                    | <i>Risk Retention</i> |
| IK6, PS6, PS12,<br>PS16, PT1, PT9            | Kerusakan/kehilangan data                            | <i>Risk Retention</i> |
| IK4, IK8, PS4,<br>PS8, PS14                  | Pencurian dokumen/media penyimpanan                  | <i>Risk Retention</i> |
| IK1, IK5, PT4,<br>PT8                        | Kesalahan pembuatan data                             | <i>Risk Retention</i> |
| IK27, IK37, IK93,<br>IK100                   | Penyebaran <i>malware</i>                            | <i>Risk Retention</i> |
| IK34, IK65, IK84                             | Kegagalan akibat penggunaan melebihi batas kapasitas | <i>Risk Retention</i> |

|                   |                                           |                       |
|-------------------|-------------------------------------------|-----------------------|
| IK88, IK95, IK143 | Kegagalan perangkat keras                 | <i>Risk Retention</i> |
| D2, D12           | Kesalahan dalam menggunakan perangkat TIK | <i>Risk Retention</i> |
| IK7, PS3          | Penyingkapan informasi                    | <i>Risk Retention</i> |
| IK91, IK98        | Pencurian perangkat keras                 | <i>Risk Retention</i> |
| D6                | Kesalahan dalam melayani pelanggan        | <i>Risk Retention</i> |
| IK10              | Waktu <i>log</i> tidak sama               | <i>Risk Retention</i> |
| IK67              | Pencurian perangkat jaringan              | <i>Risk Retention</i> |
| IK69              | Gangguan sinyal dari perangkat lain       | <i>Risk Retention</i> |
| IK70              | Kegagalan perangkat jaringan              | <i>Risk Retention</i> |
| IK123             | Lambatnya koneksi jaringan                | <i>Risk Retention</i> |
| IK126             | <i>Sniffing</i>                           | <i>Risk Retention</i> |
| IK130             | Tidak sesuainya kondisi temperatur        | <i>Risk Retention</i> |
| IK135             | Gangguan elektromagnetik                  | <i>Risk Retention</i> |

|                                                                                       |                                                      |                       |
|---------------------------------------------------------------------------------------|------------------------------------------------------|-----------------------|
| IK42, IK48, IK54,<br>IK60, IK66, IK73,<br>IK79, IK85, IK97,<br>IK116, IK120,<br>IK131 | Akses tanpa izin                                     | <i>Risk Retention</i> |
| IK50, IK56, IK62,<br>IK68, IK75, IK81,<br>IK87, IK117,<br>IK121, PT25,<br>PT28        | Perubahan konfigurasi tanpa izin                     | <i>Risk Retention</i> |
| IK3, IK14, IK17,<br>PS7, PS13, PS17,<br>PT6                                           | Penyingkapan informasi                               | <i>Risk Retention</i> |
| IK3, IK13, IK16,<br>PS2, PS10                                                         | Kerusakan/kehilangan data                            | <i>Risk Retention</i> |
| IK15, IK18, PT7                                                                       | Pencurian dokumen/media penyimpanan                  | <i>Risk Retention</i> |
| IK72                                                                                  | Kegagalan akibat penggunaan melebihi batas kapasitas | <i>Risk Retention</i> |
| IK74                                                                                  | Pencurian perangkat jaringan                         | <i>Risk Retention</i> |
| IK115                                                                                 | Kesalahan Konfigurasi                                | <i>Risk Retention</i> |

|       |                                           |                       |
|-------|-------------------------------------------|-----------------------|
| IK127 | Kegagalan dalam memulihkan data           | <i>Risk Retention</i> |
| IK128 | Gangguan ke sistem oleh vendor            | <i>Risk Retention</i> |
| PS1   | Kesalahan pembuatan data                  | <i>Risk Retention</i> |
| PT2   | Penyimpangan data yang dimasukkan         | <i>Risk Retention</i> |
| PT30  | Kesalahan dalam menggunakan perangkat TIK | <i>Risk Retention</i> |

Tabel J.2 Penetapan Kontrol Keamanan dan Sasaran Keamanan Informasi

| No<br><i>Annex</i> | Kontrol Keamanan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Sasaran Keamanan Informasi                                                          |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|                    | Kontrol Keamanan yang Ditetapkan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                     |
| A.5.1.1            | Kebijakan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Semua kebijakan tersedia dan disosialisasikan keseluruh pihak yang terkait.         |
|                    | <b><i>Administrative:</i></b> <ul style="list-style-type: none"> <li>• Pembuatan kebijakan Klasifikasian Informasi (A.8.2.1).</li> <li>• Pembuatan kebijakan Merapihkan Meja dan Membersihkan Layar (A.11.2.9).</li> <li>• Pembuatan kebijakan Manajemen Perubahan (A.12.1.2).</li> <li>• Pembuatan kebijakan Penanganan <i>Malware</i> (A.12.2.1).</li> <li>• Pembuatan kebijakan <i>Backup</i> Informasi (A.12.3.1).</li> <li>• Pembuatan kebijakan Pemasangan dan Penghapusan Perangkat Lunak (A.12.5.1).</li> <li>• Pembuatan kebijakan Manajemen Kerentanan Teknis (A.12.6.1).</li> <li>• Pembuatan kebijakan Pembatasan Penggunaan Perangkat Lunak (A.12.6.2).</li> </ul> |                                                                                     |
| A.5.1.2            | Peninjauan kebijakan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Semua kebijakan yang ada ditinjau secara berkala.                                   |
|                    | <b><i>Administrative:</i></b> <ul style="list-style-type: none"> <li>• Melakukan peninjauan kebijakan keamanan informasi berdasarkan penilaian resiko yang terkait.</li> <li>• Setiap peninjauan kebijakan keamanan informasi harus melibatkan dan disetujui oleh Direktur DPTSI-ITS.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                |                                                                                     |
| A.6.1.1            | Peran dan tanggung jawab keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Semua peran dan tanggung jawab diterapkan dan dilaksanakan oleh pihak yang terkait. |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                         |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         | <p><b><i>Administrative:</i></b></p> <ul style="list-style-type: none"> <li>• Peran dan tanggung jawab tim pengelola SMKI diterapkan sesuai dengan kebijakan SMKI. Struktur tim pengelola SMKI dapat dilihat pada Gambar 4.10.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                         |
| A.7.2.2 | Kepedulian, pendidikan dan pelatihan keamanan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Semua dosen, mahasiswa dan karyawan di ITS, sudah mengikuti program kesadaran keamanan, dan 30% karyawan DPTSI-ITS sudah mengikuti pelatihan kerja sesuai pekerjaannya. |
|         | <p><b><i>Administrative:</i></b></p> <ul style="list-style-type: none"> <li>• Mengadakan program kesadaran keamanan sekaligus memberitahukan kebijakan dan prosedur tentang keamanan informasi yang terkait kepada karyawan yang baru masuk baik PNS, non-PNS ataupun magang.</li> <li>• Menjadwalkan secara matriks dan mengadakan program kesadaran keamanan secara berkala terkait keamanan informasi, seperti peserta (internal DPTSI-ITS atau pengguna sistem), waktu, materi/topik, narasumber dan jenis pelatihan (seminar, madding ITS, publikasi <i>website</i>, atau pembaharuan <i>screensaver</i>).</li> <li>• Mengadakan pelatihan atau sertifikasi kerja bagi karyawan seperti Ms. SQL Server, Linux, pemrograman <i>web</i> (<i>PHP</i> dan <i>framework</i>-nya), pemasangan dan perbaikan <i>fiber optic</i>, CISCO, dan lainnya sesuai bidangnya secara merata dan rutin. Selain itu mengadakan pelatihan kerja bagi mahasiswa magang untuk dokumentasi sistem (<i>UML</i>, <i>flowchart</i>, <i>usecase</i>, dan lainnya) dan pemrograman <i>web</i> (<i>PHP</i> dan <i>framework</i>-nya).</li> <li>• Memperbaharui dokumen Matriks Kebutuhan Pelatihan SDM yang ada.</li> </ul> <p><b><i>Technical:</i></b></p> <ul style="list-style-type: none"> <li>• Memasang <i>screensaver</i> pada setiap komputer atau laptop dinas yang digunakan karyawan di DPTSI-ITS yang berisikan petunjuk, pengingat dan isu keamanan informasi.</li> </ul> |                                                                                                                                                                         |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                    |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
|         | <ul style="list-style-type: none"> <li>• Pengujian tingkat kesadaran terhadap keamanan informasi melalui Integra ITS. Setiap pemangku kepentingan selama 6 bulan sekali sebelum mengakses Integra ITS diharuskan menjawab pertanyaan tentang keamanan informasi untuk mengukur seberapa besar tingkat kesadarannya. Pertanyaan berisikan tentang isu-isu keamanan informasi, membedakan mana yang baik dan buruk pada aktifitas penggunaan TIK, kontrol keamanan apa yang harusnya dipasang di komputer atau perangkat <i>mobile</i> yang digunakan, dan lainnya.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                    |
| A.8.1.1 | Inventaris aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Semua aset informasi disetiap Subdit sudah didokumentasikan.                       |
|         | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Mendokumentasikan aset informasi yang dibuat, dikelola atau digunakan oleh masing-masing Subdit dan karyawan DPTSI-ITS lainnya kedalam dokumen Daftar Inventaris Aset Informasi. Dokumen ini disusun berdasarkan Daftar Inventaris Aset, Daftar Inventaris SIM dan Daftar Rekaman Mutu berikut data/informasi yang ada, seperti yang diolah sistem informasi (<i>database</i>), yang dibuat sistem (<i>log, backup, file konfigurasi</i>), maupun yang diolah manual baik berbentuk <i>file (word, spreadsheet)</i> atau dokumen. Dokumen ini berisikan nomor aset, nama aset, jenis aset (informasi, perangkat keras, perangkat lunak, dan lainnya sesuai dengan penelitian ini), bentuk aset (<i>fisik/nyata/hardcopy</i> atau <i>logic/tidak nyata/softcopy</i>), lokasi aset, pemilik aset.</li> <li>• Pencatatan perangkat keras didalam Daftar Inventaris Aset harus menyertakan informasi yang tepat terutama jumlah perangkat cadangan, dan yang sedang digunakan berikut tanggal garansi habis untuk masing-masing perangkat agar memudahkan dalam penyiapan perangkat cadangannya.</li> </ul> |                                                                                    |
| A.8.1.2 | Kepemilikan aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Semua aset informasi disetiap Subdit sudah didokumentasikan siapa pemilik asetnya. |
|         | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Mendokumentasikan siapa yang bertanggung jawab terhadap aset (pemilik aset) pada masing-masing aset secara lengkap dan jelas. Contohnya perangkat <i>AC</i> dan <i>UPS</i> pemilik asetnya adalah bapak Bustari, atau materi pelatihan dan dokumen ISO 9000 pemilik asetnya adalah ibu Widiyaningsih.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                    |

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                              |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| A.8.1.4 | Pengembalian aset                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Setiap karyawan mengisikan 5 ilmu yang dimiliki kedalam sistem <i>knowledge management</i> . |
|         | <b>Technical:</b> <ul style="list-style-type: none"> <li>• Menerapkan sistem <i>knowledge management</i> untuk mendokumentasikan ilmu-ilmu yang dimiliki karyawan selama bekerja di DPTSI-ITS.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                              |
| A.8.2.1 | Klasifikasi informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Semua aset bertipe informasi sudah diklasifikasikan berdasarkan bentuk dan kesensitifannya.  |
|         | <b>Administrative:</b> <ul style="list-style-type: none"> <li>• Mendokumentasikan klasifikasi kerahasiaan informasi berdasarkan tingkatan publik, internal dan rahasia untuk setiap data yang diolah sistem informasi (<i>database</i>), data yang dibuat sistem (<i>log, backup, file konfigurasi, ID login</i>), maupun data yang diolah manual baik berbentuk <i>file (worksheet, spreadsheet)</i> atau dokumen kertas.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                                                                              |
| A.9.2.2 | Penyediaan akses pengguna                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Semua hak akses diberikan sesuai dengan prosedur.                                            |
|         | <b>Administrative:</b> <ul style="list-style-type: none"> <li>• Melakukan verifikasi sebelum pemberian hak akses, apakah hak akses yang diberikan sesuai dengan tugas yang diemban karyawan tersebut, serta melakukan verifikasi dengan kebijakan kontrol akses.</li> <li>• Merekam hak akses yang dimiliki oleh karyawan pada <i>server</i>, perangkat lunak, perangkat jaringan dan akses fisik.</li> <li>• Mendokumentasikan prosedur penyediaan hak akses pengguna untuk sistem informasi, <i>server</i>, perangkat jaringan, komputer/laptop dinas dan akses fisik yang berisikan verifikasi tingkatan hak akses sesuai tugas, pemberian persetujuan, dokumentasi hak akses pengguna, dan lainnya.</li> <li>• Mendokumentasi prosedur penghapusan/pencabutan hak akses pengguna untuk sistem informasi, <i>server</i>, perangkat jaringan, komputer/laptop dinas dan akses fisik yang berisikan langkah-langkah dalam penghapusan hak akses.</li> </ul> |                                                                                              |



|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                     |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.9.2.3 | Manajemen hak akses <i>administrator</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Semua hak akses <i>administrator</i> diatur secara aman, dan semua <i>password</i> ( <i>default</i> vendor dan <i>administrator generic</i> ) pada perangkat sudah dikelola sesuai dengan prosedur. |
|         | <p><b><i>Administrative:</i></b></p> <ul style="list-style-type: none"> <li>• Mengidentifikasi dan mendokumentasikan hak akses apa saja yang dimiliki setiap sistem baik untuk sistem operasi, <i>DBMS</i> dan aplikasi lainnya.</li> <li>• Melakukan pembatasan dan penerapan tingkatan hak akses untuk komputer dan <i>server</i> dengan membatasi fungsi apa saja yang bisa dilakukan oleh karyawan tertentu. Misalnya hak akses dibagi menjadi tiga tingkatan yaitu pengguna biasa, <i>administrator</i> (yang dibatasi akses dan modifikasi <i>file log</i>), dan <i>administrator</i> penuh.</li> <li>• Memberikan hak akses yang berjangka waktu (<i>expired</i>) kepada karyawan yang bukan pemilik aset jika diperlukan saja, misalnya membantu karyawan pemilik aset dalam <i>troubleshooting</i>.</li> <li>• Memberikan dua jenis hak akses bagi <i>administrator</i>, satu untuk aktifitas <i>administrator</i> dan lainnya untuk aktifitas biasa.</li> <li>• Mendokumentasikan prosedur pengecekan <i>password default</i> vendor yang berisikan langkah-langkah dalam pemeriksaan apakah terdapat <i>password default</i> pada perangkat yang digunakan dan belum diganti.</li> <li>• Mendokumentasikan prosedur pengelolaan <i>sharing password administrator generic</i> yang berisikan langkah-langkah penggantian <i>password</i> secara berkala atau jika terdapat pengguna yang berhenti kerja, pemilihan kekuatan <i>password</i>, dan pengkomunikasian ke pengguna.</li> </ul> |                                                                                                                                                                                                     |
| A.9.2.4 | Manajemen informasi autentikasi rahasia dari pengguna                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Semua aktifitas <i>reset password</i> dilakukan sesuai dengan prosedur.                                                                                                                             |
|         | <p><b><i>Administrative:</i></b></p> <ul style="list-style-type: none"> <li>• Mendokumentasikan prosedur <i>reset password</i> sistem dan perangkat yang berisikan langkah-langkah dalam <i>reset password</i> untuk sistem informasi, <i>server</i>, perangkat jaringan atau komputer/laptop dinas.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                     |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                         |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| A.9.2.5  | Meninjau hak akses pengguna                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Semua hak akses ditinjau secara berkala.                                                                |
|          | <b>Administrative:</b> <ul style="list-style-type: none"> <li>• Mendokumentasikan prosedur peninjauan hak akses sistem dan perangkat yang berisikan langkah-langkah dalam peninjauan untuk melihat apakah terdapat hak akses yang belum terhapus didalam sistem, dan pengecekan kesesuaian hak akses yang diberikan dengan pekerjaan yang dilakukan karyawan.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                         |
| A.9.4.3  | Sistem manajemen <i>password</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Semua <i>server</i> , komputer dan laptop dinas sudah diatur sistem manajemen <i>password</i> baru.     |
|          | <b>Technical:</b> <ul style="list-style-type: none"> <li>• Mengatur agar <i>server</i> menggunakan <i>password</i> yang aman, seperti panjang <i>password</i> minimal 8 karakter, penggunaan kualitas kombinasi karakter, mencegah penggunaan <i>password</i> yang sama, tidak menampilkan <i>password</i> yang dimasukkan, harus mengganti <i>password</i> saat <i>login</i> pertama kali, dan harus mengganti <i>password</i> secara berkala.</li> <li>• Mengatur agar komputer atau laptop dinas menggunakan <i>password</i> yang aman, seperti panjang <i>password</i> minimal 8 karakter, penggunaan kualitas kombinasi karakter, mencegah penggunaan <i>password</i> yang sama, tidak menampilkan <i>password</i> yang dimasukkan, harus mengganti <i>password</i> saat <i>login</i> pertama kali, dan harus mengganti <i>password</i> secara berkala.</li> </ul> |                                                                                                         |
| A.11.2.2 | Utilitas pendukung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Semua layanan <i>ISP</i> sudah terpasang dan beroperasi secara benar.                                   |
|          | <b>Technical:</b> <ul style="list-style-type: none"> <li>• Menggunakan layanan <i>ISP</i> tambahan sebagai <i>backup</i> selain dari PT. Telkom.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                         |
| A.11.2.3 | Keamanan pemasangan kabel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Semua panduan dan perangkat pemasangan kabel tersedia, dan semua patok penanda kabel sudah diremajakan. |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                  |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Mendokumentasikan panduan Pengujian Kabel <i>Fiber Optic</i> yang berisikan tata cara pengujian apakah kabel tidak putus/rusak, dan panduan Perakitan Kabel (<i>Fiber Optic</i>) yang berisikan tata cara perakitan kabel <i>fiber optic</i>.</li> <li>• Merubah nama instruksi kerja <i>Cable Tester</i> menjadi panduan Pengujian Kabel <i>UTP</i>, dan instruksi kerja <i>Crimping Tools</i> menjadi panduan Perakitan Kabel (Kabel <i>UTP</i>).</li> </ul> <p><b>Physical:</b></p> <ul style="list-style-type: none"> <li>• Peremajaan patok penanda kabel yang sudah rusak atau hilang ("FO" untuk kabel <i>fiber optic</i> dan "2.0 VA" untuk kabel listrik).</li> <li>• Perangkat pemasangan kabel <i>fiber optic</i> seperti <i>crimping tool</i>, kabel cadangan, <i>jack</i>, <i>panel</i> dan lainnya.</li> </ul> |                                                                                                                  |
| A.11.2.4 | Pemeliharaan perlengkapan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Semua perangkat sudah dilakukan pemeliharaan perangkat sesuai dengan prosedur.                                   |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Melakukan pemeriksaan dan perawatan <i>server</i>, komputer, dan laptop dinas. Selain itu dilakukan perekaman setiap riwayat pemeriksaan dan perawatan yang dilakukan menggunakan <i>checklist</i> waktu, nama perangkat dan tanggal pemeriksaan/perawatan.</li> <li>• Mendokumentasikan prosedur Perawatan <i>Server</i>, dan prosedur Perawatan Komputer/Laptop Dinas untuk perawatan perangkat secara berkala.</li> <li>• Merekam semua riwayat perbaikan pada perangkat yang berisikan semua kesalahan sebenarnya atau yang diperkirakan, dan semua tindakan pencegahan atau perbaikannya.</li> <li>• Melakukan pengecekan kode <i>BIOS</i> dengan yang ada di <i>website</i> resmi vendor perangkat keras atau jaringan, apakah tidak ada penyimpangan versi setelah perangkat diperbaiki atau dibeli.</li> </ul>       |                                                                                                                  |
| A.11.2.8 | Peralatan pengguna yang tidak diawasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Semua komputer dan laptop dinas sudah dikonfigurasi agar menggunakan <i>screensaver</i> dengan <i>password</i> . |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                   |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
|          | <p><b>Technical:</b></p> <ul style="list-style-type: none"> <li>• Mengkonfigurasi komputer dan laptop dinas milik DPTSI-ITS agar sistem menjalankan <i>screensaver</i> yang diberi <i>password</i> ketika tidak digunakan atau ditinggal.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                   |
| A.11.2.9 | Kebijakan merapihkan meja dan membersihkan layar                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Menurunkan jumlah kesalahan praktik keamanan informasi didalam kantor dibanding tahun sebelumnya. |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Mendokumentasikan kebijakan <i>clear desk and screen</i> yang berisikan aturan terkait kerapihan meja kerja dari dokumen, <i>flashdisk</i> atau media penyimpanan lainnya, maupun membersihkan layar monitor dari catatan terutama informasi akun pengguna. Sebagian topik yang terdapat pada kebijakan adalah: <ul style="list-style-type: none"> <li>○ Mengunci dokumen rahasia/sensitif langsung didalam lemari jika tidak diperlukan (tidak meninggalkan di meja).</li> <li>○ Tidak menaruh <i>CD/DVD</i>, <i>flashdisk</i> atau <i>hardisk</i> eksternal di meja.</li> <li>○ Tidak meninggalkan dokumen apapun di <i>printer</i> atau <i>scanner</i> terutama yang bersifat sensitif.</li> <li>○ Tidak mencatat dan menempel kertas pada layar yang berisi <i>password</i> atau informasi rahasia apapun.</li> <li>○ Tidak meninggalkan komputer dalam keadaan tidak terkunci <i>password</i> dan <i>log-off</i>.</li> <li>○ Langsung menghapus tulisan di <i>whiteboard</i> setelah rapat.</li> </ul> </li> </ul> |                                                                                                   |
| A.12.1.1 | Mendokumentasikan prosedur operasional                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Semua prosedur tersedia dan disosialisasikan keseluruh karyawan yang terkait.                     |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Pembuatan prosedur Penyediaan Hak Akses Pengguna (A.9.2.2).</li> <li>• Pembuatan Prosedur Penghapusan/Pencabutan Hak Akses Pengguna (A.9.2.2).</li> <li>• Pembuatan prosedur Pengecekan <i>Password Default</i> Vendor (A.9.2.3).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                   |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                   |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>• Pembuatan prosedur Pengelolaan <i>Sharing Password Administrator Generic</i> (A.9.2.3).</li> <li>• Pembuatan prosedur <i>Reset Password</i> Sistem dan Perangkat (A.9.2.4).</li> <li>• Pembuatan prosedur Peninjauan Hak Akses Sistem dan Perangkat (A.9.2.5).</li> <li>• Pembuatan prosedur Perawatan <i>Server</i> (A.11.2.4).</li> <li>• Pembuatan prosedur Perawatan Komputer/Laptop Dinas (A.11.2.4).</li> <li>• Pembuatan prosedur Manajemen Perubahan (A.12.1.2).</li> <li>• Pembuatan prosedur Pemulihan dari Kegagalan Perubahan (A.12.1.2).</li> <li>• Pembuatan prosedur Penanganan <i>Malware</i> (A.12.2.1).</li> <li>• Pembuatan prosedur Peringatan <i>Malware</i> (A.12.2.1).</li> <li>• Pembuatan prosedur Pengawasan dan Pengujian Hasil <i>Backup</i> (A.12.3.1).</li> <li>• Pembuatan prosedur Pemasangan Perangkat Lunak (A.12.5.1).</li> <li>• Pembuatan prosedur Penghapusan Perangkat Lunak (A.12.5.1).</li> <li>• Pembuatan prosedur Manajemen Kerentanan Teknis (A.12.6.1).</li> <li>• Pembuatan prosedur Modifikasi Paket Instalasi Perangkat Lunak (A.14.2.4).</li> </ul> |                                                   |
| A.12.1.2 | Manajemen perubahan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Semua perubahan dilakukan sesuai dengan prosedur. |
|          | <p><b><i>Administrative:</i></b></p> <ul style="list-style-type: none"> <li>• Mengklasifikasikan apa saja aktifitas perubahan yang memerlukan persetujuan formal ataupun yang tidak memerlukannya, dan yang memerlukan penilaian dampak/isu keamanan.</li> <li>• Melakukan identifikasi dan pendokumentasian setiap perubahan yang dilakukan untuk semua Subdit di DPTSI-ITS. Dokumen tersebut berisikan waktu perubahan, petugas yang terlibat dalam perubahan, apa yang dirubah, dokumen pendukung (seperti konfigurasi atau perencanaan), dan hasil perubahan.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                   |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                          |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>• Melakukan penilaian dampak/isu keamanan yang berpotensi jika terjadi perubahan berdasarkan klasifikasi perubahan, contohnya <i>server</i> dan perangkat jaringan yang berhubungan dengan proses bisnis tertentu.</li> <li>• Mendokumentasikan kebijakan manajemen perubahan yang berisikan aturan dalam perubahan, klasifikasi perubahan, pengujian dan penilaian dampak pada perubahan, cara mengkomunikasikan perubahan, dan lainnya.</li> <li>• Mendokumentasikan prosedur pemulihan perubahan untuk mengembalikan kondisi sistem ke keadaan semula jika terjadi kegagalan dalam penerapan perubahan baru.</li> <li>• Mendokumentasikan prosedur manajemen perubahan umum yang digunakan untuk semua perubahan baik pada perangkat keras/lunak/jaringan, organisasi, proses bisnis dan lainnya.</li> </ul>                                                                                                                                                                                                  |                                                                                                                                                                          |
| A.12.1.3 | Manajemen kapasitas                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | Menurunkan insiden kegagalan akibat melebihi kapasitas sebanyak 50% dibanding tahun lalu, dan mengurangi level resiko pada resiko absensi karyawan dibanding sebelumnya. |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Peremajaan perangkat jaringan yang melebihi kapasitas dengan perangkat yang memiliki spesifikasi untuk melayani <i>request</i> yang lebih tinggi dari perangkat sebelumnya. Perangkat yang dimaksud adalah Frey Internet Router, <i>core switch</i>, Cisco ASA Firewall, Sangfor Internet Access Management, dan <i>distribution switch</i>.</li> <li>• Mengidentifikasi kebutuhan minimum jumlah karyawan di DPTSI-ITS dengan menggunakan metode <i>workload analysis</i>. Lalu menambah jumlah karyawan disetiap Subdit berdasarkan hasil <i>workload analysis</i>.</li> <li>• Mendokumentasikan perencanaan manajemen kapasitas kedepan untuk sistem kritis dengan cara melihat riwayat data penggunaan sistem dan jaringan yang dikumpulkan oleh Cacti dan melakukan analisa tren penggunaannya.</li> <li>• Mendokumentasikan perencanaan kapasitas kedepan untuk karyawan di DPTSI-ITS dengan cara analisa tren pada data riwayat kebutuhan penambahan karyawan.</li> </ul> |                                                                                                                                                                          |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                        |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| A.12.2.1 | Kontrol terhadap <i>malware</i>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Menurunkan jumlah insiden <i>malware</i> sebanyak 50% dibanding tahun sebelumnya.      |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Mengklasifikasikan sistem kritis yang akan dilakukan peninjauan apakah terdapat <i>file</i> atau penambahan tanpa izin secara formal dan berkala. Setelah itu menjadwalkan aktifitas peninjauan yang akan dilakukan.</li> <li>• Melakukan karantina sistem apapun jika terdapat infeksi <i>malware</i> agar tidak menyebar ke sistem lain sebelum dibersihkan.</li> <li>• Menetapkan peran dan tanggung jawab untuk mengurus masalah <i>malware</i>, seperti penanganan <i>malware</i> pada sistem, pelatihan penggunaan perangkat <i>anti-malware</i>, pelaporan dan pemulihan dari serangan <i>malware</i>.</li> <li>• Mendokumentasikan kebijakan penanganan <i>malware</i> yang berisikan aturan dalam penanganan <i>malware</i>, klasifikasi sistem kritis yang ditinjau, dan cara mendapatkan <i>file</i> atau perangkat lunak pada <i>internet</i> atau media lainnya baik untuk pengguna maupun <i>administrator</i>.</li> <li>• Mendokumentasikan prosedur penanganan <i>malware</i> yang berisikan langkah-langkah pelaporan, penanganan dan pemulihan dari serangan <i>malware</i>.</li> <li>• Mendokumentasikan prosedur peringatan <i>malware</i> yang berisikan bagaimana pengumpulan informasi mengenai <i>malware</i> baru dari <i>internet</i>, verifikasi kebenaran informasi, dan pemberitahuan informasi kepada pengguna.</li> </ul> <p><b>Technical:</b></p> <ul style="list-style-type: none"> <li>• Menggunakan perangkat lunak untuk meng-<i>clone hardisk</i> dan meng-<i>clone</i> keseluruhan sistem jika sistem yang terinfeksi <i>malware</i> tidak dapat ditangani dengan cara apapun. <i>Clone</i> disimpan untuk penelitian lebih lanjut. Sistem yang terinfeksi tersebut dilakukan instalasi ulang dengan memperhatikan <i>backup</i> data yang tersedia.</li> </ul> |                                                                                        |
| A.12.3.1 | <i>Backup</i> informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Semua aktifitas <i>backup</i> dilakukan sesuai dengan prosedur dan kebijakan yang ada. |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                    |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Mendokumentasikan kebijakan <i>backup</i> yang berisikan aturan dalam melakukan <i>backup</i> (baik informasi, perangkat lunak dan sistem), banyaknya <i>copy</i> hasil <i>backup</i>, serta cara pengujian dan pengamanannya.</li> <li>• Mendefinisikan apa saja yang perlu dilakukan <i>backup</i> secara berganda sesuai dengan kebutuhan bisnis (misalnya data <i>log</i> pada SIEM AlienVault atau sistem lainnya).</li> <li>• Melakukan ujicoba <i>backup</i> secara berkala data <i>backup</i> yang disimpan dengan melakukan restorasi data ke sistem <i>clone</i> yang disediakan untuk dilakukan pengujian.</li> <li>• Mendokumentasi prosedur pengawasan dan pengujian hasil <i>backup</i> yang berisikan pemeriksaan aktifitas <i>backup</i> dan kegagalan yang terjadi, pengujian hasil <i>backup</i> kedalam sistem untuk pengujian, dan penilaian hasil uji coba berdasarkan data yang berhasil dipulihkan.</li> </ul> <p><b>Technical:</b></p> <ul style="list-style-type: none"> <li>• Sistem <i>clone</i> untuk pengujian <i>backup</i> yang berisikan sistem operasi, perangkat lunak dan konfigurasi yang identik dengan sistem aslinya yang di <i>backup</i>.</li> </ul> |                                                                    |
| A.12.5.1 | Pemasangan perangkat lunak pada sistem operasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Semua pemasangan perangkat lunak dilakukan sesuai dengan prosedur. |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Menyimpan perangkat lunak sebelumnya beserta catatan lengkap yang berisikan informasi perangkat lunak, prosedur, dan rincian konfigurasi.</li> <li>• Mendokumentasikan kebijakan pemasangan dan penghapusan perangkat lunak yang berisikan peran dan tanggung jawab karyawan, aturan pemasangan perangkat lunak pada komputer dan <i>server</i>, apa yang harus disimpan dan dilakukan ketika pemasangan, dan lainnya.</li> <li>• Mendokumentasikan prosedur pemasangan atau penghapusan perangkat lunak yang tidak dikembangkan DPTSI-ITS yang berisikan langkah-langkah dalam pemasangan, pengujian atau penghapusan perangkat lunak pada komputer dan <i>server</i>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                    |



|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                          |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
|          | <p><b>Technical:</b></p> <ul style="list-style-type: none"> <li>• Memasang sistem manajemen konfigurasi (seperti Puppet, Chef dan lainnya) untuk mengontrol semua konfigurasi <i>server</i> yang berupa <i>template</i>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                                          |
| A.12.6.1 | Manajemen kerentanan teknis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Versi perangkat lunak yang sudah diklasifikasikan harus sama dengan versi rilis terbaru. |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Menetapkan secara khusus karyawan yang melakukan manajemen kerentanan teknis untuk masalah <i>patch/update</i> dari Subdit Infrastruktur untuk mengelola <i>server</i> (sistem operasi dan perangkat lunaknya) dan perangkat jaringan, dan dari Subdit Pelayanan untuk mengelola komputer dan laptop dinas (sistem operasi dan perangkat lunaknya).</li> <li>• Mengklasifikasikan tingkat kepentingan pemasangan <i>patch</i> pada perangkat lunak, apakah tingkatan <i>high</i> seperti yang berkaitan dengan proses bisnis (contohnya Ms. SQL Server, PHP server) atau keamanan informasi (contohnya <i>anti-virus</i>), tingkatan <i>medium</i> seperti perangkat lunak pendukung (contohnya Ms. Office, Adobe Photoshop), dan tingkatan <i>low</i> seperti <i>driver</i> dan perangkat lunak lainnya.</li> <li>• Mengawasi kerentanan baru berdasarkan klasifikasi melalui forum/<i>website</i> keamanan informasi (seperti NIST National Vulnerability Database di <a href="https://nvd.nist.gov/">https://nvd.nist.gov/</a>, Offensive Security's Exploit Database Archive di <a href="https://www.exploit-db.com/">https://www.exploit-db.com/</a>, atau CVE di <a href="http://www.cvedetails.com/">http://www.cvedetails.com/</a>) dan mengawasi rilis terbaru <i>patch/update</i> dari <i>website</i> vendor perangkat lunak secara berkala dan terjadwal.</li> <li>• Melakukan aktifitas identifikasi resiko dan penanganan resiko ketika kerentanan telah teridentifikasi. Selain itu memperbaharui laporan proses penilaian resiko di Lampiran I dan laporan proses penanganan resiko di Lampiran J.</li> <li>• Membandingkan resiko yang ada ketika memasang <i>patch</i> (contohnya jika menurunnya performa dan konflik dengan sistem) dengan kerentanan yang ada.</li> </ul> |                                                                                          |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                     |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------|
|          | <ul style="list-style-type: none"> <li>• Jika <i>patch</i> tidak bisa dipasang maka harus direkam. DPTSI-ITS dapat mempertimbangkan menon-aktifkan layanan tertentu yang terkait kerentanan, mengubah konfigurasi perangkat jaringan, menambah pengawasan ketika serangan terdeteksi, atau memberikan pelatihan kepada karyawan tentang kerentanan.</li> <li>• Melakukan perekaman riwayat aktifitas pemasangan <i>patch</i>, seperti waktu <i>patch</i>, petugas, nama perangkat lunak, hasil aktifitas (gagal/berhasil), alasan gagal, dan penanggulangan untuk <i>patch</i> yang gagal.</li> <li>• Melakukan manajemen kerentanan teknis berdasarkan dokumen kebijakan dan prosedur untuk penambahan informasi pembantu ketika terjadi insiden.</li> <li>• Mendokumentasikan kebijakan manajemen kerentanan teknis yang berisikan peran dan tanggung jawab karyawan, aturan pengawasan kerentanan dan pembaharuan <i>patch</i>, dan lainnya.</li> <li>• Mendokumentasikan prosedur manajemen kerentanan teknis yang berisikan langkah-langkah dalam manajemen <i>patch</i> mulai dari identifikasi sampai pengujian <i>patch</i> yang akan dipasang dan penyediaan informasi untuk manajemen insiden (termasuk kerentanan yang telah teridentifikasi namun belum memenuhi penanganan yang tepat).</li> </ul> |                                                                     |
| A.12.6.2 | Pembatasan pemasangan perangkat lunak                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Semua perangkat lunak yang dilarang tidak terpasang didalam sistem. |
|          | <b>Administrative:</b> <ul style="list-style-type: none"> <li>• Mendokumentasikan kebijakan pembatasan penggunaan perangkat lunak yang berisikan rincian perangkat lunak apa saja yang boleh dipasang (baik yang tidak perlu perizinan ataupun yang memerlukan perizinan dahulu) dan yang tidak boleh dipasang.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                     |
| A.13.1.1 | Kontrol jaringan                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Fitur baru terpasang pada perangkat secara benar.                   |
|          | <b>Technical:</b> <ul style="list-style-type: none"> <li>• Pembelian lisensi fitur <i>anti-virus</i> pada perangkat Cisco ASA Firewall 5540.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                     |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                 |
|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| A.14.2.4 | Pembatasan pada perubahan paket perangkat lunak                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Semua modifikasi paket instalasi perangkat lunak dilakukan sesuai dengan prosedur.                              |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Setiap aktifitas modifikasi paket instalasi perangkat lunak yang dilakukan harus mempertimbangkan persetujuan atau rekomendasi dari vendor, kemungkinan mendapatkan pembaharuan dari vendor, dampak dari perubahan, dan kompatibilitas dengan perangkat lunak lain.</li> <li>• Setiap aktifitas modifikasi paket instalasi perangkat lunak dilakukan perekaman riwayatnya seperti waktu modifikasi, petugas, perangkat lunak yang dimodifikasi, apa yang dimodifikasi dari perangkat lunak tersebut, dan hasil pengujian.</li> <li>• Menguji secara formal hasil modifikasi paket instalasi perangkat lunak yang dilakukan dan mendapatkan izin dari Kasubdit Pengembangan.</li> <li>• Mendokumentasikan prosedur modifikasi paket instalasi perangkat lunak yang berisikan langkah-langkah dalam perencanaan, pengujian dan pendokumentasian perubahan.</li> </ul> |                                                                                                                 |
| A.14.2.5 | Prinsip keahlian teknis yang aman                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Semua pengembangan SIM baru atau pembaharuan sudah mengikuti penggunaan standar teknis dan <i>source code</i> . |
|          | <p><b>Administrative:</b></p> <ul style="list-style-type: none"> <li>• Membuat standar teknis untuk pemrograman yang aman untuk bahasa pemrograman <i>PHP</i> dan Ms. SQL Server yang berisi tata cara penulisan <i>source code</i> dan struktur yang disetujui, teknik autentikasi pengguna, mengamankan <i>session</i> ataupun <i>cookies</i>, validasi data, menghilangkan <i>debug</i> pada <i>source code</i>, dan lainnya.</li> <li>• Mengharuskan setiap karyawan diluar Subdit Pengembangan yang ingin membangun sistem informasi mengikuti standar teknis dan memasukkan standar <i>source code</i> yang dibuat.</li> <li>• Meninjau standar teknis dan standar <i>source code</i> secara berkala untuk memastikan agar selalu terbaharui dalam menangani potensi ancaman terbaru.</li> </ul>                                                                                                                                     |                                                                                                                 |

|          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                              |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|
|          | <b>Technical:</b> <ul style="list-style-type: none"> <li>Memiliki standar <i>source code</i> yang merupakan fungsi tertentu yang sudah diuji dan diizinkan untuk dimasukkan ke perangkat lunak baru untuk memenuhi standar keamanan, seperti fungsi autentikasi, enkripsi, <i>backup</i> data dan lainnya.</li> </ul>                                                                                                                                                                                                                                                                                                                                          |                                                                              |
| A.17.2.1 | Ketersediaan dari fasilitas pemrosesan informasi                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Setiap perangkat keras atau jaringan sudah memiliki cadangan dan komponennya |
|          | <b>Administrative:</b> <ul style="list-style-type: none"> <li>Mendefinisikan beberapa perangkat keras/jaringan atau komponennya yang dirasakan kritis untuk segera disediakan cadangannya dengan mempertimbangkan proses bisnis yang terlibat.</li> </ul> <b>Technical:</b> <ul style="list-style-type: none"> <li>Menyiapkan cadangan perangkat (<i>firewall</i>, <i>core switch</i>, <i>distribution switch</i> dan lainnya) ataupun komponen (<i>processor</i>, <i>memory</i>, <i>hardisk</i>, dan lainnya), jika suatu perangkat atau komponen perangkat didefinisikan kritis, sedang digunakan/beroperasional dan sudah melewati umur garansi.</li> </ul> |                                                                              |

Tabel J.3 Hubungan Kelompok Resiko dengan Domain Kontrol Keamanan SNI ISO/IEC 27001

| No Annex | Domain Kontrol Keamanan      | Kelompok Resiko                                                                                                                                                                                                                                                                                                                                                            |
|----------|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.5      | Kebijakan keamanan informasi | <ul style="list-style-type: none"> <li>Kegagalan perangkat jaringan.</li> <li>Terkena aktifitas <i>social engineering</i>.</li> <li>Kegagalan perangkat keras.</li> <li>Penurunan kondisi media penyimpanan.</li> <li>Kerusakan/kehilangan data.</li> <li>Kesalahan/<i>bug</i> pada perangkat lunak.</li> <li>Aktifitas <i>worm</i>.</li> <li>Akses tanpa izin.</li> </ul> |

|     |                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.5 | Kebijakan keamanan informasi<br>(lanj.) | <ul style="list-style-type: none"> <li>• Penyebaran <i>malware</i>.</li> <li>• Kegagalan perangkat lunak.</li> <li>• Kegagalan dalam memulihkan data.</li> </ul>                                                                                                                                                                                                                                                                                                                                                         |
| A.7 | Keamanan sumber daya manusia            | <ul style="list-style-type: none"> <li>• Kesalahan konfigurasi.</li> <li>• Terkena aktifitas <i>social engineering</i>.</li> <li>• Kerusakan kabel.</li> <li>• Penyebaran <i>malware</i>.</li> <li>• Kesalahan pembuatan data.</li> <li>• Kurang kualifikasi dalam mengkonfigurasi perangkat.</li> <li>• Kesalahan dalam membuat sistem informasi.</li> <li>• Kesalahan pembuatan yang menyebabkan <i>bug/error</i>.</li> </ul>                                                                                          |
| A.8 | Manajemen aset                          | <ul style="list-style-type: none"> <li>• Kegagalan perangkat jaringan.</li> <li>• Kesalahan konfigurasi.</li> <li>• Terkena aktifitas <i>social engineering</i>.</li> <li>• Kegagalan perangkat keras.</li> <li>• Penurunan kondisi media penyimpanan.</li> <li>• Kerusakan kabel.</li> <li>• Kesalahan pembuatan data.</li> <li>• Kurang kualifikasi dalam mengkonfigurasi perangkat.</li> <li>• Kesalahan dalam membuat sistem informasi.</li> <li>• Kesalahan pembuatan yang menyebabkan <i>bug/error</i>.</li> </ul> |
| A.9 | Kontrol akses                           | <ul style="list-style-type: none"> <li>• Akses tanpa izin.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

|      |                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.11 | Keamanan fisik dan lingkungan                                  | <ul style="list-style-type: none"> <li>• Kegagalan perangkat jaringan.</li> <li>• Kegagalan perangkat keras.</li> <li>• Kerusakan kabel.</li> <li>• Akses tanpa izin.</li> <li>• Penyebaran <i>malware</i>.</li> <li>• Kegagalan koneksi.</li> </ul>                                                                                                                                                                                                                        |
| A.12 | Keamanan operasional                                           | <ul style="list-style-type: none"> <li>• Kegagalan perangkat jaringan.</li> <li>• Kegagalan perangkat keras.</li> <li>• Kegagalan akibat penggunaan melebihi batas kapasitas.</li> <li>• Absensi karyawan.</li> <li>• Kerusakan/kehilangan data.</li> <li>• Kesalahan/<i>bug</i> pada perangkat lunak.</li> <li>• Aktifitas <i>worm</i>.</li> <li>• Penyebaran <i>malware</i>.</li> <li>• Kegagalan perangkat lunak.</li> <li>• Kegagalan dalam memulihkan data.</li> </ul> |
| A.13 | Keamanan komunikasi                                            | <ul style="list-style-type: none"> <li>• Aktifitas <i>worm</i>.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                  |
| A.14 | Akuisisi, pengembangan dan pemeliharaan sistem                 | <ul style="list-style-type: none"> <li>• Kesalahan/<i>bug</i> pada perangkat lunak.</li> <li>• Kegagalan perangkat lunak.</li> <li>• Kesalahan dalam membuat sistem informasi.</li> <li>• Kesalahan pembuatan yang menyebabkan <i>bug/error</i>.</li> </ul>                                                                                                                                                                                                                 |
| A.17 | Aspek keamanan informasi akan manajemen keberlangsungan bisnis | <ul style="list-style-type: none"> <li>• Kegagalan perangkat jaringan.</li> <li>• Kegagalan perangkat keras.</li> <li>• Penurunan kondisi media penyimpanan.</li> </ul>                                                                                                                                                                                                                                                                                                     |

## **6. Kebijakan/Dokumen Terkait**

Kebijakan atau dokumen yang terkait dengan dokumen ini adalah sebagai berikut:

1. Laporan [Proses Penilaian Resiko] dapat dilihat pada Lampiran I.
2. Dokumen [*Statement of Applicability*] dapat dilihat pada Lampiran K.
3. Dokumen standar SNI ISO/IEC 27001:2013.
4. Dokumen standar SNI ISO/IEC 27002:2013.

Direktorat Pengembangan Teknologi Sistem Informasi ITS

## *STATEMENT OF APPLICABILITY*

|                |                                                 |
|----------------|-------------------------------------------------|
| Nama Dokumen   | Dokumen <i>Statement of Applicability</i> (SoA) |
| Versi          | 1                                               |
| Tanggal        | 28/10/2017                                      |
| Dibuat oleh    | Furqon Mauladani                                |
| Disetujui oleh |                                                 |

### **1. Pendahuluan**

Tujuan dari dokumen ini adalah meringkas kontrol keamanan apa saja yang sudah diterapkan, dan yang direncanakan untuk diterapkan beserta penanggung jawabnya. Dokumen ini memudahkan untuk memeriksa apakah sasaran yang direncanakan pada dokumen [Sasaran Keamanan Informasi] terpenuhi dan apakah penerapan kontrol keamanan pada laporan [Proses Penanganan Resiko] berjalan lancar.

### **2. Ruang Lingkup**

Dokumen ini mencakup keseluruhan kontrol keamanan yang ada pada *Annex A* didalam dokumen standar SNI ISO/IEC 27001:2013.

### **3. Dokumen *Statement of Applicability***

Hasil dari pembuatan dokumen *Statement of Applicability* dapat dilihat pada halaman dibawah ini. Maksud dari PHK adalah persyaratan hukum atau kontrak, KB adalah kebutuhan bisnis, dan PR adalah penanganan resiko.



Tabel K.1 *Statement of Applicability*

| Domain Kontrol Keamanan                        | Kontrol Keamanan dan Sasaran Kontrol Keamanan             | Kontrol Saat Ini | Alasan Pemilihan Kontrol Keamanan |    |    | Penanggung Jawab                                                                                                                           |
|------------------------------------------------|-----------------------------------------------------------|------------------|-----------------------------------|----|----|--------------------------------------------------------------------------------------------------------------------------------------------|
|                                                |                                                           |                  | PHK                               | KB | PR |                                                                                                                                            |
| A.5<br><br>Kebijakan Keamanan Informasi        | A.5.1. Arahan pihak manajemen terhadap keamanan informasi |                  |                                   |    |    |                                                                                                                                            |
|                                                | A.5.1.1. Kebijakan keamanan informasi                     | Ya               |                                   |    | ✓  | <ul style="list-style-type: none"><li>• Direktur DPTSI-ITS (Bapak Febriliyan).</li><li>• Kasubdit Infrastruktur (Bapak Royyana).</li></ul> |
|                                                | A.5.1.2. Peninjauan kebijakan keamanan informasi          | Tidak            |                                   | ✓  |    | <ul style="list-style-type: none"><li>• Kasubdit Pelayanan (Ibu Hanim).</li><li>• Kasubdit Pengembangan (Ibu Anny).</li></ul>              |
| A.6<br><br>Organisasi untuk keamanan informasi | A.6.1. Organisasi internal                                |                  |                                   |    |    |                                                                                                                                            |
|                                                | A.6.1.1. Peran dan tanggung jawab keamanan informasi      | Ya               |                                   | ✓  |    | <ul style="list-style-type: none"><li>• Rektor ITS.</li><li>• Direktur DPTSI-ITS (Bapak Febriliyan).</li></ul>                             |

|                                                             |                                                       |       |  |  |  |  |
|-------------------------------------------------------------|-------------------------------------------------------|-------|--|--|--|--|
| A.6<br>Organisasi untuk<br>keamanan<br>informasi<br>(lanj.) | A.6.1.2. Pembagian tugas                              | Ya    |  |  |  |  |
|                                                             | A.6.1.3. Menghubungi organisasi/pemerintah            | Ya    |  |  |  |  |
|                                                             | A.6.1.4. Menghubungi kelompok dengan minat tertentu   | Tidak |  |  |  |  |
|                                                             | A.6.1.5. Manajemen proyek untuk keamanan informasi    | Ya    |  |  |  |  |
|                                                             | A.6.2. Perangkat <i>mobile</i> dan <i>teleworking</i> |       |  |  |  |  |
|                                                             | A.6.2.1. Kebijakan perangkat <i>mobile</i>            | Tidak |  |  |  |  |
|                                                             | A.6.2.2. <i>Teleworking</i>                           | Tidak |  |  |  |  |
| A.7<br>Keamanan<br>Sumber Daya<br>Manusia                   | A.7.1. Sebelum perekrutan karyawan                    |       |  |  |  |  |
|                                                             | A.7.1.1. Penyaringan karyawan                         | Ya    |  |  |  |  |
|                                                             | A.7.1.2. Syarat dan ketentuan dalam pekerjaan         | Ya    |  |  |  |  |
|                                                             | A.7.2. Selama karyawan bekerja                        |       |  |  |  |  |
|                                                             | A.7.2.1. Tanggung jawab manajemen                     | Ya    |  |  |  |  |

|                                                      |                                                                 |       |  |  |   |                                                                                |
|------------------------------------------------------|-----------------------------------------------------------------|-------|--|--|---|--------------------------------------------------------------------------------|
| A.7<br>Keamanan<br>Sumber Daya<br>Manusia<br>(lanj.) | A.7.2.2. Kesadaran, pendidikan dan pelatihan keamanan informasi | Ya    |  |  | ✓ | • Kasubdit Pelayanan (Ibu Hanim).                                              |
|                                                      | A.7.2.3. Proses pendisiplinan                                   | Ya    |  |  |   |                                                                                |
|                                                      | A.7.3. Pemberhentian dan penggantian karyawan                   |       |  |  |   |                                                                                |
|                                                      | A.7.3.1. Tanggung jawab pemberhentian dan penggantian karyawan  | Tidak |  |  |   |                                                                                |
| A.8<br>Manajemen Aset                                | A.8.1. Tanggung jawab terhadap aset                             |       |  |  |   |                                                                                |
|                                                      | A.8.1.1. Inventaris aset                                        | Ya    |  |  | ✓ | • Kasubdit Infrastruktur (Bapak Royyana).<br>• Kasubdit Pelayanan (Ibu Hanim). |
|                                                      | A.8.1.2. Kepemilikan aset                                       | Ya    |  |  | ✓ | • Kasubdit Pengembangan (Ibu Anny).                                            |
|                                                      | A.8.1.3. Persyaratan penggunaan aset                            | Ya    |  |  |   |                                                                                |
|                                                      | A.8.1.4. Pengembalian aset                                      | Ya    |  |  | ✓ | • Subdit Pengembangan (Ibu Lestari).                                           |
|                                                      | A.8.2. Klasifikasi informasi                                    |       |  |  |   |                                                                                |

|                                  |                                                |       |  |  |   |                                                                                                                                                                                                                                       |
|----------------------------------|------------------------------------------------|-------|--|--|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.8<br>Manajemen Aset<br>(lanj.) | A.8.2.1. Klasifikasi informasi                 | Ya    |  |  | ✓ | <ul style="list-style-type: none"> <li>• Direktur DPTSI-ITS (Bapak Febriliyan).</li> <li>• Kasubdit Infrastruktur (Bapak Royyana).</li> <li>• Kasubdit Pelayanan (Ibu Hanim).</li> <li>• Kasubdit Pengembangan (Ibu Anny).</li> </ul> |
|                                  | A.8.2.2. Pemberian <i>label</i> informasi      | Tidak |  |  |   |                                                                                                                                                                                                                                       |
|                                  | A.8.2.3. Penanganan aset                       | Ya    |  |  |   |                                                                                                                                                                                                                                       |
|                                  | A.8.3. Penanganan media                        |       |  |  |   |                                                                                                                                                                                                                                       |
|                                  | A.8.3.1. Manajemen <i>removable media</i>      | Tidak |  |  |   |                                                                                                                                                                                                                                       |
|                                  | A.8.3.2. Pembuangan media                      | Ya    |  |  |   |                                                                                                                                                                                                                                       |
|                                  | A.8.3.3. Pengiriman media fisik                | Tidak |  |  |   |                                                                                                                                                                                                                                       |
| A.9<br>Kontrol Akses             | A.9.1. Kebutuhan bisnis terhadap kontrol akses |       |  |  |   |                                                                                                                                                                                                                                       |
|                                  | A.9.1.1. Kebijakan kontrol akses               | Ya    |  |  |   |                                                                                                                                                                                                                                       |

|                                 |                                                                |    |  |  |   |                                                                                                                                        |
|---------------------------------|----------------------------------------------------------------|----|--|--|---|----------------------------------------------------------------------------------------------------------------------------------------|
| A.9<br>Kontrol Akses<br>(lanj.) | A.9.1.2. Akses ke jaringan dan layanan jaringan                | Ya |  |  |   |                                                                                                                                        |
|                                 | A.9.2. Manajemen akses pengguna                                |    |  |  |   |                                                                                                                                        |
|                                 | A.9.2.1. Pendaftaran dan penghapusan pengguna                  | Ya |  |  |   |                                                                                                                                        |
|                                 | A.9.2.2. Penyediaan akses pengguna                             | Ya |  |  | ✓ | <ul style="list-style-type: none"> <li>• Subdit Infrastruktur (Bapak Wicaksono).</li> <li>• Subdit Pelayanan (Bapak Rizky).</li> </ul> |
|                                 | A.9.2.3. Manajemen hak akses <i>administrator</i>              | Ya |  |  | ✓ |                                                                                                                                        |
|                                 | A.9.2.4. Manajemen informasi autentikasi rahasia dari pengguna | Ya |  |  | ✓ |                                                                                                                                        |
|                                 | A.9.2.5. Meninjau hak akses pengguna                           | Ya |  |  | ✓ |                                                                                                                                        |
|                                 | A.9.2.6. Penghapusan atau penyesuaian hak akses                | Ya |  |  |   |                                                                                                                                        |
|                                 | A.9.3. Tanggung jawab pengguna                                 |    |  |  |   |                                                                                                                                        |
|                                 | A.9.3.1. Penggunaan informasi autentikasi rahasia              | Ya |  |  |   |                                                                                                                                        |
|                                 | A.9.4. Kontrol akses sistem dan aplikasi                       |    |  |  |   |                                                                                                                                        |
|                                 | A.9.4.1. Pembatasan akses informasi                            | Ya |  |  |   |                                                                                                                                        |
|                                 | A.9.4.2. Prosedur <i>login</i> yang aman                       | Ya |  |  |   |                                                                                                                                        |

|                                          |                                                              |       |  |  |   |                                                                                                                                      |
|------------------------------------------|--------------------------------------------------------------|-------|--|--|---|--------------------------------------------------------------------------------------------------------------------------------------|
| A.9<br>Kontrol Akses<br>(lanj.)          | A.9.4.3. Sistem manajemen <i>password</i>                    | Ya    |  |  | ✓ | <ul style="list-style-type: none"> <li>• Subdit Infrastruktur (Bapak Jananta).</li> <li>• Subdit Pelayanan (Bapak Rizky).</li> </ul> |
|                                          | A.9.4.4. Penggunaan aplikasi utilitas yang diizinkan         | Tidak |  |  |   |                                                                                                                                      |
|                                          | A.9.4.5. Kontrol akses ke <i>source code</i> perangkat lunak | Ya    |  |  |   |                                                                                                                                      |
| A.10<br>Kriptografi                      | A.10.1. Kontrol kriptografi                                  |       |  |  |   |                                                                                                                                      |
|                                          | A.10.1.1. Kebijakan dalam penggunaan kontrol kriptografi     | Ya    |  |  |   |                                                                                                                                      |
|                                          | A.10.1.2. Manajemen kunci                                    | Tidak |  |  |   |                                                                                                                                      |
| A.11<br>Keamanan Fisik<br>dan Lingkungan | A.11.1. Area aman                                            |       |  |  |   |                                                                                                                                      |
|                                          | A.11.1.1. Perlindungan keamanan fisik                        | Ya    |  |  |   |                                                                                                                                      |
|                                          | A.11.1.2. Kontrol keluar-masuk fisik                         | Ya    |  |  |   |                                                                                                                                      |
|                                          | A.11.1.3. Pengamanan kantor, ruangan dan fasilitas           | Ya    |  |  |   |                                                                                                                                      |

|                                                     |                                                              |       |  |  |   |                                                                                      |
|-----------------------------------------------------|--------------------------------------------------------------|-------|--|--|---|--------------------------------------------------------------------------------------|
| A.11<br>Keamanan Fisik<br>dan Lingkungan<br>(lanj.) | A.11.1.4. Perlindungan dari ancaman eksternal dan lingkungan | Ya    |  |  |   |                                                                                      |
|                                                     | A.11.1.5. Bekerja di area yang aman                          | Ya    |  |  |   |                                                                                      |
|                                                     | A.11.1.6. Area pengiriman dan bongkar-muat                   | Tidak |  |  |   |                                                                                      |
|                                                     | A.11.2. Peralatan                                            |       |  |  |   |                                                                                      |
|                                                     | A.11.2.1. Penempatan dan perlindungan peralatan              | Ya    |  |  |   |                                                                                      |
|                                                     | A.11.2.2. Utilitas pendukung                                 | Ya    |  |  | ✓ | • Kasubdit Infrastruktur (Bapak Royyana).                                            |
|                                                     | A.11.2.3. Keamanan pemasangan kabel                          | Ya    |  |  | ✓ | • Subdit Infrastruktur (Bapak Achmad Bustari).<br>• Direktorat Sarana dan Prasarana. |
|                                                     | A.11.2.4. Pemeliharaan perlengkapan                          | Ya    |  |  | ✓ | • Subdit Infrastruktur (Bapak Wicaksono).<br>• Subdit Pelayanan (Bapak Rizky).       |
|                                                     | A.11.2.5. Pemindahan aset                                    | Ya    |  |  |   |                                                                                      |

|                                                     |                                                                    |       |  |  |   |                                                                                                                                                                                     |
|-----------------------------------------------------|--------------------------------------------------------------------|-------|--|--|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A.11<br>Keamanan Fisik<br>dan Lingkungan<br>(lanj.) | A.11.2.6. Keamanan peralatan dan aset yang dibawa keluar           | Tidak |  |  |   |                                                                                                                                                                                     |
|                                                     | A.11.2.7. Pembuangan atau penggunaan kembali peralatan secara aman | Ya    |  |  |   |                                                                                                                                                                                     |
|                                                     | A.11.2.8. Peralatan pengguna yang tidak diawasi                    | Ya    |  |  | ✓ | • Subdit Pelayanan (Bapak Rizky).                                                                                                                                                   |
|                                                     | A.11.2.9. Kebijakan merapihkan meja dan membersihkan layar         | Tidak |  |  | ✓ | • Kasubdit Pelayanan (Ibu Hanim).                                                                                                                                                   |
| A.12<br>Keamanan<br>Operasional                     | A.12.1. Prosedur operasional dan tanggung jawab                    |       |  |  |   |                                                                                                                                                                                     |
|                                                     | A.12.1.1. Mendokumentasikan prosedur operasional                   | Ya    |  |  | ✓ | <ul style="list-style-type: none"> <li>• Kasubdit Infrastruktur (Bapak Royyana).</li> <li>• Kasubdit Pelayanan (Ibu Hanim).</li> <li>• Kasubdit Pengembangan (Ibu Anny).</li> </ul> |
|                                                     | A.12.1.2. Manajemen perubahan                                      | Ya    |  |  | ✓ | • Kasubdit Pelayanan (Ibu Hanim).                                                                                                                                                   |



|                                            |                                                                        |    |  |  |   |                                                                                                                                       |
|--------------------------------------------|------------------------------------------------------------------------|----|--|--|---|---------------------------------------------------------------------------------------------------------------------------------------|
| A.12<br>Keamanan<br>Operasional<br>(lanj.) | A.12.1.3. Manajemen kapasitas                                          | Ya |  |  | ✓ | <ul style="list-style-type: none"> <li>• Kasubdit Infrastruktur (Bapak Royyana).</li> <li>• Direktorat SDM dan Organisasi.</li> </ul> |
|                                            | A.12.1.4. Pemisahan lingkungan pengembangan, pengujian dan operasional | Ya |  |  |   |                                                                                                                                       |
|                                            | A.12.2. Perlindungan dari <i>malware</i>                               |    |  |  |   |                                                                                                                                       |
|                                            | A.12.2.1. Kontrol terhadap <i>malware</i>                              | Ya |  |  | ✓ | <ul style="list-style-type: none"> <li>• Subdit Infrastruktur (Bapak Jananta).</li> <li>• Subdit Pelayanan (Bapak Rizky).</li> </ul>  |
|                                            | A.12.3. <i>Backup</i>                                                  |    |  |  |   |                                                                                                                                       |
|                                            | A.12.3.1. <i>Backup</i> informasi                                      | Ya |  |  | ✓ | <ul style="list-style-type: none"> <li>• Subdit Infrastruktur (Bapak Wicaksono).</li> </ul>                                           |
|                                            | A.12.4. Perekaman dan pengawasan                                       |    |  |  |   |                                                                                                                                       |
|                                            | A.12.4.1. Mencatat kejadian                                            | Ya |  |  |   |                                                                                                                                       |
|                                            | A.12.4.2. Perlindungan informasi <i>log</i>                            | Ya |  |  |   |                                                                                                                                       |

|                                            |                                                          |       |  |  |   |                                                                                                                                        |
|--------------------------------------------|----------------------------------------------------------|-------|--|--|---|----------------------------------------------------------------------------------------------------------------------------------------|
| A.12<br>Keamanan<br>Operasional<br>(lanj.) | A.12.4.3. <i>Log administrator</i> dan petugas           | Tidak |  |  |   |                                                                                                                                        |
|                                            | A.12.4.4. Sinkronisasi jam                               | Ya    |  |  |   |                                                                                                                                        |
|                                            | A.12.5. Kontrol perangkat lunak operasional              |       |  |  |   |                                                                                                                                        |
|                                            | A.12.5.1. Pemasangan perangkat lunak pada sistem operasi | Ya    |  |  | ✓ | <ul style="list-style-type: none"> <li>• Subdit Infrastruktur (Bapak Jananta).</li> <li>• Subdit Pelayanan (Bapak Rizky).</li> </ul>   |
|                                            | A.12.6. Manajemen kerentanan teknis                      |       |  |  |   |                                                                                                                                        |
|                                            | A.12.6.1. Manajemen kerentanan teknis                    | Ya    |  |  | ✓ | <ul style="list-style-type: none"> <li>• Subdit Infrastruktur (Bapak Jananta).</li> <li>• Subdit Pelayanan (Bapak Rizky).</li> </ul>   |
|                                            | A.12.6.2. Pembatasan pemasangan perangkat lunak          | Tidak |  |  | ✓ | <ul style="list-style-type: none"> <li>• Kasubdit Infrastruktur (Bapak Royyana).</li> <li>• Kasubdit Pelayanan (Ibu Hanim).</li> </ul> |
|                                            | A.12.7. Pertimbangan audit sistem informasi              |       |  |  |   |                                                                                                                                        |

|                                            |                                                                   |       |  |  |   |                                           |
|--------------------------------------------|-------------------------------------------------------------------|-------|--|--|---|-------------------------------------------|
| A.12<br>Keamanan<br>Operasional<br>(lanj.) | A.12.7.1. Kontrol audit sistem informasi                          | Tidak |  |  |   |                                           |
| A.13<br>Keamanan<br>Komunikasi             | A.13.1. Manajemen keamanan jaringan                               |       |  |  |   |                                           |
|                                            | A.13.1.1. Kontrol jaringan                                        | Ya    |  |  | ✓ | • Subdit Infrastruktur (Bapak Wicaksono). |
|                                            | A.13.1.2. Keamanan layanan jaringan                               | Ya    |  |  |   |                                           |
|                                            | A.13.1.3. Pemisahan pada jaringan                                 | Ya    |  |  |   |                                           |
|                                            | A.13.2. Pertukaran informasi                                      |       |  |  |   |                                           |
|                                            | A.13.2.1. Kebijakan dan prosedur pertukaran informasi             | Ya    |  |  |   |                                           |
|                                            | A.13.2.2. Perjanjian dalam pertukaran informasi                   | Tidak |  |  |   |                                           |
|                                            | A.13.2.3. Pesan elektronik                                        | Ya    |  |  |   |                                           |
|                                            | A.13.2.4. Perjanjian kerahasiaan atau tidak menyebarkan informasi | Ya    |  |  |   |                                           |

|                                                             |                                                                           |       |  |  |   |                                                                                                                                      |
|-------------------------------------------------------------|---------------------------------------------------------------------------|-------|--|--|---|--------------------------------------------------------------------------------------------------------------------------------------|
| A.14<br>Akusisi,<br>Pengembangan,<br>Pemeliharaan<br>Sistem | A.14.1. Persyaratan keamanan pada sistem informasi                        |       |  |  |   |                                                                                                                                      |
|                                                             | A.14.1.1. Analisa dan spesifikasi kebutuhan keamanan informasi            | Ya    |  |  |   |                                                                                                                                      |
|                                                             | A.14.1.2. Pengamanan layanan aplikasi di jaringan publik                  | Tidak |  |  |   |                                                                                                                                      |
|                                                             | A.14.1.3. Melindungi layanan transaksi aplikasi                           | Tidak |  |  |   |                                                                                                                                      |
|                                                             | A.14.2. Keamanan dalam proses pengembangan dan dukungan                   |       |  |  |   |                                                                                                                                      |
|                                                             | A.14.2.1. Kebijakan pengembangan yang aman                                | Ya    |  |  |   |                                                                                                                                      |
|                                                             | A.14.2.2. Prosedur kontrol perubahan sistem                               | Ya    |  |  |   |                                                                                                                                      |
|                                                             | A.14.2.3. Tinjauan teknis pada aplikasi setelah dilakukan perubahan dasar | Ya    |  |  |   |                                                                                                                                      |
|                                                             | A.14.2.4. Pembatasan pada perubahan paket perangkat lunak                 | Tidak |  |  | ✓ | <ul style="list-style-type: none"> <li>• Subdit Infrastruktur (Bapak Jananta).</li> <li>• Subdit Pelayanan (Bapak Rizky).</li> </ul> |
|                                                             | A.14.2.5. Prinsip keahlian teknis yang aman                               | Tidak |  |  | ✓ | <ul style="list-style-type: none"> <li>• Subdit Pengembangan (Ibu Lestari).</li> </ul>                                               |

|                                                                        |                                                                     |       |  |  |  |  |
|------------------------------------------------------------------------|---------------------------------------------------------------------|-------|--|--|--|--|
| A.14<br>Akusisi,<br>Pengembangan,<br>Pemeliharaan<br>Sistem<br>(lanj.) | A.14.2.6. Lingkungan pengembangan yang aman                         | Ya    |  |  |  |  |
|                                                                        | A.14.2.7. Pengembangan oleh pihak ketiga                            | Tidak |  |  |  |  |
|                                                                        | A.14.2.8. Pengujian keamanan sistem                                 | Ya    |  |  |  |  |
|                                                                        | A.14.2.9. Pengujian penerimaan sistem                               | Ya    |  |  |  |  |
|                                                                        | A.14.3. Pengujian data                                              |       |  |  |  |  |
|                                                                        | A.14.3.1. Perlindungan data pengujian                               | Tidak |  |  |  |  |
| A.15<br>Relasi dengan<br>Vendor                                        | A.15.1. Keamanan informasi dalam hubungan dengan vendor             |       |  |  |  |  |
|                                                                        | A.15.1.1. Kebijakan keamanan informasi untuk hubungan dengan vendor | Ya    |  |  |  |  |
|                                                                        | A.15.1.2. Merujuk keamanan dengan perjanjian vendor                 | Ya    |  |  |  |  |
|                                                                        | A.15.1.3. Rantai pasok teknologi informasi dan komunikasi           | Tidak |  |  |  |  |
|                                                                        | A.15.2. Manajemen kualitas layanan vendor                           |       |  |  |  |  |

|                                                       |                                                                    |       |  |  |  |  |
|-------------------------------------------------------|--------------------------------------------------------------------|-------|--|--|--|--|
| A.15<br>Relasi dengan<br>Vendor<br>(lanj.)            | A.15.2.1. Mengawasi dan meninjau layanan vendor                    | Ya    |  |  |  |  |
|                                                       | A.15.2.2. Mengatur perubahan pada layanan vendor                   | Ya    |  |  |  |  |
| A.16<br>Manajemen<br>Insiden<br>Keamanan<br>Informasi | A.16.1. Manajemen insiden keamanan informasi dan peningkatannya    |       |  |  |  |  |
|                                                       | A.16.1.1. Tanggung jawab dan prosedur                              | Ya    |  |  |  |  |
|                                                       | A.16.1.2. Pelaporan insiden keamanan informasi                     | Ya    |  |  |  |  |
|                                                       | A.16.1.3. Pelaporan kelemahan keamanan informasi                   | Tidak |  |  |  |  |
|                                                       | A.16.1.4. Penilaian dan keputusan dalam insiden keamanan informasi | Ya    |  |  |  |  |
|                                                       | A.16.1.5. Menanggapi insiden keamanan informasi                    | Ya    |  |  |  |  |
|                                                       | A.16.1.6. Pembelajaran dari insiden keamanan informasi             | Ya    |  |  |  |  |
|                                                       | A.16.1.7. Pengumpulan bukti                                        | Ya    |  |  |  |  |

|                                                                                       |                                                                                       |       |  |  |   |                                       |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|-------|--|--|---|---------------------------------------|
| A.17<br>Aspek<br>Keamanan<br>Informasi akan<br>Manajemen<br>Keberlangsungan<br>Bisnis | A.17.1. Keberlangsungan keamanan informasi                                            |       |  |  |   |                                       |
|                                                                                       | A.17.1.1. Merencanakan keberlangsungan keamanan informasi                             | Ya    |  |  |   |                                       |
|                                                                                       | A.17.1.2. Menerapkan keberlangsungan keamanan informasi                               | Tidak |  |  |   |                                       |
|                                                                                       | A.17.1.3. Memverifikasi, meninjau dan mengevaluasi keberlangsungan keamanan informasi | Tidak |  |  |   |                                       |
|                                                                                       | A.17.2. Redundansi                                                                    |       |  |  |   |                                       |
|                                                                                       | A.17.2.1. Ketersediaan dari fasilitas pemrosesan informasi                            | Ya    |  |  | ✓ | • Subdit Infrastruktur (Bapak Cahya). |
| A.18<br>Kepatuhan                                                                     | A.18.1. Kepatuhan akan persyaratan hukum dan kontrak                                  |       |  |  |   |                                       |
|                                                                                       | A.18.1.1. Identifikasi kebutuhan undang-undang dan kontrak yang dapat digunakan       | Ya    |  |  |   |                                       |
|                                                                                       | A.18.1.2. Hak kekayaan intelektual                                                    | Ya    |  |  |   |                                       |
|                                                                                       | A.18.1.3. Perlindungan untuk rekaman                                                  | Tidak |  |  |   |                                       |

|                              |                                                                |       |  |  |  |  |
|------------------------------|----------------------------------------------------------------|-------|--|--|--|--|
| A.18<br>Kepatuhan<br>(lanj.) | A.18.1.4. Kerahasiaan dan perlindungan untuk informasi pribadi | Tidak |  |  |  |  |
|                              | A.18.1.5. Peraturan untuk kontrol kriptografi                  | Tidak |  |  |  |  |



#### **4. Kebijakan/Dokumen Terkait**

Kebijakan atau dokumen yang terkait dengan dokumen ini adalah sebagai berikut:

1. Laporan [Proses Penanganan Resiko] dapat dilihat pada Lampiran I.
2. Dokumen [Sasaran Keamanan Informasi] dapat dilihat pada Lampiran L.
3. Dokumen standar SNI ISO/IEC 27001:2013.

Direktorat Pengembangan Teknologi Sistem Informasi ITS

## SASARAN KEAMANAN INFORMASI

|                |                                    |
|----------------|------------------------------------|
| Nama Dokumen   | Dokumen Sasaran Keamanan Informasi |
| Versi          | 1                                  |
| Tanggal        | 28/10/2017                         |
| Dibuat oleh    | Furqon Mauladani                   |
| Disetujui oleh |                                    |

### 1. Pendahuluan

Tujuan dari dokumen ini adalah menjelaskan setiap sasaran dari kontrol keamanan yang sudah diterapkan maupun yang akan diterapkan sebagai patokan untuk mengukur efektivitas penerapan SMKTI pada periode yang ditetapkan. Sasaran keamanan informasi dapat ditetapkan sesuai hasil manajemen resiko keamanan informasi dan prioritas penanganan resiko dengan mempertimbangkan ketersediaan dan kemampuan sumber daya.

### 2. Ruang Lingkup

Dokumen ini mencakup keseluruhan kontrol keamanan yang sudah diterapkan maupun yang direncanakan untuk diterapkan pada dokumen [*Statement of Applicability*].

### 3. Dokumen Sasaran Keamanan Informasi

Hasil dari pembuatan dokumen Sasaran Keamanan Informasi dapat dilihat pada halaman dibawah ini.

Tabel L.1 Sasaran Keamanan Informasi

| No Annex | Kontrol Keamanan                            | Sasaran                                                                             | Metode Pengukuran                                                                                                                                                                                                                                               | Frekuensi Pengukuran |
|----------|---------------------------------------------|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| A.5.1.1  | Kebijakan keamanan informasi                | Semua kebijakan tersedia dan disosialisasikan keseluruh pihak yang terkait.         | <ul style="list-style-type: none"> <li>Jumlah dokumen kebijakan yang sudah dibuat <b>dibagi</b> jumlah dokumen kebijakan yang direncanakan.</li> <li>Jumlah karyawan yang telah mengikuti sosialisasi kebijakan <b>dibagi</b> jumlah total karyawan.</li> </ul> | Per 1 tahun          |
| A.5.1.2  | Peninjauan kebijakan keamanan informasi     | Semua kebijakan yang ada ditinjau secara berkala.                                   | Jumlah kebijakan yang telah ditinjau <b>dibagi</b> jumlah total kebijakan.                                                                                                                                                                                      | Per 1 tahun          |
| A.6.1.1  | Peran dan tanggung jawab keamanan informasi | Semua peran dan tanggung jawab diterapkan dan dilaksanakan oleh pihak yang terkait. | Periksa SKP karyawan yang diberikan peran dan tanggung jawab keamanan informasi.                                                                                                                                                                                | Per 1 tahun          |

|         |                                                         |                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                         |             |
|---------|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| A.7.2.2 | Kepedulian, pendidikan dan pelatihan keamanan informasi | <ul style="list-style-type: none"> <li>• Semua dosen, mahasiswa dan karyawan di ITS, sudah mengikuti program kesadaran keamanan.</li> <li>• 30% karyawan DPTSI-ITS sudah mengikuti pelatihan kerja sesuai pekerjaannya.</li> </ul> | <ul style="list-style-type: none"> <li>• Jumlah dosen, mahasiswa dan karyawan yang telah mengikuti program kesadaran keamanan <b>dibagi</b> jumlah total dosen, mahasiswa dan karyawan.</li> <li>• Jumlah karyawan yang telah mengikuti pelatihan kerja <b>dibagi</b> jumlah total karyawan.</li> </ul> | Per 6 bulan |
| A.8.1.1 | Inventaris aset                                         | Semua aset informasi disetiap Subdit sudah didokumentasikan.                                                                                                                                                                       | Jumlah aset masing-masing Subdit yang telah didokumentasikan <b>dibagi</b> jumlah total aset yang dimiliki oleh masing-masing Subdit.                                                                                                                                                                   | Per 6 bulan |
| A.8.1.2 | Kepemilikan aset                                        | Semua aset informasi disetiap Subdit sudah didokumentasikan siapa pemilik asetnya.                                                                                                                                                 | Jumlah aset masing-masing Subdit yang telah didokumentasikan pemilik asetnya <b>dibagi</b> jumlah total aset yang dimiliki oleh masing-masing Subdit.                                                                                                                                                   | Per 1 tahun |
| A.8.1.4 | Pengembalian aset                                       | Setiap karyawan mengisikan 5 ilmu yang dimiliki kedalam sistem <i>knowledge management</i> .                                                                                                                                       | Jumlah ilmu yang ditambahkan kedalam sistem <b>dibagi</b> jumlah total karyawan.                                                                                                                                                                                                                        | Per 3 bulan |
| A.8.2.1 | Klasifikasi informasi                                   | Semua aset bertipe informasi sudah diklasifikasikan berdasarkan bentuk dan kesensitifannya.                                                                                                                                        | Jumlah aset masing-masing Subdit bertipe informasi yang telah diklasifikasikan <b>dibagi</b> jumlah total aset bertipe informasi yang dimiliki oleh masing-masing Subdit.                                                                                                                               | Per 6 bulan |

|         |                                                       |                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                               |
|---------|-------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|
| A.9.2.2 | Penyediaan akses pengguna                             | Semua hak akses diberikan sesuai dengan prosedur.                                                                                                                                   | Jumlah hak ases yang diberikan sesuai prosedur <b>dibagi</b> jumlah semua hak akses yang ada pada semua perangkat.                                                                                                                                                                                                                                                                                                                                            | Per 6 bulan                                                                                                   |
| A.9.2.3 | Manajemen hak akses <i>administrator</i>              | Semua hak akses <i>administrator</i> diatur secara aman, dan semua <i>password (default vendor dan administrator generic)</i> pada perangkat sudah dikelola sesuai dengan prosedur. | <ul style="list-style-type: none"> <li>• Periksa apakah terdapat hak akses <i>administrator</i> yang belum diatur secara aman.</li> <li>• Jumlah perangkat yang sudah diperiksa apakah terdapat <i>password default vendor</i> <b>dibagi</b> jumlah perangkat yang bisa memiliki <i>password default</i> vendor.</li> <li>• Periksa aktifitas pengelolaan <i>password administrator generic</i> yang dilakukan berdasarkan prosedur pada formulir.</li> </ul> | <ul style="list-style-type: none"> <li>• Per 3 bulan</li> <li>• Per 6 bulan</li> <li>• Per 1 tahun</li> </ul> |
| A.9.2.4 | Manajemen informasi autentikasi rahasia dari pengguna | Semua aktifitas <i>reset password</i> dilakukan sesuai dengan prosedur.                                                                                                             | Jumlah aktifitas <i>reset password</i> yang dilakukan berdasarkan prosedur pada formulir <b>dibagi</b> jumlah aktifitas <i>reset password</i> yang dilakukan pada SKP kerja milik karyawan.                                                                                                                                                                                                                                                                   | Per 1 tahun                                                                                                   |
| A.9.2.5 | Meninjau hak akses pengguna                           | Semua hak akses ditinjau secara berkala sesuai dengan prosedur.                                                                                                                     | Periksa semua perangkat yang sudah ditinjau dan yang belum ditinjau berdasarkan hasil peninjauan.                                                                                                                                                                                                                                                                                                                                                             | Per 1 tahun                                                                                                   |

|          |                                  |                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                 |             |
|----------|----------------------------------|---------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| A.9.4.3  | Sistem manajemen <i>password</i> | Semua <i>server</i> , komputer dan laptop dinas sudah diatur sistem manajemen <i>password</i> baru.     | Jumlah sistem yang sudah diatur sistem manajemen <i>password</i> -nya <b>dibagi</b> jumlah semua sistem yang dapat diatur sistem manajemen <i>password</i> -nya.                                                                                                                                                                                                                                                | Per 6 bulan |
| A.11.2.2 | Utilitas pendukung               | Semua layanan <i>ISP</i> sudah terpasang dan beroperasi secara benar.                                   | Periksa aktifitas operasional semua layanan <i>ISP</i> yang aktif.                                                                                                                                                                                                                                                                                                                                              | Per 1 tahun |
| A.11.2.3 | Keamanan pemasangan kabel        | Semua panduan dan perangkat pemasangan kabel tersedia, dan semua patok penanda kabel sudah diremajakan. | <ul style="list-style-type: none"> <li>• Jumlah dokumen panduan yang sudah dibuat <b>dibagi</b> jumlah dokumen panduan yang direncanakan.</li> <li>• Jumlah perangkat pemasangan kabel yang sudah dimiliki <b>dibagi</b> jumlah perangkat pemasangan kabel yang seharusnya dimiliki.</li> <li>• Periksa setiap patok penanda kabel yang terpasang pada semua jalur kabel yang dikubur didalam tanah.</li> </ul> | Per 1 tahun |
| A.11.2.4 | Pemeliharaan perlengkapan        | Semua perangkat sudah dilakukan pemeliharaan perangkat sesuai dengan prosedur.                          | Jumlah aktifitas pemeliharaan perlengkapan yang dilakukan berdasarkan prosedur pada formulir <b>dibagi</b> jumlah aktifitas pemeliharaan perlengkapan yang seharusnya dilakukan berdasarkan jadwal.                                                                                                                                                                                                             | Per 3 bulan |

|          |                                                 |                                                                                                                  |                                                                                                                                                                                                                                                                  |             |
|----------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| A.11.2.8 | Peralatan pengguna yang tidak diawasi           | Semua komputer dan laptop dinas sudah dikonfigurasi agar menggunakan <i>screensaver</i> dengan <i>password</i> . | Jumlah <i>server</i> , komputer dan laptop dinas yang sudah dikonfigurasi <b>dibagi</b> jumlah semua <i>server</i> , komputer dan laptop dinas yang sudah dikonfigurasi.                                                                                         | Per 6 bulan |
| A.11.2.9 | Kebijakan merapikan meja dan membersihkan layar | Menurunkan jumlah kesalahan praktik keamanan informasi didalam kantor dibanding tahun sebelumnya.                | Jumlah aktifitas yang tidak patuh terhadap kebijakan sekarang <b>dibagi</b> jumlah aktifitas yang tidak patuh terhadap kebijakan tahun lalu.                                                                                                                     | Per 6 bulan |
| A.12.1.1 | Mendokumentasikan prosedur operasional          | Semua prosedur tersedia dan disosialisasikan keseluruh karyawan yang terkait.                                    | <ul style="list-style-type: none"> <li>• Jumlah dokumen prosedur yang sudah dibuat <b>dibagi</b> jumlah dokumen prosedur yang direncanakan.</li> <li>• Jumlah karyawan yang telah mengikuti sosialisasi prosedur <b>dibagi</b> jumlah total karyawan.</li> </ul> | Per 1 tahun |
| A.12.1.2 | Manajemen perubahan                             | Semua perubahan dilakukan sesuai dengan prosedur.                                                                | Jumlah aktifitas perubahan yang dilakukan berdasarkan prosedur pada formulir <b>dibagi</b> jumlah aktifitas perubahan yang dilakukan pada SKP kerja milik karyawan.                                                                                              | Per 6 bulan |

|          |                                                |                                                                                                                                                                          |                                                                                                                                                                                                                                |             |
|----------|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| A.12.1.3 | Manajemen kapasitas                            | Menurunkan insiden kegagalan akibat melebihi kapasitas sebanyak 50% dibanding tahun lalu, dan mengurangi level resiko pada resiko absensi karyawan dibanding sebelumnya. | <ul style="list-style-type: none"> <li>Persentasi jumlah insiden tahun lalu <b>dikurangi</b> persentasi jumlah insiden sekarang.</li> <li>Perbandingan laporan hasil pengelolaan resiko sebelumnya dengan sekarang.</li> </ul> | Per 1 tahun |
| A.12.2.1 | Kontrol terhadap <i>malware</i>                | Menurunkan jumlah insiden <i>malware</i> sebanyak 50% dibanding tahun sebelumnya.                                                                                        | Persentasi jumlah insiden tahun lalu <b>dikurangi</b> persentasi jumlah insiden sekarang.                                                                                                                                      | Per 3 bulan |
| A.12.3.1 | <i>Backup</i> informasi                        | Semua aktifitas <i>backup</i> dilakukan sesuai dengan prosedur dan kebijakan yang ada.                                                                                   | Jumlah aktifitas <i>backup</i> yang dilakukan berdasarkan prosedur pada formulir <b>dibagi</b> jumlah aktifitas <i>backup</i> yang seharusnya dilakukan berdasarkan jadwal.                                                    | Per 6 bulan |
| A.12.5.1 | Pemasangan perangkat lunak pada sistem operasi | Semua pemasangan perangkat lunak dilakukan sesuai dengan prosedur.                                                                                                       | Jumlah aktifitas pemasangan perangkat lunak yang dilakukan berdasarkan prosedur pada formulir <b>dibagi</b> jumlah perangkat lunak yang terpasang di perangkat keras.                                                          | Per 1 tahun |
| A.12.6.1 | Manajemen kerentanan teknis                    | Versi perangkat lunak yang sudah diklasifikasikan harus sama dengan versi rilis terbaru.                                                                                 | Periksa dan bandingkan versi perangkat lunak dengan versi terbaru.                                                                                                                                                             | Per 6 bulan |



|          |                                                  |                                                                                                                 |                                                                                                                                                                                                            |             |
|----------|--------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| A.12.6.2 | Pembatasan pemasangan perangkat lunak            | Semua perangkat lunak yang dilarang tidak terpasang didalam sistem.                                             | Periksa perangkat lunak apa saja yang terpasang pada sistem.                                                                                                                                               | Per 6 bulan |
| A.13.1.1 | Kontrol jaringan                                 | Fitur baru terpasang pada perangkat secara benar.                                                               | Periksa fitur yang seharusnya dipasang pada perangkat.                                                                                                                                                     | Per 6 bulan |
| A.14.2.4 | Pembatasan pada perubahan paket perangkat lunak  | Semua modifikasi paket instalasi perangkat lunak dilakukan sesuai dengan prosedur.                              | Jumlah aktifitas modifikasi paket perangkat lunak yang dilakukan berdasarkan prosedur pada formulir <b>dibagi</b> jumlah perangkat lunak yang dilakukan modifikasi pada paketnya.                          | Per 6 bulan |
| A.14.2.5 | Prinsip keahlian teknis yang aman                | Semua pengembangan SIM baru atau pembaharuan sudah mengikuti penggunaan standar teknis dan <i>source code</i> . | Jumlah SIM baru/pembaharuan yang mengikuti standar teknis dan <i>source code</i> <b>dibagi</b> jumlah total SIM baru/pembaharuan yang dibangun oleh Subdit Pengembangan.                                   | Per 1 tahun |
| A.17.2.1 | Ketersediaan dari fasilitas pemrosesan informasi | Setiap perangkat keras atau jaringan sudah memiliki cadangan dan komponennya.                                   | Jumlah perangkat keras/jaringan yang sudah memiliki cadangan dan komponennya sesuai definisi <b>dibagi</b> jumlah total perangkat keras/jaringan yang sedang beroperasi, kritis dan melewati umur garansi. | Per 6 bulan |

#### **4. Kebijakan/Dokumen Terkait**

Kebijakan atau dokumen yang terkait dengan dokumen ini adalah sebagai berikut:

1. Dokumen [*Statement of Applicability*] dapat dilihat pada Lampiran K.