ITS
Institut
Teknologi
Sepuluh Nopember

TUGAS AKHIR - CF 1380

PEMBUATAN KEBIJAKAN KEAMANAN INFORMASI BERDASARKAN ANALISIS RISIKO MENGGUNAKAN METODE OCTAVE DI FAKULTAS TEKNOLOGI INFORMASI (FTIF) INSTITUT TEKNOLOGI SEPULUH NOPEMBER

RACHMAWATI FINDIANA
NRP 5205 100 077

Dosen Pembimbing
Ir. Aris Tjahyanto, M.Kom

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2009

FINAL PROJECT - CF 1380

DESIGNING OF INFORMATION SECURITY POLICY BASED ON RISK ANALYSIS USING THE OCTAVE METHOD IN INFORMATION TECHNOLOGI FACULTY OF INSTITUT TECHNOLOGI SEPULUH NOPEMBER

RACHMAWATI FINDIANA
NRP 5205 100 077

Dosen Pembimbing
Ir. Aris Tjahyanto, M.Kom

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2009

PEMBUATAN KEBIJAKAN KEAMANAN INFORMASI BERDASARKAN ANALISIS RISIKO MENGGUNAKAN METODE OCTAVE DI FAKULTAS TEKNOLOGI INFORMASI ISNTITUT TEKNOLOGI SEPULUH NOPEMBER

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya

Oleh :

RACHMAWATI FINDIANA
NRP 5205 100 077

Surabaya, Juli 2009

KETUA
JURUSAN SISTEM INFORMASI

Ir. A. HOLIL NOOR ALI M.KOM
NIP 131 996 150

PEMBUATAN KEBIJAKAN KEAMANAN INFORMASI BERDASARKAN ANALISIS RISIKO MENGGUNAKAN METODE OCTAVE DI FAKULTAS TEKNOLOGI INFORMASI ISNTITUT TEKNOLOGI SEPULUH NOPEMBER

TUGAS AKHIR

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya

Oleh :

RACHMAWATI FINDIANA
NRP 5205 100 077

Disetujui Tim Penguji: Tanggal Ujian : 21 Juli 2009
Periode Wisuda : Oktober 2009

Ir. Aris Tjahyanto, M.Kom **(Pembimbing)**

Bekti Cahyo Hidayanto, S.Si., M.Kom **(Penguji 1)**

Ahmad Muklason, S.Kom, M.Sc **(Penguji 2)**

PEMBUATAN KEBIJAKAN KEAMANAN INFORMASI BERDASARKAN ANALISIS RISIKO MENGGUNAKAN METODE OCTAVE DI FAKULTAS TEKNOLOGI INFORMASI INSTITUT TEKNOLOGI SEPULUH NOPEMBER

Nama Mahasiswa	: Rachmawati Findiana
NRP	: 5205 100 077
Jurusan	: Sistem Informasi FTIf – ITS
Dosen Pembimbing	: Ir. Aris Tjahyanto, M.Kom

Abstrak

Implementasi teknologi informasi di Fakultas Teknologi Informasi (FTIf) selain memberikan keuntungan juga memunculkan berbagai ancaman resiko. Diantara ancaman resiko tersebut adalah risiko keamanan informasi. Contoh risiko keamanan informasi penyalahgunaan hak akses dan password. Oleh karena itu Tugas Akhir ini berupaya membuat kebijakan keamanan informasi sebagai sarana pengendalian risiko keamanan.

Pembuatan kebijakan keamanan informasi dalam tugas akhir ini dilakukan dengan melakukan analisis risiko. Metode analisis resiko yang digunakan dalam tugas akhir ini adalah metode octave. Tahap terakhir adalah melakukan pemetaan dokumen kebijakan keamanan informasi berdasarkan prinsip-prinsip CIA (confidentiality, integrity, availibility)

Hasil penelitian ini adalah dokumen kebijakan keamanan informasi. Dokumen ini dapat digunakan sebagai pedoman untuk menangani setiap permasalahan keamanan informasi yang terjadi di lingkungan FTIf Institut Teknologi Sepuluh Nopember (ITS).

Kata kunci: keamanan informasi, kebijakan keamanan informasi, analisis risiko, metode octave.

Halaman ini sengaja dikosongkan.

DESIGNING OF INFORMATION SECURITY POLICY BASED ON RISK ANALYSIS USING THE OCTAVE METHOD IN INFORMATION TECHNOLOGI FACULTY OF INSTITUT TECHNOLOGY SEPULUH NOPEMBER

Nama Mahasiswa	: Rachmawati Findiana
NRP	: 5205 100 077
Jurusan	: Sistem Informasi FTIf – ITS
Dosen Pembimbing	: Ir. Aris Tjahyanto, M.Kom

Abstract

The implementation of information technology in information technology faculty of Institut Teknologi Sepuluh Nopember comes with its benefits and risk threat. One of the risk threat is the security risk.The example of security risk is Access and password fraud.. Therefore this final project try to make information security policy as information security control tool.

The information security policy in this final project is designed by with risk analysis. The analysis risk method used in this final project is octave method.. The last phase is mapping information security policy document based on the CIA principles (Confidentiality, integrity and availability).

The outcome of this final project is information security policy document This document can be used as guidelines for handling information security problems occured in the environment of Information Technology Faculty of Institut Teknologi Sepuluh Nopember.

Keywords: information security, information security policy, risk analysis, octave methods.

Halaman ini sengaja dikosongkan.

KATA PENGANTAR

Alhamdulillahirabbilalamiin atas segala rahmat dan karuniaNYA, sehingga tugas akhir berjudul "PEMBUATAN KEBIJAKAN KEAMANAN INFORMASI BERDASARKAN ANALISIS RISIKO MENGGUNAKAN METODE OCTAVE DI FAKULTAS TEKNOLOGI INFORMASI (FTIF) INSTITUT TEKNOLOGI SEPULUH NOPEMBER (ITS) SURABAYA " akhirnya dapat diselesaikan dan menghantarkan penulis menjadi sarjana komputer dari Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember Surabaya. Terima kasih dan penghargaan setinggi-tingginya juga penulis sampaikan kepada:

1. Ibu, Bapak, Kakak dan adikku semua yang tidak pernah bosan memberi aku dorongan dan semangat
2. Bpk. Aris Tjahyanto, M.Kom selaku dosen pembimbing yang telah memberikan bimbingan dan motivasi kepada penulis.
3. Semua teman-temanku diantaranya anas, kaka, amna, tika dan anita atas semua bantuan, motivasi, kerjasama, dan waktu-waktu yang tak akan terlupakan yang telah kalian ciptakan antara kita.
4. Bpk. Ir Ahmad Holil Noor Ali, M.Kom selaku Ketua Jurusan Sistem Informasi ITS
5. Seluruh Bapak dan Ibu Dosen pengajar di Jurusan Sistem Informasi ITS yang telah memberikan ilmu yang berharga kepada penulis.
6. Seluruh staf karyawan Jurusan Sistem Informasi dan karyawan Fakultas Teknologi Informasi atas dukungannya sehingga tugas akhir ini dapat terselesaikan.
7. Semua teman-teman di Sistem Informasi, SI'01 (DISC), SI'02 (NFORS), SI'03 (SHOGUN), SI'05 (PHOENIX),

SI'06, dan SI'07, terima kasih telah menjadi bagian dari SI.

8. Serta semua pihak yang tidak dapat disebutkan satu persatu yang telah ikut membantu baik secara langsung maupun tidak langsung selama penulisan tugas akhir ini.

Penulis sangat menyadari bahwa Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu penulisan mengharapkan komentar, kritik dan saran dari berbagai pihak untuk berbagai kemungkinan pengembangan lebih lanjut.

Akhirnya penulis berharap semoga keberadaan tugas akhir ini bermanfaat bagi ilmu pengetahuan dan berbagai pihak.

Juli 2009

Penulis

DAFTAR ISI

Abstrak ix
Abstract xi
KATA PENGANTAR xiii
DAFTAR ISI xv
DAFTAR GAMBAR xvii
DAFTAR TABEL xviii
DAFTAR DEFINISI DAN ISTILAH xix
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Permasalahan 3
1.3 Batasan 3
1.4 Tujuan 3
1.5 Manfaat 3
1.6 Sistematika Penulisan 4
BAB II TINJAUAN PUSTAKA 7
2.1 Keamanan Informasi 7
2.1.1 Komponen Keamanan Informasi 7
2.1.2 Aspek Keamanan Informasi 8
2.2 Kebijakan Keamanan Informasi 10
2.2.1 Kategori Kebijakan Keamanan Informasi 11
2.2.2 Dasar Formulasi Kebijakan Keamanan Informasi 12
2.3 Analisis Risiko 13
2.3.1 Metode OCTAVE 14
2.3.2 Pengenalan Metode OCTAVE 15
2.3.3 Tipe Ancaman dan Pengukuran Keamanan 16
2.3.4 Langkah-langkah Metode OCTAVE 17
2.3.5 Output OCTAVE 19
2.4 Standar Industri 19
2.5 ISO 17799 20
BAB III METODOLOGI 25
3.1 Tahap Persiapan 25
3.1.1 Studi Literatur 25
3.1.2 Identifikasi Permasalahan 26
3.2 Tahap Pengumpulan Data dan Informasi 26
3.2.1 Wawancara 26
3.2.2 Pengamatan Kembali Dokumen Terkait 27

3.2.3 Observasi 27
3.3 Tahap penilaian (assessment) Risiko 27
3.3.1 Membuat Profil Ancaman berdasarkan Aset 27
3.3.2 Mengidentifikasikan Kerentanan Infrastruktur 28
3.3.3 Membuat Perencanaan dan Strategi Keamanan 28
3.4 Tahap Penyusunan Dokumen Kebijakan Keamanan Informasi 28
3.5 Tahap Pemetaan (Mapping) 28
3.6 Tahap Penyusunan Buku Tugas Akhir, ... 29
BAB IV PEMBUATAN KEBIJAKAN KEAMANAN INFORMASI 31
4.1 Analisis Risiko Metode OCTAVE 31
4.1.1 Deskripsi FTI ITS 31
4.1.2 Membuat Profil Ancaman berbasis Aset 32
4.1.3 Mengidentifikasikan Kerentanan Infrastruktur 42
4.1.3.1 System Of Interest, Access Path, dan Komponen Utama. 43
4.1.3.2 Tools / Pendekatan Evaluasi Kerentanan 45
4.1.3.3 Evaluasi Komponen Pilihan 46
4.1.4 Membuat Perencanaan dan Strategi Keamanan 50
4.1.4.1 Analisis Risiko 50
4.1.4.2 Mengembangkan Strategi Perlindungan 75
4.2 Penyusunan Dokumen Kebijakan Keamanan Informasi 87
4.3 Pemetaan (Mapping) 92
BAB V PENUTUP 101
5.1 Simpulan 101
5.1 Saran 102
DAFTAR PUSTAKA 103
LAMPIRAN A Pengumpulan Data dan Informasi A-1
LAMPIRAN A-1 Struktur Organisasi A-3
LAMPIRAN A-2 Data Inventarisasi FTIf A-9
LAMPIRAN A-3 Hasil Wawancara & Survey A-13
BIODATA PENULIS 104

DAFTAR GAMBAR

Gambar 2.1 Elemen-elemen keamanan informasi [6] 9
Gambar 2.2 Strategi Manajemen Keamanan Informasi [4] 13
Gambar 2.3 Pembagian Ancaman – Kantor Federal untuk Keamanan Teknologi Informasi *(BSI)* [12] 16
Gambar 2.4 Pembagian secara logic pengukuran keamanan pada proses OCTAVE [12] 17
Gambar 2.5 *Pembagian Proses OCTAVE* [12] 18
Gambar 2.6 Struktur dari kesepuluh wilayah standar [14] 23
Gambar 3.1 Metodologi Penelitian 29
Gambar 4.1 Peta Infrastruktur FTIf 47
Gambar 4.2 Skema Dokumen 87

DAFTAR TABEL

Tabel 2.1 Prinsip, Atribut, dan Output Keamanan Informasi [12].....15
Tabel 4.1 Aset kritis 33
Tabel 4.2 Kebutuhan keamanan aset kritis 34
Tabel 4.3 Daftar Ancaman berdasarkan sumbernya 36
Tabel 4.4 Komponen utama untuk aset kritis 43
Tabel 4.5 *Systems of Interest* dan komponen kelas utama.....44
Tabel 4.6 Pendekatan evaluasi kerentanan 46
Tabel 4.7 Sistem yang telah dievaluasi kerentanannya 48
Tabel 4.8 Ringkasan dari evaluasi kerentanan.....48
Tabel 4.9 Tindakan dan Rekomendasi 49
Tabel 4.10 Nilai Probabilitas dan Dampak Risiko.....51
Tabel 4.11 Kriteria Evaluasi untuk Dampak Risiko 61

DAFTAR DEFINISI DAN ISTILAH

Istilah		Keterangan
FTIf	:	Fakultas Teknologi Informasi
ITS	:	Institut Teknologi Sepuluh Nopember
KKI	:	Kebijakan Keamanan Informasi
Aset	:	Aset ádalah sesuatu yang mempunyai nilai pada organisasi
Backup	:	Pembuatan salinan/copy /cadangan
Client	:	Komputer yang memanfaatkan sumber daya dalam jaringan yang disediakan oleh komputer lainnya (Server).
Otorisasi	:	Wewenang yang diberikan kepada user sehubungan dengan hak pemakaian software, pengubahan data-data yang ada dalam software dan penghapusan data-data yang ada dalam software yang bersangkutan.
PC (*Personal computer*)	:	Komputer yang dirancang untuk digunakan oleh satu orang pada waktu tertentu.
Router	:	Perangkat keras yang berfungsi sebagai terminal untuk menghubungkan komputer ke jaringan melalui switch/hub
Server	:	Komputer yang menyediakan sumber daya dan mengendalikan akses di dalam suatu jaringan
Teknologi Informasi	:	Alat atau teknologi untuk mendapatkan dan mengolah informasi yang berhubungan dengan sistem Informasi.

Istilah		Keterangan
User	:	Pemakai / pengguna
Workstation	:	Sebuah komputer personal yang dihubungkan ke jaringan

BAB I
PENDAHULUAN

Bab pendahuluan ini membahas latar belakang pengerjaan tugas akhir, rumusan permasalahan yang dihadapi dalam pengerjaan tugas akhir, batasan permasalahan pengerjaan tugas akhir, tujuan pengerjaan tugas akhir, dan manfaat dari pengerjaan tugas akhir.

1.1 Latar Belakang

"Informasi adalah suatu aset bisnis yang sebagaimana aset bisnis lainnya memiliki nilai esensial dan karenanya harus dilindungi keamanannya" [1]. Perlindugan ini dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan dari investasi dan kesempatan bisnis.

Beragam bentuk informasi yang mungkin dimiliki oleh sebuah perusahaan atau organisasi antara lain informasi yang tersimpan dalam komputer dan atau media penyimpanan lainnya, informasi yang ditransmisikan melalui jaringan dan atau media lain yang serupa, informasi yang dilakukan dalam pembicaraan (termasuk percakapan melalui telepon), dan metode-metode lain yang dapat digunakan untuk menyampaikan informasi dan ide-ide baru organisasi atau perusahaan.

Seiring dengan perkembangan teknologi dan sistem informasi yang semakin pesat, risiko keamanan yang melekat pada informasi juga semakin besar sehingga menyebabkan gangguan pada kelancaran bisnis dalam perusahaan. Berdasarkan hasil survey tahunan yang dilakukan Computer Security Institute bersama dengan FBI sejak tahun 1996 sampai tahun 2008 [2] mengenai keamanan informasi menunjukkan bahwa :

- Kejahatan komputer menyebabkan kerusakan signifikan. Tidak semua organisasi yang korban pelanggaran keamanan oleh komputer mampu mengukur kerugian mereka. Namun, kerugian dari 42% dari responden survei yang bisa total $

265.589.940. Terutama, yang pencurian informasi mengakibatkan tertinggi kerugian keuangan, melanjutkan tren yang meningkat, diikuti oleh penipuan keuangan.

- Kejahatan komputer semakin meningkat. Masalah keamanan informasi tidak terbatas ke Amerika Serikat, dalam kenyataannya, banyak kejahatan yang dilaporkan di CSI / FBI penelitian berasal dari luar Amerika Serikat.
- Gangguan bisnis. Bila terjadi gangguan layanan, Anda perlu staf TI mengatasi masalah dengan segera. Mudah-mudahan, mereka bisa mengembalikan data dari backup file, dan kembali ke sistem layanan tanpa downtime signifikan.

Fakultas Teknologi Informasi (FTIf) merupakan salah satu fakultas di ITS yang menyelenggarakan aktivitas pendidikan di bidang pengembangan teknologi informasi sehingga dituntut untuk selalu mengembangkan diri seiring dengan perkembangan teknologi [3]. Hal ini menyebabkan keamanan informasi menjadi hal yang sangat penting untuk diperhatikan.

Perkembangan teknologi informasi tidak sepenuhnya bebas risiko, terutama risiko keamanan. Hal ini terbukti dengan terjadinya pembobolan Formulir Rencana Studi (FRS) online, padahal FRS online merupakan aplikasi utama yang menyangkut kegiatan akademik di ITS. Hal ini disebabkan tidak adanya manajemen keamanan informasi yang dibuat untuk mengantisipasi masalah-masalah keamanan yang mungkin terjadi.

Kebijakan Keamanan Informasi merupakan salah satu bagian dari manajemen keamanan informasi yang dapat dikembangkan untuk meminimalisir atau mencegah risiko-risiko mengenai keamanan informasi seperti pembobolan FRS online seperti yang telah disebutkan diatas, penyalahgunaan akses dan permasalahan lainnya.

Octave merupakan metodologi yang meningkatkan proses pengambilan keputusan tentang perlindungan dan pengelolaan sumber daya di suatu organisasi berdasarkan penilaian risiko.

1.2 Rumusan Permasalahan

Permasalahan yang diangkat dalam proyek tugas akhir ini adalah:

1. Aset-aset apa saja yang berperan dalam keamanan Informasi yang harus dilindungi keamanannya?
2. Bagaimanan hasil dari penilaian (*assessment*) risiko dengan metode OCTAVE?
3. Bagaimana rancangan kebijakan keamanan informasi yang dibuat dapat mengakomodasikan prinsip-prinsip *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan)?

1.3 Batasan

Dari permasalahan yang telah disebutkan di atas, maka batasan-batasan dalam tugas akhir ini adalah:

1. Pengerjaan Kebijakan Keamanan Informasi yang dibuat hanya hanya sebatas usulan / draft.
2. Penggunaan *Internasional Organisation for Standardization* (ISO) 17799 sebagai checklist keamanan informasi untuk membantu dalam pemenuhan pengukuran pada kebijakan yang telah dibuat.

1.4 Tujuan

Tujuan tugas akhir ini adalah untuk mendapatkan dokumen kebijakan keamanan informasi dalam lingkup FTIf ITS berdasarkan hasil analisis menggunakan metode octave.

1.5 Manfaat

Manfaat dari tugas akhir ini adalah sebagai berikut:

1. Memantapkan kriterian terhadap risiko
2. Membantu perusahaan untuk mengatur tindakan dalam mencapai tujuan organisasi karena Kebijakan keamanan informasi dapat dijadikan sebagai pedoman karyawan dalam berperilaku.

3. Membantu meningkatkan kesadaran (*awareness*).
4. Meningkatkan ketersediaan informasi, integritas dan kerahasiaan, baik dari dalam dan luar organisasi.
5. Membantu pihak manajemen dalam membuat keputusan bisnis yang cerdas tentang efektivitas biaya untuk mengurangi atau menghilangkan tiap ancaman dan dasar pengambilan keputusanyang tidak pada kenyataan ancaman yang ada, akan tetapi lebih pada risiko yang terkait dengan bisnis.
6. Membantu meraih kepercayaan *stakeholders* karena Kebijakan Keamanan informasi dapat menjadi sarana publikasi dan komunikasi yang akan menunjukkan kepada pelanggan, patner dan pihak pemerintah bahwa kualitas pelayanan dan keamanan yang baik dalam proses bisnis telah dikendalikan dengan benar.
7. Mempermudah auditor internal maupun eksternal untuk melakukan proses audit yang terukur.

1.6 Sistematika Penulisan

Sistematika penulisan Laporan Tugas Akhir dibagi menjadi bab sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi uraian mengenai latar belakang permasalahan, tujuan dari Tugas Akhir, manfaat Tugas Akhir, perumusan masalah, batasan masalah serta sistematika yang digunakan dalam pembahasan masalah ini.

BAB II TINJAUAN PUSTAKA

Bab ini akan menjelaskan mengenai definisi dan penjelasan mengenai pustaka-pustaka yang menjadi referensi.

BAB III METODOLOGI

Bab ini akan menjelaskan mengenai metode-metode yang digunakan dalam penyelesaian tugas akhir.

BAB IV PEMBUATAN KEBIJAKAN KEAMANAN INFORMASI

Bab ini akan membahas mengenai pembuatan kebijakan keamanan informasi di FTIf. Pembuatan kebijakan keamanan diawali dengan melakukan analisis risiko, pengembangan strategi perlindungan, dan perencanan mitigasi untuk aset kritis.

BAB V PENUTUP

Bab ini merangkum hasil akhir dari pembuatan Tugas Akhir menjadi sebuah simpulan dan dilengkapi dengan saran-saran untuk perbaikan ataupun penelitian lanjutan. Simpulan merupakan rangkuman dari hasil pembuatan sistem informasi. Sedangkan saran merupakan usulan atau rekomendasi dari peneliti terhadap hasil Tugas Akhir untuk perbaikan ataupun penelitian lanjutan sehingga hasil Tugas Akhir ini dapat diimplementasikan dengan baik.

Halaman ini sengaja dikosongkan

2. *Integrity (integritas)* aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin fihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
3. *Availability (ketersediaan)* aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Gambar 2.1 Elemen-elemen keamanan informasi [6]

Dari waktu ke waktu aspek keamanan informasi menjadi semakin luas. Dan hal ini disebutkan oleh Dr. Michael E.Whitman dan Herbert J. Mattord [7] dalam bukunya Management Of Information Security adalah:

- *Privacy*
  Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik.
- *Identification*
  Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali individu pengguna. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi secara umum dilakukan dalam penggunaan *user name* atau *user ID.*
- *Authentication*

Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang mereka klaim.

- *Authorization*
  Setelah identitas pengguna diautentikasi, sebuah proses yang disebut autorisasi memberikan jaminan bahwa pengguna (manusia ataupun komputer) telah mendapatkan autorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari aset informasi.
- *Accountability*
  Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktifitas terhadap aset informasi yang telah dilakukan, dan siapa yang melakukan aktifitas itu.
  Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak.

2.2 Kebijakan Keamanan Informasi

"Kebijakan adalah rangkaian konsep dan asas yang menjadi pedoman dan dasar rencana dalam pelaksanaan suatu pekerjaan, kepemimpinan, dan cara bertindak"[8]. Istilah ini dapat diterapkan pada pemerintahan, organisasi dan kelompok sektor swasta, serta individu. Kebijakan berbeda dengan peraturan dan hukum. Jika hukum dapat memaksakan atau melarang suatu perilaku (misalnya suatu hukum yang mengharuskan pembayaran pajak penghasilan), kebijakan hanya menjadi pedoman tindakan yang paling mungkin memperoleh hasil yang diinginkan.

Kebijakan atau kajian kebijakan dapat pula merujuk pada proses pembuatan keputusan-keputusan penting organisasi, termasuk identifikasi berbagai alternatif seperti prioritas program atau pengeluaran, dan pemilihannya berdasarkan dampaknya. Kebijakan juga dapat diartikan sebagai mekanisme politis, manajemen, finansial, atau administratif untuk mencapai suatu

BAB II
TINJAUAN PUSTAKA

Bab tinjauan pustaka ini akan memaparkan teori-teori yang mendasari munculnya permasalahan dan solusi dalam merumuskan kebijakan keamanan Informasi.

2.1 Keamanan Informasi

Keamanan Informasi (*Information Security*) biasa disebut IS atau infosec. Keamanan Informasi yang diartikan secara harfiah Keamanan (Bahasa Indonesia) dan *Security* (Bahasa Inggris), berasal dari bahasa yunani "*Secure*" yang berarti adalah aman. Sedangkan Informasi dan *Information* berasal dari "*To-Inform*" yang berarti adalah memberitahu. Berikut ini adalah berbagai pendapat mengenai keamanan informasi:

- "Keamanan Informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki" [4].
- "Keamanan Informasi adalah melindungi informasi dan sistem informasi dari akses yang tidak diotorisasi, pengguna, penyingkapan, gangguan, modifikasi, atau kerusakan" [5].

Berdasarkan dari definisi diatas dapat disimpulkan bahwa "keamanan informasi" merupakan suatu upaya untuk mengamankan aset milik perusahaan dari akses yang dapat menyebabkan penyingkapan, gangguan, modifikasi atau kerusakan. Salah satu upaya yang dilakukan adalah merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan.

2.1.1 Komponen Keamanan Informasi

"Keamanan informasi adalah perlindungan informasi terhadap sistem dan perangkat yang digunakan, menyimpan, dan mengirimkannya" [6]. Keamanan informasi melindungi informasi

dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi dan peluang usaha. Di bawah ini terdapat beberapa komponen yang berkontribusi dalam program keamanan informasi secara keseluruhan.

- *Physical Security,* merupakan strategi untuk mengamankan pekerja atau anggota organisasi, aset perangkat keras, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
- *Personal Security,* merupakan *overlap* dengan '*phisycal security*' dalam melindungi orang-orang dalam organisasi.
- *Operation Security,* merupakan strategi untuk mengamankan kemampuan organisasi atau perusahaan dalam bekerja tanpa gangguan.
- *Communications Security,* merupakan strategi untuk mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
- *Network Security* , merupakan strategi untuk mengamankan peralatan jaringan data organisasi, isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

2.1.2 Aspek Keamanan Informasi

Keamanan informasi memiliki beberapa aspek yang harus dipahami untuk dapat diterapkan. Beberapa aspek tersebut, tiga yang pertama disebut C.I.A (*Confidentiality, Integrity & Availability) "triangle model"* (Gambar 2.1). Berikut adalah penjelasan yang dapat diberikan:

1. *Confidentiality (kerahasiaan)* aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

tujuan eksplisit. Sehingga kebijakan keamanan Informasi dapat diartikan sebagai berikut :

- "kebijakan keamanan informasi merupakan gabungan dari arahan, aturan, dan praktik yang menentukan bagaimana sebuah organisasi mengelola, melindungi, dan mendistribusikan informasi" [9].
- "kebijakan keamanan informasi adalah hasil dari pembangunan yang sesuai kontrol ditetapkan, dalam bentuk kebijakan, praktik, prosedures, struktur organisasi dan beberapa fungsi dalam perangkat lunak, perangkat keras dan infrastruktur teknologi informasi untuk menjamin keamanan seluruh informasi"[10].
- "kebijakan Keamanan Informasi merupakan jenis usaha yang khusus mendokumentasikan aturan untuk melindungi informasi dan sistem yang menyimpan dan memproses informasi"[11].

Kesimpulannya, kebijakan keamanan informasi merupakan gabungan dari arahan, aturan, dan praktik yang menentukan bagaimanan sebuah organisasi mengelola, melindungi, dan mendistribusikan informasi. Kebijakan keamanan informasi biasanya didokumentasikan dalam satu atau lebih dokumen. Dalam sebuah organisasi, dokumen kebijakan ini ditulis untuk menyediakan tingkat tinggi deskripsi kontrol dari berbagai organisasi yang akan digunakan untuk melindungi informasi.

2.2.1 Kategori Kebijakan Keamanan Informasi

Dalam keamanan informasi [6], ada tiga kategori umum dari kebijakan yaitu:

- *Enterprise Information Security Policy (EISP)* menentukan kebijakan departemen keamanan informasi dan menciptakan kondisi keamanan informasi di setiap bagian organisasi.
- *Issue Spesific Security Policy (ISSP)* adalah sebuah peraturan yang menjelaskan perilaku yang dapat diterima dan tidak dapat diterima dari segi keamanan informasi pada setiap

teknologi yang digunakan, misalnya e-mail atau penggunaan internet.

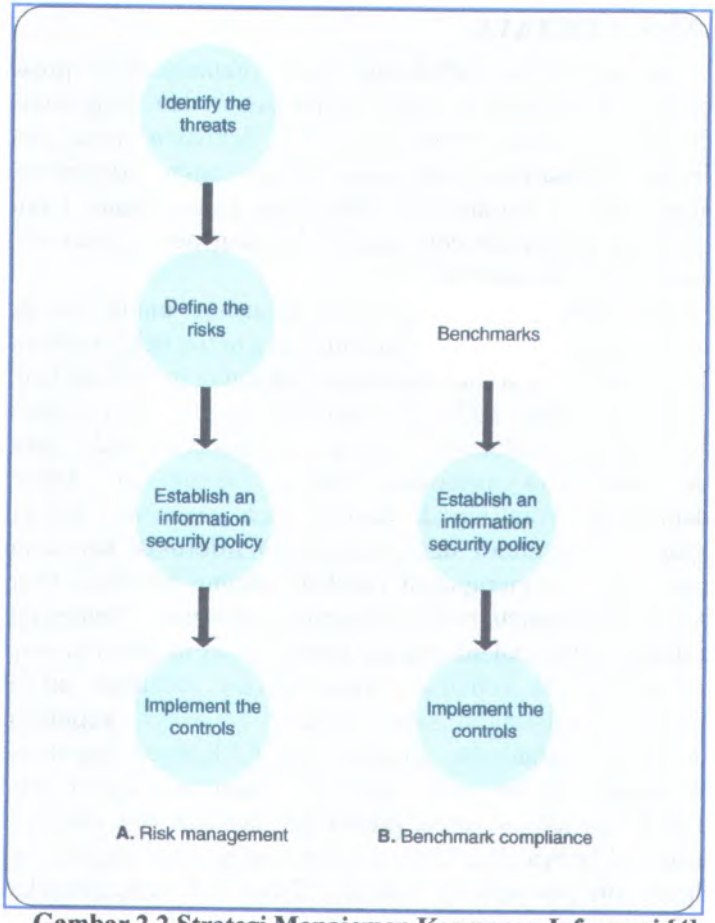
- *System Spesific Policy (SSP)* pengendali konfigurasi penggunaan perangkat atau teknologi secara teknis atau manajerial.

2.2.2 Dasar Formulasi Kebijakan Keamanan Informasi

Strategi manajemen keamanan informasi terdiri dari empat langkah (gambar 2.2), yaitu mengidentifikasikan ancaman yang dapat menyerang sumber daya informasi perusahaan, mendefinisikan risiko terhadap ancaman yang mengganggu, menetapkan kebijakan keamanan informasi, dan mengimplementasikan kontrol yang dialamatkan pada risiko. Selain itu ancaman yang mengganggu risiko juga harus di kontrol.

Pendekatan yang dapat digunakan dalam memformulasikan kebijakan keamanan Informasi ada 3 (tiga), yaitu:

1. *Risk management* pendekatan ini digunakan jika kebijakan keamanan informasi yang dibuat didasarkan pada tingkat keamanan sumber daya informasi perusahaan dibandingkan dengan risiko yang dihadapi.
2. *Information security benchmark* adalah tingkat keamanan yang disarankan pada keadaan normal harus menawarkan perlindungan yang cukup terhadap gangguan yang tidak terotorisasi.
   - Tolok ukur adalah tingkat kinerja yang disarankan.
   - Ditetapkan oleh pemerintah dan asosiasi industri.
   - Mencerminkan komponen-komponen program keamanan informasi yang baik menurut otoritas-otoritas tersebut.
3. *Benchmark compliance* dapat diasumsikan bahwa pemerintah dan otoritas industri telah melakukan pekerjaan yang baik dalam mempertimbangkan berbagai ancaman serta risiko dan tolok ukur tersebut.



Gambar 2.2 Strategi Manajemen Keamanan Informasi [4]

2.3 Analisis Risiko

Analisis risiko memegang peranan yang penting dalam penerapan keamanan informasi. Salah satu diantara banyak metode *risk assesment* adalah metode octave yang dikembangkan oleh Carneigie Mellon Software Engineering Institute, Pittsburg. Metode inilah yang digunakan dalam penelitian tugas akhir ini.

2.3.1 Metode OCTAVE

"Octave adalah metodologi yang meningkatkan proses pengambilan keputusan tentang perlindungan dan pengelolaan sumber daya di suatu perusahaan" [12]. Penilaian risiko pada metode ini didasarkan pada tiga prinsip dasar administrasi keamanan, yaitu : kerahasiaan, integritas, ketersediaan. Untuk melaksanakan prinsip tersebut perlu dilakukan pengklasifikasian sederhana informasi penting.

Pendekatan metodologi octave dirancang untuk menjadi *self-directed* sehingga memungkinkan orang untuk belajar tentang masalah keamanan dan meningkatkan keamanan organisasi tanpa sikap yang tak perlu pada ahli luar dan vendor [12]. Sebuah evaluasi dengan sendirinya hanya menyediakan arah untuk kegiatan keamanan informasi sebuah organisasi. Berarti perbaikan tidak akan terjadi kecuali oleh organisasi melalui penerapan hasil evaluasi dan pengelolaan informasi keamanan dan risiko. Octave merupakan langkah penting pertama dalam pendekatan manajemen risiko keamanan informasi. Pendekatan octave didefinisikan dalam satu set kriteria yang meliputi prinsip-prinsip, atribut, dan keluaran. Prinsip-prinsip mendasar adalah konsep yang berdasarkan sifat evaluasi. Misalnya, keputusan sepihak adalah salah satu prinsip octave. Konsep keputusan sepihak berarti bahwa orang-orang di dalam organisasi telah berada di posisi terbaik untuk memimpin evaluasi dan membuat keputusan. Akhirnya, output yang menentukan hasil analisis tim yang harus dicapai selama evaluasi. Tabel 2.1 mencantumkan prinsip-prinsip struktur, atribut, dan output.

Tabel 2.1 Prinsip, Atribut, dan Output Keamanan Informasi [12]

Prinsip, Atribut, dan ouput keamanan informasi		
Prinsip	Atribut	
Pengukuran secara langsung Definisi Proses Dasar untuk proses selanjutnya Fokus pada beberapa aset kritis Integrasi Manajemen omunikasi Terbuka Perspektif Global Tim Kerja	Tim Analisis dan Keahlian tim atalog dari Profil Ancaman Katalog dari aktifitas evaluasi kerentanan yang telah didefinisikan Dokumentasi evaluasi hasil evaluasi ruang lingkup dan tahap selanjutnya Fokus pada risiko dan aktifitas Isu Teknologi dan Organisasi Partisipasi teknologi informasi dan bisnis Pendekatan Kolaborasi dan partisipasi manajemen senior	
Output		
Fase I	Fase II	Fase III
Aset Kritis Kebutuhan Keamanan untuk Aset Kritis Ancaman pada Aset kritis Praktek Keamanan saat ini Kerentanan organisasi saat ini	Komponen Utama Kerentanan Teknologi saat ini	Risiko Aset Kritis Pengukuran Risiko Strategi perlindungan Perencanaan mitigasi risiko

2.3.2 Pengenalan Metode OCTAVE

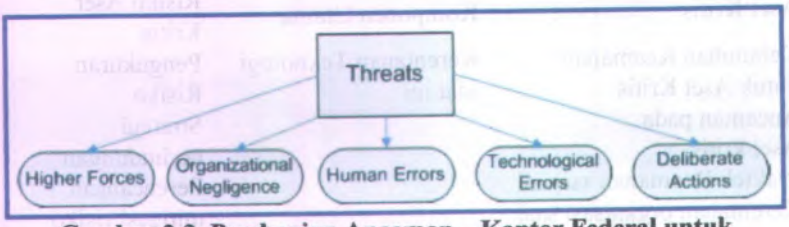
Langkah pertama untuk mengelola risiko keamanan informasi adalah mengenali risiko organisasi yang ada. Setelah itu, organisasi dapat membuat rencana penanggulangan dan reduksi risiko terhadap masing-masing risiko yang telah diketahui. Metode octave(*The Operationally Critical Threat, Aset, and Vulnerability Evaluation*) memungkinkan organisasi melakukan hal di atas. "Octave adalah sebuah pendekatan terhadap evaluasi risiko keamanan informasi yang komprehensif, sistematik, terarah, dan dilakukan sendiri" [12]. Pendekatannya disusun dalam satu set kriteria yang mendefinisikan elemen

esensial dari evaluasi risiko keamanan informasi. Octave memerlukan katalog informasi untuk mengukur praktek organisasi, menganalisa ancaman, dan membangun strategi proteksi. Katalog ini meliputi:

- *catalog of practices* – sebuah koleksi strategi dan praktek keamanan informasi,
- *generic threat profile* – sebuah koleksi sumber ancaman utama, dan
- *catalog of vulnerabilities* – sebuah koleksi dari kerentanan berdasarkan platform dan aplikasi.

2.3.3 Tipe Ancaman dan Pengukuran Keamanan

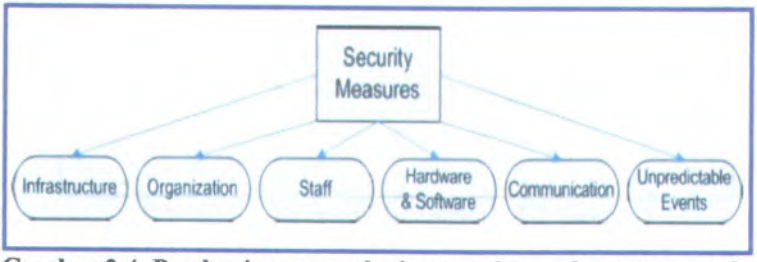
Pertimbangan pengambilan tipe ancaman dalam octave diilustrasikan dalam gambar 2.3



Gambar 2.3 Pembagian Ancaman – Kantor Federal untuk Keamanan Teknologi Informasi *(BSI)* [12]

"*Higher Forces*" adalah ancaman yang tidak dapat diketahui waktu terjadinya dan tidak secara langsung mempengaruhi organisasi (misalnya kebakaran, banjir kegagalan jaringan). *Organisasi Negligence* adalah usaha yang dilakukan oleh organisasi untuk meminimalkan risiko yang dihasilkan dari sistem pengolahan data yang telah disusun (misalnya akses ke sumber daya yang tidak sah, atau kurangnya kontrol sumberdaya). Kesalahan manusia juga sangat penting karena sebagian besar ancaman banyak ditimbulkan oleh faktor ini. Octave juga membuat staf lebih menyadari berbagai ancaman yang terjadi. Kesalahan penggunaan teknologi terkadang secara langsung

diakibatkan oleh tindakan yang sengaja. Kesengajaan menyebabkan kegagalan jaringan menjadi kesalahan teknologi dan langsung berdampak pada organisasi. Sedangkan serangan eksternal biasanya diambil menjadi pertimbangan di kemudian hari.

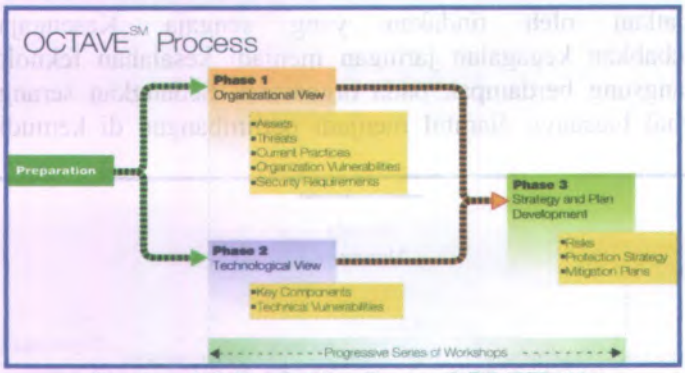


Gambar 2.4 Pembagian secara logic pengukuran keamanan pada proses OCTAVE [12]

Infrastruktur, organisasi, staff, hardware & software, komunikasi, dan kejadian yang tidak dapat di presiksi merupakan pengukuran yang dilaksanakan pada saat proses octave. Pengukuran ini dilakukan dalam rangka untuk mencegah kerugian, bukan dalam memperbaiki kerusakan. Perhitungan risiko diberikan ketika peristiwa terjadi sehingga rencana untuk mengatasi keadaan darurat dapat dikembangkan dan diterapkan dalam kasus kejadian yang tidak dapat diprediksi.

2.3.4 Langkah-langkah Metode OCTAVE

Metode octave menggunakan pendekatan tiga fase untuk menguji isu-isu teknologi, menyusun sebuah gambaran komprehensif keamanan informasi yang dibutuhkan oleh organisasi (gambar 2.5). Metode ini menggunakan informasi mengenai aset, praktek keamanan informasi dan strategi keamanan informasi. Setiap fase terdiri dari beberapa proses. Berikut adalah fase dan proses yang ada dalam metode octave [12]:



Gambar 2.5 ***Pembagian Proses OCTAVE*** **[12]**

1. **Fase Pertama. Sudut Pandang Organisasi** ***(Organizational View)***
   Fase pertama dalam octave adalah membuat Profil Ancaman berbasis Aset *(Aset-Based Threat Profiles)*. Fase ini meliputi pengumpulan pengetahuan untuk memperoleh informasi mengenai aset, keamanan yang dibutuhkan oleh setiap aset, area yang diperhatikan, strategi perlindungan yang sedang diterapkan,dan kerentanan organisasi terkini. Pada fase ini data yang diperoleh dikonsolidasikan dan dianalisis ke dalam sebuah profil aset kritis organisasi.

2. **Fase Ke dua. Sudut Pandang Teknologi (*Technological view*)**
   Fase ke dua dalam octave adalah mengidentifikasikan kerentanan infrastruktur *(Identify Infrastructure Vulnerabilities)*. Fase ini melihat Kerentanan secara teknis yang terjadi pada aset kritis dan komponen infrastruktur utama yang mendukung aset tersebut.

3. **Fase Ke Tiga. Membuat Perencanaan dan Strategi Keamanan (*Develop Security Strategy and Plans*)**
   Fase ke tiga dalam octave adalah membuat perencanaan dan strategi keamanan (*Develop Security Strategy and Plans*).

Pada fase ini didefinisikan risiko terkait dengan aset kritis, membuat rencana mitigasi untuk risiko tersebut, dan membuat strategi perlindungan pada organisasi.

2.3.5 Output OCTAVE

Manajemen keamanan risiko memerlukan keseimbangan antara aktivitas proaktif dan reaktif. Selama evaluasi menggunakan metode OCTAVE aspek keamanan dapat terlihat dari berbagai sudut pandang sehingga dimungkinkan tercapainya keseimbangan dan kesesuaian dengan kebutuhan organsisasi/perusahaan.

Output utama dari metode OCTAVE adalah:

1. Strategi perlindungan menyeluruh terhadap aset organisasi/perusahaan. Setelah analisis risiko dengan menggunakan metode OCTAVE, seluruh kebijakan organisasi/perusahaan diharapkan selalu mempertimbangkan aspek keamanan.
2. Rencana mitigasi risiko. Risiko yang paling utama untuk dimitigasi adalah risiko terhadap aset-aset terpenting (aset kritis).
3. Rencana Aksi. Rencana ini meliputi beberapa rencana jangka pendek untuk mengatasi beberapa kelemahan tertentu.

2.4 Standar Industri

- United Kingdom's BS7799 [4]. standar Inggris menentukan satu set pengendalian dasar standar ini pertama kali dipublikasikan oleh British Standards Institute pada tahun 1995, kemudian dipublikasikan oleh International Standars Organization sebagai ISO 17799 pada tahun 2000 dan dibuat tersedia bagi para pengadopsi potensial secara online pada tahun 2003.
- BSI IT Baseline Protection Manual [4]. Pendekatan baseline ini juga diikuti oleh German Bundesamt fur Sicherheit in der Informationstechnik (BSI). baselines ini ditujukan untuk memberikan keamanan yang cukup jika yang menjadi tujuan

adalah kebutuhan proteksi normal. baselines dapat juga digunakan sebagai landasan perlindungan dengan kadar yang lebih tinggi jika dibutuhkan.

- COBIT [4]. COBIT, dari the Information Systems Audit and Control Association and Foundation (ISACAF), berfokus pada proses yang dapat diikuti perusahaan dalam menyusun standar, dengan berfokus pada penulisan dan pemeliharaan dokumentasi.
- GASSP [4]. Generally Accepted System Security Principles (GASSP) adalah produk dari Dewan Riset Nasional Amerika Serikat. Penekanan adalah pada alasan penentuan kebijakan keamanan.
- ISF Standard of Good Practice [4]. The Information Security Forum Standard mengambil pendekatan baseline, dengan memberikan perhatian yang cukup banyak pada perilaku pengguna yang diharapkan untuk kesuksesan program tersebut. Edisi 2005 berisi topik-topik seperti pesan instan yang aman, keamanan server WEB dan perlindungan virus.
- National Institut of Standard (NIST) [4] menyediakan kerangka untuk mengevaluasi keamanan di 17 daerah topik utama. NIST juga memberikan petunjuk tentang cara untuk mengukur efektivitas dalam setiap kategori.
- Program sertifikasi, yang meliputi:
  - *Information Systems Audit and Control Association (ISACA)*
  - *International Information System Security Certification Consortium (ISC)*
  - *SANS (SysAdmin, Audit, Network, Security) Institute*

2.5 ISO 17799

Information Technology – Code of practice for information Security Management dalam ISO/IEC 17799:2002 [13] adalah standar yang dijadikan referensi dalam lingkungan model keamanan informasi. Deskripsi dan struktur umumnya dikenal secara luas sebagai " *The Ten Sections of ISO/IEC 17799*" [13].

Tujuan ISO 17799 adalah untuk memberikan rekomendasi manajemen keamanan informasi untuk digunakan oleh mereka yang bertanggung jawab dalam: inisiasi, implementasi, atau pengelolaan keamanan informasi pada organisasinya. ISO/IEC 17799 terdiri atas 127 kendali dalam 10 kategori keamanan informasi.

1) Kebijakan Keamanan
   Memberikan arah dan dukungan terhadap manajemen keamanan informasi yang akan diterapkan dalam organisasi. Hal ini tidak selalu menjadi yang pertama dilakukan dalam manajemen keamanan informasi, tetapi bisa merupakan refleksi dari hasil risk assessment yang telah dilakukan. *Information Security Policy* harus senantiasa dianalisa dan diupdate secara regular karena adanya perubahan-perubahan ancaman terhadap keamanan informasi.
2) Keamanan Organisasi
   Bertujuan untuk mengatur keamanan informasi didalam organisasi, mengelola keamanan fasilitas pemrosesan informasi organisasi dan aset informasi yang diakses oleh pihak ketiga, mengelola keamanan informasi jika tanggungjawab pemrosesan informasi dilakukan oleh pihak ketiga atau organisasi lain.
3) Klasifikasi dan pengontrolan aset
   Diperlukan untuk mengelola langkah proteksi yang tepat untuk aset organisasi dan menjamin bahwa aset informasi memperoleh tingkat perlindungan yang tepat.
4) Keamanan Perorangan
   Bertujuan untuk mengurangi kesalahan manusia, pencurian, kesalahan pengguna fasilitas, menjamin bahwa pengguna mengetahui ancaman terhadap keamanan informasi dan dilengkapi peralatan pendukung kebijakan keamanan informasi dalam kerja mereka, meminimalkan kerusakan akibat insiden keamanan dan malfungsi serta belajar dari insiden yang pernah terjadi.

5) Keamanan secara fisik dan lingkungan
Memiliki tujuan mencegah akses tanpa otorisasi, kerusakan, dan interfensi terhadap tempat kerja dan informasi; mencegah kehilangan, kerusakan aset, dan gangguan terhadap aktifitas organisasi; mencegah pencurian informasi dan fasilitas pemrosesan informasi.
6) Manajemen Komunikasi dan operasi
Bertujuan untuk menjamin keamanan operasi pada fasilitas pemrosesan informasi, meminimalkan risiko kegagalan sistem, melindungi integritas software dan informasi, mengelola integrity dan availability proses informasi dan komunikasi; menjemin perlindungan informasi dalam jaringan dan perlindungan terhadap infrastruktur pendukung, mencegah kerusakan aset dan interupsi terhadap aktifitas organisasi, mencegah kehilangan, modifikasi, atau kesalahan pertukaran informasi antar organisasi.
7) Pengontrolan akses
Bertujuan untuk mengendalikan akses pada informasi perusahaan, mencegah akses tanpa otorisasi kedalam sistem informasi, menjamin perlindungan layanan jaringan; mencegah akses computer tanpa otorisasi, mendeteksi aktifitas tanpa otorisasi, menjamin keamanan informasi saat menggunakan perangkat bergerak dan jaringan telekomunikasi.
8) Sistem Pengembangan dan Pemeliharaan
Bertujuan untuk menjamin keamanan terbangun dalam sistem operasional organisai; mencegah kehilangan, modifikasi, atau kesalahan pemakaian data pengguna dalam sistem aplikasi; melindungi confidentiality, authenticity, dan integritas informasi; menjamin proyek teknologi informasi dan aktifitas pendukungnya berada dalam keamanan; mengelola keamanan software aplikasi dan data.

9) Manajemen Kelanjutan Usaha
   Bertujuan untuk melakukan reaksi terhadap gangguan aktifitas organisasi dan proses bisnis yang kritis bagi organisasi ketika terjadi bencana.
10) Penyesuaian/Ketaatan
   Memiliki tujuan: menghindari pelanggaran terhadap setiap hukum criminal dan social, peraturan perundang-undangan, dan obligasi kontrak dalam setiap kebutuhan keamanan informasi; menjamin terpenuhinya organizational security policy dan standar keamanan informasi dalam penerapan manajemen keamanan informasi organisasi; memaksimalkan efektifitas dan meminimalkan pengaruh kepada atau dari proses audit.

Gambar 2.6 Struktur dari kesepuluh wilayah standar [14]

Halaman ini sengaja dikosongkan

BAB III
METODOLOGI

Metodologi dalam tugas akhir digunakan sebagai panduan dalam proses pengerjaan tugas akhir ini agar tahapan dalam pengerjaannya dapat berjalan secara terarah dan sistematis. Tahapan metodologi penelitian dalam penyusunan Tugas Akhir ini secara umum terdiri dari 6 tahap yakni:

a. Persiapan
b. Pengumpulan Data dan Informasi
c. Penilaian (*Assessment*) Risiko
d. Penyusunan Dokumen Kebijakan Keamanan Informasi
e. Pemetaan (*Mapping*)
f. Penyusunan Buku Tugas Akhir.

Hubungan antar tahapan penelitian terangkum dalam gambar 3.1 Alur metodologi. Berikut penjelasan dari setiap tahap pada metodologi penelitian diatas.

3.1 Tahap Persiapan

Merupakan awal dari kegiatan penelitian, dimana pada tahap ini akan terdiri dari dua bagian, yaitu:

3.1.1 Studi Literatur

Studi Literatur yang dilakukan dalam pembuatan tugas akhir ini adalah pembelajaran literatur yang terkait dengan permasalahan yang ada, seperti pembelajaran mengenai keamanan informasi, penilaian risiko, dan proses pembuatan kebijakan keamanan informasi. Pembelajaran tersebut dilakukan dengan pencarian berbagai macam literature yang relevan dan dapat menghubungkan semua variabel-variabel yang ada dengan pembuatan Kebijakan Keamanan Informasi. Literatur yang digunakan didapatkan dari *text book*, tugas akhir dan tesis, maupun sumber bacaan *softcopy* yang didapatkan dari internet

3.1.2 Identifikasi Permasalahan

Pada tahapan ini akan dikaji sebab-sebab timbulnya permasalahan, bagaimana masalah akan dirumuskan, tujuan dan manfaat penelitian sehingga akhirnya akan dimengerti hal apa saja yang diharapkan dari hasil penelitian ini. Disini permasalahan akan dirumuskan lebih rinci, serta melakukan pengkajian tentang pembuatan usulan kebijakan keamanan informasi, meliputi konsep-konsepnya, kemungkinan penerapan dan pengkajiannya, untuk dapat mengidentifikasikan hal-hal yang mempengaruhi perumusan kebutuhan kebijakan keamanan informasi. Selain itu juga dilakukan pemahaman secara menyeluruh mengenai organisasi, baik tujuan maupun arah organisasi. Sehingga Kebijakan yang akan dikembakan sesuai dengan kebijakan yang ada, aturan, peraturan dan undang-undang.

3.2 Tahap Pengumpulan Data dan Informasi

Tahap ini dilakukan untuk mengumpulkan semua informasi penting dalam penilaian (*assessment*) terkait dengan keamanan FTIf Institut Teknologi Sepuluh Nopember. Teknik yang dilakukan untuk mendapatkan informasi yaitu melalui wawancara, Pengamatan kembali dokumen terkait dan observasi. Berikut adalah penjelasan dari teknik-teknik yang digunakan dalam tahap ini:

3.2.1 Wawancara

Wawancara dilakukan secara langsung kepada orang yang mempunyai wewenang pada proses bisnis yang dijadikan objek penelitian. Dari tahapan wawancara diharapkan dapat diperoleh informasi mengenai gambaran FTIf, aset-aset yang dimiliki serta informasi mengenai permasalahan yang sering terjadi dan menjadi ancaman dalam keamanan informasi dan data baik dari sudut pandang pihak manajemen maupun staff dalam FTIf.

Secara umum, langkah-langkah wawancara antara lain:

- Memilih sumber informasi (narasumber/orang yang diwawancarai)
- Merancang pertanyaan interview

- Menyiapkan untuk interview
- Memandu interview
- Menindaklanjuti hasil interview

3.2.2 Pengamatan Kembali Dokumen Terkait

Pengamatan kembali dokumen FTIf ITS adalah salah satu cara paling efektif untuk mengumpulkan informasi tentang situasi sistem yang ada. Dokumentasi sistem yang ada saat ini, formulir-formulir dan dokumen-dokumen yang digunakan untuk menjalankan aktifitas bisnis, laporan-laporan yang disusun secara berkala, merupakan sumber informasi yang penting yang mendeskrispsikan lingkungan dari komponen perusahaan.

3.2.3 Observasi

Merupakan teknik pengumpulan data dengan melakukan pengamatan secara langsung proses bisnis yang berjalan di FTIf tanpa harus terlibat langsung di dalam proses bisnisnya. Dalam observasi ini surveyor dapat mengkonfirmasikan langsung hasil data yang di dapat pada teknik lain yang ada.

3.3 Tahap penilaian (*assessment*) Risiko

Setelah tahap pengumpulan semua informasi telah terkumpul, maka tahap selanjutnya adalah melakukan penilaian risiko pada aset-aset yang telah teridentifikasikan pada tahap sebelumnya.

3.3.1 Membuat Profil Ancaman berdasarkan Aset

Fase pertama dalam OCTAVE adalah membuat Profil Ancaman berbasis Aset *(Aset-Based Threat Profiles)*. Fase ini meliputi pengumpulan pengetahuan untuk memperoleh informasi mengenai aset, keamanan yang dibutuhkan oleh setiap aset, area yang diperhatikan, strategi perlindungan yang sedang diterapkan,dan kerentanan organisasi terkini. Pada fase ini data yang diperoleh dikonsolidasikan dan dianalisis ke dalam sebuah profil aset kritis organisasi.

3.3.2 Mengidentifikasikan Kerentanan Infrastruktur

Fase ke dua dalam octave adalah mengidentifikasikan kerentanan infrastruktur (*Identify Infrastructure Vulnerabilities)*. Fase ini melihat kerentanan (*vulnerability)* secara teknis yang terjadi pada aset kritis dan komponen infrastruktur utama yang mendukung aset tersebut.

3.3.3 Membuat Perencanaan dan Strategi Keamanan

Dilakukan proses analisa risiko melalui pendefinisian kriteria evaluasi dampak bagi organisasi untuk membuat landasan umum penentuan *impact value* (high, medium, low), demikian juga untuk ancaman terhadap aset kritis. Dari hasil proses analisa risiko, maka selanjutnya dapat mengembangkan strategi yang tepat untuk melindungi aset yang berfokus pada perbaikan praktek keamanan organisasi. Selain itu juga membuat perencanaan mitigasi bila terjadi *accident.*

3.4 Tahap Penyusunan Dokumen Kebijakan Keamanan Informasi

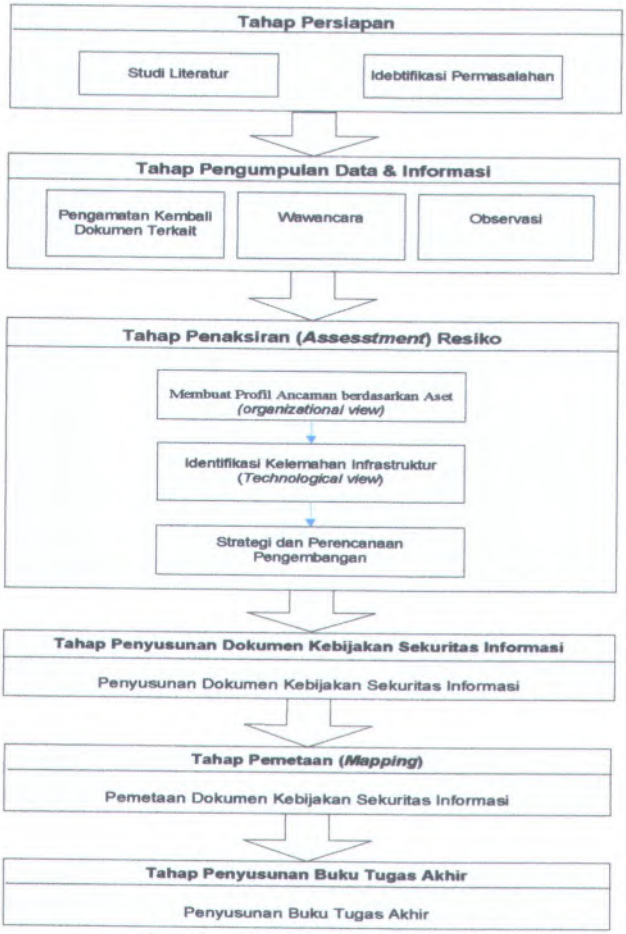
Pada tahap ini dilakukan penyusunan dokumen kebijakan keamanan informasi dengan mengacu pada hasil analisis risiko yang telah dilakukan pada tahap sebelumnya. Dari hasil analisis risiko tersebut akan dapat dikembangkan satu atau mungkin lebih kebijakan keamanan yang merupakan komponen dari dokumen kebijakan keamanan informasi.

3.5 Tahap Pemetaan (*Mapping*)

Setelah dokumen kebijakan keamanan informasi selesai dibuat, langkah selanjutnya adalah melakukan pemetaan (*mapping*) pada prinsip-prinsip CIA, yaitu kerahasiaan (*confidentiality)*, integritas (*integrity)* dan ketersediaan (*availability)*. Hasil dari pemetaan ini adalah didapatkannya dokumen kebijakan keamanan informasi yang dapat mengakomodasikan prinsip-prinsip CIA tersebut.

3.6 Tahap Penyusunan Buku Tugas Akhir,

Setiap langkah-langkah pengerjaan tugas akhir dari awal sampai akhir didokumentasikan dan ditulis dalam sebuah laporan yang sesuai dengan format tugas akhir sehingga menghasilkan buku tugas akhir.



Gambar 3.1 Metodologi Penelitian

Halaman ini sengaja dikosongkan

BAB IV
PEMBUATAN KEBIJAKAN KEAMANAN INFORMASI

Bab ini membahas pembuatan kebijakan keamanan informasi di FTIf. Pembuatan kebijakan keamanan diawali dengan melakukan analisis risiko. Adapun metode yang digunakan untuk analisis risiko adalah octave sehingga pelaksanaan analisis risiko dilakukan berdasarkan langkah-langkah yang ada dalam metode octave. Sebelum melakukan analisis risiko dilakukan kajian terlebih dahulu pada organisasi. Hasil dari dokumentasi kebijakan keamanan informasi pada tugas akhir ini akan dibuatkan secara terpisah menjadi buku tersendiri di luar buku tugas akhir ini.

4.1 Analisis Risiko Metode OCTAVE

Sebelum melakukan analisis risiko, terlebih dahulu akan digambarkan secara singkat mengenai FTIf. Analisis Risiko ini terdiri 3 tahap, yaitu membuat profil ancaman berbasis aset, mengidentifikaikan kerentanan infrastruktur, dan Membuat Perencanaan dan Strategi Keamanan.

4.1.1 Deskripsi FTI ITS

FTIf merupakan salah satu fakultas di ITS yang telah disahkan berdasarkan Surat Keputusan Menteri Pendidikan Nasional Republik Indonesia Nomor 109/O/2002, FTIf ITS terdiri dari dua jurusan, yaitu Jurusan Teknik Informatika dan Program Studi Sistem Informasi.

FTIf mempunyai Visi menjadikan FTIf ITS sebagai lembaga yang unggul dalam bidang pendidikan, penelitian, dan penerapan teknologi informasi dan mampu mempersiapkan sumber daya manusia yang berkualitas dan percepatan dapat mengikuti perkembangan teknologi informasi [3]. Untuk

mendukung visi tersebut ada beberapa misi yang saat ini dijalankan di FTIf. Berikut adalah misi dari FTIf:

1. Menegakkan moral dan etika dalam pelaksanaan Tridharma perguruan tinggi.
2. Memperkuat pelaksanaan program-program sarjana dan lulusan pendidikan, dan program pendidikan yang dikelola oleh FTIf ITS.
3. Memperkuat kemampuan kegiatan penelitian dan penyebarluasan hasil penelitian dan paket teknologi yang tepat yang berguna untuk meningkatkan kualitas kehidupan masyarakat.
4. Memperkuat jalinan kerja sama dengan pihak luar dan meningkatkan daya saing dengan kompetitor.

Perkembangan teknologi informasi yang relatif cepat menuntut FTIf untuk selalu mengembangkan diri. Tidak hanya terbatas pada akademisi di lingkungan FTif saja, pengembangan diri juga dilakukan dengan mendorong penelitian-penelitian yang berorientasi sosial.

4.1.2 Membuat Profil Ancaman berbasis Aset

Tahap ini merupakan hasil evaluasi pada organisasi untuk menentukan aset yang paling penting bagi organisasi (aset kritis) dan mengidentifikasikan apa yang sedang dilakukan untuk melindungi aset mereka. Profil ancaman yang dibuat akan mengidentifikasikan mengenai aset penting, kebutuhan keamanan, dan area kritis yang ada pada organisasi. Identifikasi kebutuhan keamanan yang ada pada aset kritis didasarkan pada kerahasiaan, integritas dan ketersediannya pada organisasi. Sedangkan identifikasi area kritis didasarkan pada sumber ancaman yang ada pada aset kritis. Sumber ancaman yang ada pada aset kritis dikategorikan sebagai berikut:

1. Aktor manusia menggunakan jaringan merupakan ancaman terhadap aset kritis melalui akses jaringan komputer.
2. Aktor manusia menggunakan akses fisik merupakan ancaman terhadap aset kritis melalui akses fisik terhdap sistem.

3. Permasalahan sistem merupakan ancaman akibat gangguan pada teknologi sistem.
4. Permasalahan lain merupakan ancaman akibat hal lain yang tidak terkendali.

Tabel 4.1 sampai 4.3 menyediakan informasi mengenai aset kritis, kebutuhan keamanan, dan area kritis.

Tabel 4.1 Aset kritis

Aset Kritis	Alasan
Data Keuangan	Setiap uang yang masuk dan keluar harus dicatat sehingga tidak terjadi kesalahan dalam penulisan laporan keuangana.
Sistem Rekaman Data	Rekaman data dan informasi dimaksudkan untuk memungkinkan pelacakan kembali data dan informasi yang diperlukan serta memberikan peringatan dini kepada pihak yang melakukan tindakan perbaikan.
Sistem Informasi Akademik	Semua informasi akademik dikelola di system ini, seperti biodata mahasiswa, nilai mahasiswa, dll.
Aplikasi Perkantoran	Software ini digunakan sebagai pendukung untuk pelaksanaan kegiatan di FTIf.
Jaringan	Semua bagian di FTIf sudah memanfaatkan jaringan untuk mengakses informasi, yang dianggap penting seperti sistem informasi akademik, email, internet, dll
Server	Komputer yang menyediakan sumber daya dan mengendalikan akses di dalam suatu jaringan.
PC	Hampir semua staf, dosen, dan mahasiswa bergantung pada PC - semua orang menggunakan *workstation* untuk mengakses informasi yang dianggap penting: Sistem Informasi Akademik, email, internet dan sebagainya

Tabel 4.2 Kebutuhan keamanan aset kritis

Aset Kritis	Kebutuhan Keamanan	Penjelasan
Data Keuangan	Ketersediaan *(Availability)*	Akses tersedia selama jam kerja, yaitu pukul 8.00-16.00
	Kerahasiaan *(Confidentiality)*	Informasi yang ada harus dijaga kerahasiaannya
	Integritas (Integrity)	Hanya pengguna yang berwenang yang diperbolehkan untuk mengubah informasi.
Sistem Rekaman Data	Ketersediaan *(Availability)*	Akses tersedia selama jam kerja, yaitu pukul 8.00-16.00
	Kerahasiaan *(Confidentiality)*	Informasi yang ada harus dijaga kerahasiaannya
	Integritas (Integrity)	Hanya pengguna yang berwenang yang diperbolehkan untuk mengubah informasi.
Sistem Informasi Akademik	**Ketersediaan *(Availability)***	Akses tersedia selama 24/7 selama pengguna berada di jaringan internal
	Kerahasiaan *(Confidentiality)*	Informasi yang ada harus dijaga kerahasiaannya
	Integritas (Integrity)	Hanya pengguna yang berwenang yang diperbolehkan untuk mengubah informasi.
Aplikasi Perkantoran	**Ketersediaan *(Availability)***	Akses pada aplikasi ini tersedia selama jam kerja, yaitu pukul 8.00-16.00 Informasi harus tersedia jika dibutuhkan
	Kerahasiaan *(Confidentiality)*	Informasi harus dijaga kerahasiaannya (terbatas untuk orang-orang yang diberi ijin)

Aset Kritis	Kebutuhan Keamanan	Penjelasan
	Integritas (Integrity)	Hanya pengguna yang berwenang yang diperbolehkan untuk mengubah informasi. Data yang diisikan harus lengkap dan akurat
Jaringan	**Ketersediaan *(Availability)***	• Sistem tersedia mulai pukul 8.00-23.00(Bagi mahasiswa) • Sistem tersedia selama jam kerja, yaitu mulai pukul 8.00-16.00 (Bagi semua karyawan)
	Kerahasiaan *(Confidentiality)*	Informasi harus dijaga kerahasiaannya (terbatas untuk orang-orang yang diberi ijin)
	Integritas (*Integrity*)	Hanya pengguna yang berwenang yang diperbolehkan untuk menggunakan layanan ini
Server	**Ketersediaan *(Availability)***	• Sistem tersedia mulai pukul 8.00-23.00(Bagi mahasiswa) • Sistem tersedia selama jam kerja, yaitu mulai pukul 8.00-16.00 (Bagi semua karyawan)
	Kerahasiaan *(Confidentiality)*	Informasi harus dijaga kerahasiaannya (terbatas untuk orang-orang yang diberi ijin)
	Integritas (Integrity)	Hanya pengguna yang berwenang yang diperbolehkan untuk menggunakan layanan ini

Aset Kritis	Kebutuhan Keamanan	Penjelasan
PC	**Ketersediaan** *(Availability)*	• Sistem tersedia mulai pukul 8.00-23.00(Bagi mahasiswa) • Sistem tersedia selama jam kerja, yaitu mulai pukul 8.00-16.00 (Bagi semua karyawan)
	Kerahasiaan *(Confidentiality)*	Semua informasi yang tersimpan di PC harus dijaga kerahasiannya
	Integritas (Integrity)	Perangkat lunak harus seragam Informasi harus lengkap dan akurat

Tabel 4.3 Daftar Ancaman berdasarkan sumbernya

Aset Kritis	Sumber Ancaman	Ancaman
Data Keuangan	Aktor Manusia yang menggunakan jaringan	-

Aset Kritis	Sumber Ancaman	Ancaman
	Aktor Manusia menggunakan Akses Fisik	**Penyingkapan, Modifikasi** Data dibaca oleh pihak yang tidak berwenang Data diubah oleh pihak yang tidak berwenang Salah memasukkan data **Hilang/Rusak** Data Hilang/Rusak **Gangguan** Rusaknya media penyimpan data (Contoh : hardisk, CD, disket) Pencurian media penyimpan data (Contoh : hardisk, CD, disket)
	Permasalahan Sistem	-
	Permasalahan lain	Membicarakan isu mengenai permasalahan ini ke area publik
Aplikasi Perkantoran	Aktor Manusia yang menggunakan jaringan	-
	Aktor Manusia menggunakan Akses Fisik	**Penyingkapan, Modifikasi** Penggunaan aplikasi oleh pihak yang tidak berwenang Perubahan konfigurasi aplikasi oleh pihak yang tidak berwenang sehingga aplikasi tidak dapat digunakan Password aplikasi di ketahui oleh pihak yang tidak berwenang

Aset Kritis	Sumber Ancaman	Ancaman
	Permasalahan Sistem	**Gangguan** Listrik Padam, banjir, peristiwa eksternal yang dapat mengakibatkan penolakan akses Serangan virus terhadap aplikasi Kegagalan operasional software
	Permasalahan lain	-
Sistem Rekaman Data	Aktor Manusia yang menggunakan jaringan	-
	Aktor Manusia menggunakan Akses Fisik	**Penyingkapan, Modifikasi** Data dibaca oleh pihak yang tidak berwenang Data diubah oleh pihak yang tidak berwenang Salah memasukkan data **Hilang/Rusak** Data Hilang/Rusak **Gangguan** Rusaknya media penyimpan data (Contoh : hardisk, CD, disket) Pencurian media penyimpan data (Contoh : hardisk, CD, disket)
	Permasalahan Sistem	-

Aset Kritis	Sumber Ancaman	Ancaman
	Permasalahan lain	Membicarakan isu mengenai permasalahan ini ke area publik
Sistem Informasi Akademik	Aktor Manusia yang menggunakan jaringan	**Penyingkapan, Modifikasi** Penyalahgunaan akses Terlalu banyak yang mengakses Masuknya Virus Kesalahan memasukkan data Serangan dari luar (DoS) Password aplikasi di ketahui oleh pihak yang tidak berwenang Perubahan konfigurasi aplikasi oleh pihak yang tidak berwenang sehingga aplikasi tidak dapat digunakan
	Aktor Manusia menggunakan Akses Fisik	**Penyingkapan, Modifikasi** Sharing Password **Hilang/Rusak** Pencurian kode program
	Permasalahan Sistem	**Gangguan** Konektivitas Ketidakstabilan jaringan area lokal akan menciptakan sebuah backlog Kegagalan operasional software Listrik Padam, banjir dan kejadian eksternal yang dapat mengakibatkan penolakan akses.
	Permasalahan lain	Membicarakan isu mengenai permasalahan ini ke area publik

Aset Kritis	Sumber Ancaman	Ancaman
Jaringan	Aktor Manusia yang menggunakan jaringan	**Penyingkapan, Modifikasi** Penyadapan Jaringan melalui aset jaringan seperti router, switch, dll
	Aktor Manusia menggunakan Akses Fisik	**Penyingkapan, Modifikasi** Akses firewall oleh pihak yang tidak berwenang Konfigurasi router oleh pihak yang tidak berwenang **Hilang/Rusak** Rusaknya aset jaringan seperti router, switch, dll Pencurian aset jaringan seperti router, switch, dll **Gangguan** Kesalahan dalam konfigurasi firewall, kabel jaringan (*human error*)
	Permasalahan Sistem	**Hilang/Rusak** Rusaknya modem karena kelebihan beban kerja
	Permasalahan lain	Rusaknya kabel oleh gigitan tikus Listrik Padam, banjir, peristiwa eksternal yang dapat mengakibatkan penolakan akses

Aset Kritis	Sumber Ancaman	Ancaman
Server	Aktor Manusia yang menggunakan jaringan	**Penyingkapan, Modifikasi** Penyadapan informasi penting dari Server melalui jaringan (Contoh : menggunakan ID *guess* melalui fasilitas telnet Serangan *hacker* pada server melalui jaringan
	Aktor Manusia menggunakan Akses Fisik	**Penyingkapan, Modifikasi** Password Server diketahui oleh orang lain Kesalahan Konfigurasi dan perawatan Server oleh staff **Hilang/Rusak** Rusaknya Server karena beban kerja yang terlalu tinggi Pencurian Server dan atau komponennya Kebakaran pada ruang server Rusaknya komponen server karena terbakar atau berkarat
	Permasalahan Sistem	Masuknya Virus Password Server diketahui oleh
	Permasalahan lain	Listrik Padam, banjir, peristiwa eksternal Membicarakan isu mengenai permasalahan ini ke area publik
PC	Aktor Manusia yang menggunakan jaringan	**Penyingkapan, Modifikasi** Penyadapan informasi penting dari PC melalui jaringan

Aset Kritis	Sumber Ancaman	Ancaman
	Aktor Manusia menggunakan Akses Fisik	**Penyingkapan, Modifikasi** Password PC diketahui oleh orang lain Kesalahan Konfigurasi PC **Hilang/Rusak** Pencurian PC Rusaknya PC karena kurang baiknya perawatan atau human error Kebakaran pada ruang PC
	Permasalahan Sistem	**Penyingkapan** Berbagi Jaringan **Hilang/Rusak** Kerusakan software Kerusakan Hardware **Gangguan** *malicious code*, Contohnya Virus, dll Tidak Tersedianya SDM
	Permasalahan lain	Listrik padam Bencana alam Penyalahgunaan internet

4.1.3 Mengidentifikasikan Kerentanan Infrastruktur

Identifikasi kerentanan infrastruktur dilakukan untuk memeriksa kelemahan komponen operasional utama (kerentanan teknologi) yang dapat mengakibatkan tindakan yang tidak sah terhadap aset kritis. Untuk mengidentifikasikan kerentanan yang ada harus dilakukan hal-hal berikut:

4.1.3.1 *System Of Interest, Access Path,* dan Komponen Utama

Mengidentifikasikan komponen utama untuk mengevaluasi kerentanan infrastruktur. Identifikasi komponen utama memberikan gambaran bagaimana FTIf mengelola kerentanan teknologi. Langkah yang dilakukan adalah dengan meninjau ancaman pada aset kritis dengan sumber ancamannya yang dilakukan oleh manusia dengan mengguanakan jaringan. Gambar 4.1 menunjukkan Peta Infrastruktur jaringan yang ada di FTIf. Gambar tersebut menunjukkan beberapa akses yang dapat dilakukan di FTIf. Komponen utama untuk PC adalah komponen server, komponen jaringan, komponen keamanan, Desktop workstation, laptops, Media penyimpanan data, dan wireless.

Berikut salah satu contoh tabel yang mengidentifikasikan komponen kelas utama yang ada di FTIf.

Tabel 4.4 Komponen utama untuk aset kritis

Aset Kritis	Komponen Kelas	Alasan
Jaringan	✓ Server	Semua sistem yang ada di jurusan disimpan disini, seperti sistem Elearning, monta, file sharing, dll
	✓ Komponen jaringan	Router – Jalan utama untuk mengakses secara internal
	✓ Komponen Keamanan	Firewall – Kunci keamanan untuk akses dari PC
	✓ DesLaptops	Digunakan untuk akses internal

Aset Kritis	Komponen Kelas	Alasan
	✓ Komponen Wireless	Digunakan untuk akses internal

Berikut adalah tabel system yang menarik dan komponen kelas utama untuk setiap aset kritis.

Tabel 4.5 *Systems of Interest* dan komponen kelas utama

Sistem Informasi Akademik	
System(s) of Interest	Sistem Informasi Akademik
Komponen kelas Utama	Personal komputer yang terhubung dengan jaringan internal, baik melalui kabel jaringan maupun wireless (termasuk laptops) Firewall Router Switch Server Sistem Informasi Akademik
Aplikasi Perkantoran	
System(s) of Interest	Aplikasi Perkantoran
Komponen kelas Utama	Personal computer (termasuk laptops) Firewall Router Switch

PC	
System(s) of Interest	Personal komputer, akan tetapi juga merupakan subsistem dari lain seperti Sistem Informasi Akademik, Elearning, dan aplikasi perkantoran
Komponen kelas Utama	Firewall Router Switch
Server	
System(s) of Interest	Server merupakan subsistem dari yang lain seperti Sistem Informasi Akademik, Elearning, dan aplikasi perkantoran.
Komponen kelas Utama	Personal komputer (termasuk laptops) Firewall Router Switch

4.1.3.2 *Tools* / Pendekatan Evaluasi Kerentanan

Setelah komponen utama dan *system of interest* telah diidentifikasikan, maka tahap selanjutnya adalah melakukan identifikasi *tool* atau pendekatan yang dapat digunakan untuk mengevaluasi komponen-komponen tersebut. Berikut adalah tools atau Pendekatan yang dipilih untuk mengevaluasi kerentanan.

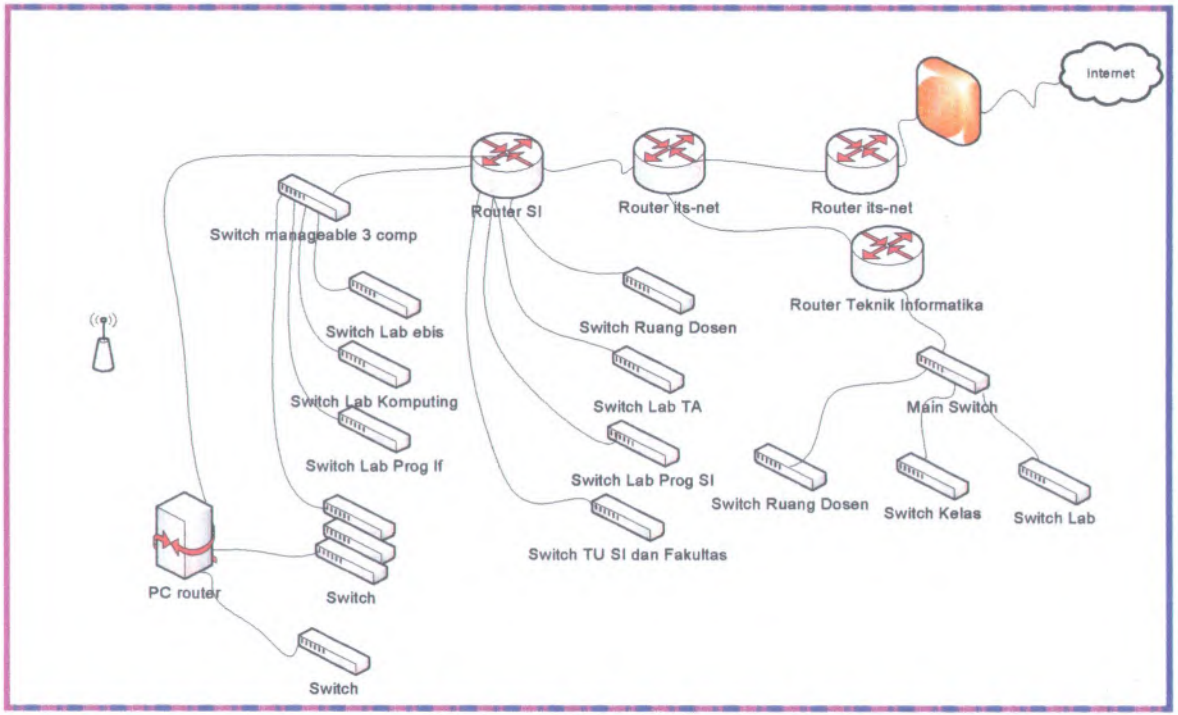
Tabel 4.6 Pendekatan evaluasi kerentanan

Komponen Kunci	IP Addresses[1]	Pendekatan Evaluasi Kerentanan	Tool	Alasan
PC	10.126.15.123 10.151.51.51 10.126.151.52	Staf IT/ Network administrator bertanggung jawab terhadap perlindungan data dan informasi yang ada pada suatu area perangkat komputer yang saling terkoneksi	Security Analysis Tools	Tool ini digunakan untuk mengetahui kerentanan software / hardware
			Firewall	Tool ini digunakan mengatur paket data yang diperbolehkan untuk di akses dari dan ke internet

4.1.3.3 Evaluasi Komponen Pilihan

Evaluasi komponen dilakukan dengan cara berikut. Pertama-tama dipilih komponen infrastruktur yang akan dievaluasi kerentananya. Setelah itu tools yang dipilih dijalankan, dan hasilnya dianalisa dan dibuat rangkuman.

[1] Bukan IP address sebenarnya



Gambar 4.1 Peta Infrastruktur FTIf

4.1.3.3.1 *Hasil Komponen yang dievaluasi*

Berdasarkan dari komponen yang telah dipilih untuk dievaluasi kerentanannya, hanya ada dua sistem yang berhasil diidentifikasikan untuk dievaluasi, yaitu Desktop PC (client) dan firewall. Tabel 4.7 meringkas secara aktual komponen utama yang telah dievaluasi.

Tabel 4.7 Sistem yang telah dievaluasi kerentanannya

Sistem yang telah diidentifikasikan	Telah dievaluasi (Y / T)
Desktop PC (client)	Y

4.1.3.3.2 *Hasil Analisis Evaluasi Kerentanan*

Hasil analis evaluasi kerentanan menjelaskan mengenai komponen IP address yang telah dipilih beserta tools/metode/pendekatan yang digunakan untuk mengevaluasi kerentanan. Tabel 4.8 merupakan ringkasan hasil dari evaluasi kerentanan untuk komponen yang telah dipilih.

Tabel 4.8 Ringkasan dari evaluasi kerentanan

Komponen Kelas	Komponen IP Address yang dipilih	Tool/Metode/ Pendekatan	Ringkasan Kerentanan
Desktop PC (clients)– Windows XP	10.126.15.123 10.151.51.51 10.126.151.52	Security Analysis Tools	software yang digunakan pada IP 10.151.51.51 perlu diupgrade

		Firewall	Layanan jaringan (*file sharing)* pada IP 10.151.51.51 tidak boleh untuk diakses karena Virus trojan menyerang komputer tsb dan terjadi penyalahgunaan

Berikut ini merupakan tabel 4.9 merupakan ringkasan dari tindakan dan rekomendasi yang diberikan setelah evaluasi kerentanan terhadap infrastruktur telah dilaksanakan.

Tabel 4.9 Tindakan dan Rekomendasi

Rekomendasi dan tindakan untuk kerentanan teknologi yang dialamatkan
Masalah konfigurasi pada komputer kurang dapat dijalankan dengan baik. Hal ini mengindikasikan bahwa staf IT kurang dapat bersaing dengan revisi terbaru. Untuk itu perlu dilakukan penyelidikan lebih lanjut ke dalam proses TI yang digunakan untuk membuat dan memelihara PC yang diperlukan dan menentukan apakah berbagai konfigurasi adalah warisan atau tidak diberbolehkannya perubahan.
Manajemen kerentanan tidak benar-benar dilakukan dengan baik. Staf IT mengakui bahwa mereka tidak selalu dapat menjalankan scanner. Untuk itu manajemen kerentanan harus diinvestigasi dan kelemahan prosedur dikoreksi. Sebuah rencana dibuat untuk meningkatkan pengetahuan dan keterampilan dari staf IT.

4.1.4 Membuat Perencanaan dan Strategi Keamanan

Pada tahap ini dilakukan pendefinisian risiko terkait dengan aset kritis, membuat rencana mitigasi untuk risiko tersebut, dan mengembangkan strategi perlindungan.

4.1.4.1 Analisis Risiko

Analisis risiko ini dilakukan dengan mengkaji semua informasi yang diperoleh dari proses sebelumnya dan membuat profil risiko untuk setiap aset kritis. Profil risiko merupakan perluasan dari profil ancaman dengan menambahkan pengukuran kualitatif dan kuantitatif terhadap dampak pada organisasi untuk setiap kemungkinan ancaman yang terjadi.

Hasil dari tahap ini adalah mendeskripsikan dampak untuk setiap ancaman pada organisasi , membuat kriteria evaluasi risiko dan memberikan nilai terhadap setiap dampak yang terjadi pada aset kritis.

4.1.4.1.1 *Deskripsi Nilai dan Dampak Risiko*

Setiap hasil dari profil ancaman mempunyai satu atau lebih dampak pada organisasi. Tabel 4.10 menjelaskan deskripsi kontekstual dampak yang ditimbulkan dari setiap ancaman. Beberapa Ancaman dapat mempunyai beberapa dampak dan mempunyai nilai yang berbeda-beda. Nilai dampak ditentukan berdasarkan definisi kriteria evaluasi dampak risiko (lihat tabel 4.11).

- ✓ Probabilitas : Peluang munculnya ancaman
  - Rendah : Frekuensi ancaman kurang dari 1 kali / tahun
  - Sedang : Frekuensi ancaman kurang dari 1-5 kali / tahun
  - Tinggi : Frekuensi ancaman lebih dari 5 kali / tahun
- ✓ Dampak

  Rendah : Tingkat ancaman terendah
  Sedang : Tingkat ancaman sedang
  Tinggi : Tingkat ancaman tinggi

Tabel 4.10 Nilai Probabilitas dan Dampak Risiko

Aset Kritis	Ancaman	Probabilitas			Dampak			
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya
Data Keuangan	Data dibaca oleh pihak yang tidak berwenang	✓	-	-	-	-	L	-
	Data diubah oleh pihak yang tidak berwenang	-	✓	-	L	-	L	-
	Rusaknya media penyimpan data (Contoh : hardisk, CD, disket)	-	✓	-	-	L	-	-
	Hilang/rusaknya dokumen	-	✓	-	L	L	L	-
Sistem Rekaman	Data dibaca oleh pihak yang tidak berwenang	✓	-	-	L	-	L	-

Aset Kritis	Ancaman	Probabilitas			Dampak			
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya
Data	Data diubah oleh pihak yang tidak berwenang	-	✓	-	L	-	-	-
	Rusaknya media penyimpan data (Contoh : hardisk, CD, disket)	-	✓	-	L	L	L	-
	Hilang/rusaknya dokumen		✓	-	-	L	L	-
Sistem Informasi Akademik	Penyalahgunaan akses	-	✓	-	-	-	M	-
	Terlalu banyak yang mengakses	-	✓	-	-	-	L	-
	Masuknya Virus	✓	-	-	-	-	M	-
	Kesalahan memasukkan data	✓	-	-	-	-	M	-

Aset Kritis	Ancaman	Probabilitas			Dampak			
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya
	Serangan dari luar (DoS)	✓	-	-	M	-	-	-
	Password aplikasi di ketahui oleh pihak yang tidak berwenang	✓	-	-	M	-	L	-
	Perubahan konfigurasi aplikasi oleh pihak yang tidak berwenang sehingga aplikasi tidak dapat digunakan	-	✓	-	L	-	M	-
	Sharing Password	-	✓	-	-	-	L	-
	Pencurian kode program	✓	-	-	-	M	-	-
	Konektivitas	-	✓	-	-	-	L	-

Aset Kritis	Ancaman	Probabilitas			Dampak			
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya
	Ketidakstabilan jaringan area lokal akan menciptakan sebuah backlog	✓	-	-	-	-	L	-
	Kegagalan operasional software	✓	-	-	-	-	M	-
	Listrik Padam, banjir dan kejadian eksternal yang dapat mengakibatkan penolakan akses.	✓			-			M
	Membicarakan isu mengenai permasalahan ini ke area publik	✓	-	-	L	-	-	-
Aplikasi Perkantoran	Kesalahan memasukkan data	✓	-	-	-	-	L	-
	Serangan virus terhadap aplikasi	✓	-	-	-	-	L	-

Aset Kritis	Ancaman	Probabilitas			Dampak			
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya
	Penyalahgunaan akses oleh pihak yang tidak berwenang	✓	-	-	-	-	L	-
	Password aplikasi di ketahui oleh pihak yang tidak berwenang	✓	-	-	-	-	L	-
	Pencurian data keuangan.	✓	-	-	M	-	L	-
	Listrik Padam, banjir dan kejadian eksternal yang dapat mengakibatkan penolakan akses.	-	✓	-	-	-	L	-
	Kegagalan operasional software	✓	-	-	-	-	L	-
	Membicarakan isu mengenai permasalahan ini ke area publik	✓	-	-	L	-	-	-

Aset Kritis	Ancaman	Probabilitas			Dampak			
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya
Jaringan	Konfigurasi komponen fisik jaringan oleh pihak yang tidak berkepentingan	✓	-	-	-	-	L	-
	Penyadapan informasi melalui jaringan melalui router, switch, WLAN dll	✓	-	-	-	-	L	-
	Rusaknya komponen fisik jaringan seperti router, switch, dll	-	✓	-	-	L	L	-
	Pencurian komponen fisik jaringan seperti router, switch, dll	✓	-	-	-	L	-	-

Aset Kritis	Ancaman	Probabilitas			Dampak			
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya
	Rusaknya modem karena kelebihan beban kerja	✓	-	-	-	L	L	-
	Kesalahan dalam konfigurasi firewall (human error)	✓	-	-	-	-	L	-
	Penyalahgunaan akses jaringan	-	✓	-	-	-	L	-
Server	Penyalahgunaan akses	✓	-	-	-	-	L	-
	Masuknya Virus	✓	-	-	-	-	L	-
	Pencurian Server dan atau komponennya	✓	-	-	-	M	L	M
	Kesalahan Konfigurasi dan perawatan Server oleh staf	✓	-	-	-	-	L	-

Aset Kritis	Ancaman	Probabilitas			Dampak			
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya
	Password Server diketahui oleh orang lain	✓	-	-	L	-	L	-
	Penyadapan informasi penting dari Server melalui jaringan (Contoh : menggunakan ID guess melalui fasilitas telnet	✓	-	-	-	-	L	-
	Kebakaran pada ruang server	✓	-	-	-	M	M	M
	Rusaknya komponen server karena terbakar atau berkarat	✓	-	-	-	L	L	L
	Rusaknya Server karena beban kerja yang terlalu tinggi	✓	-	-	-	-	L	L

Aset Kritis	Ancaman	Probabilitas			Dampak			
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya
	Serangan hacker pada server melalui jaringan	✓	-	-	-	-	L	-
	Matinya aliran listrik	-	✓	-	-	-	L	-
PC	Pencurian PC	✓	-	-	-	M	L	-
	Password PC diketahui oleh orang lain	✓	-	-	-	-	L	-
	Kesalahan Konfigurasi PC	✓	-	-	-	-	L	-
	Rusaknya PC karena kurang baiknya perawatan atau human error	✓	-	-	-	L	L	-
	Kebakaran pada ruang PC	✓	-	-	-	L	L	L

Aset Kritis	Ancaman	Probabilitas			Dampak			
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya
	Pengguna menghapus file atau software yang ada,	✓	-	-	-	-	L	-
	Kerusakan software	✓	-	-	-	-	L	-
	Masuknya Virus	-	-	✓	-	-	L	-
	Listrik padam	-	✓	-	-	-	L	-
	Bencana alam	✓	-	-	-	M	L	M
	Penyalahgunaan akses	✓	-	-	-	-	L	-

4.1.4.1.2 *Kriteria Evaluasi untuk dampak risiko*

Setelah deskripsi dampak untuk hasil ancaman telah lengkap, maka kriteria evaluasi dampak harus didefinisikan (Tabel 4.11). Berikut adalah area yang menjadi pertimbangan ketika menentukan jika dampak tinggi, sedang atau rendah:

Reputasi/ Kepercayaan pelanggan

Produktifitas

Keuangan

Lainnya

Tabel 4.11 Kriteria Evaluasi untuk Dampak Risiko

Dampak Area	Tinggi	Sedang	Rendah
Reputasi/Kepercayaan Pelanggan	Reputasi perusahaan rusak dan tidak bisa diperbaiki.	Reputasi Organisasi terganggu diperlukan upaya dan biaya untuk memperbaiki reputasi perusahaan.	Dampak terhadap reputasi sangat rendah; hanya sedikit atau bahkan tidak ada upaya yang diperlukan untuk mengatasinya.
		Melanggar Undang-	Melanggar Undang-

Dampak Area	Tinggi	Sedang	Rendah
		Undang Privasi Publik(penyingkapan kepada personil)	Undang Privasi Non-Publik(penyingkapan kepada personil)
Produktifitas	40% atau lebih kenaikan jam kerja diperlukan setidaknya 10% dari staf umum untuk dua hari	Penambahan pekerjaan 10-40% dalam sehari.	Mengganggu Staf kurang dari satu hari dan tidak ada pengukuran upaya peningkatan pekerjaan.
Keuangan	Terjadi penambahan biaya operasi tahunan lebih besar 15%	Terjadi penambahan biaya operasi tahunan setidaknya 2-15 %	Terjadi penambahan biaya operasi tahunan setidaknya 2 %
Lainnya	Tidak dapat melacak kinerja fasilitas atau layanan yang akurat	Kerusakan fasilitas bangunan memerlukan relokasi sementara.	Kerusakan fasilitas hanya memerlukan sedikit perbaikan

4.1.4.1.3 *Kuantifikasi Risiko*

Berdasarkan analisis terhadap data-data yang diperoleh sebelumnya, maka kuantifikasi risiko yang mungkin terjadi pada FTIf dapat dilakukan. Berikut ini adalah rumus kuantifikasi pada risiko.

Risiko = Probabilitas X Dampak

- ✓ Probabilitas : Peluang munculnya ancaman
  - Rendah : Frekuensi ancaman kurang dari 1 kali / tahun (Skor:0.32)
  - Sedang : Frekuensi ancaman kurang dari 1-5 kali / tahun (Skor:0.64)
  - Tinggi : Frekuensi ancaman lebih dari 5 kali / tahun (Skor:0.96)

- ✓ Dampak
  Rendah : Tingkat ancaman terendah (Skor:0.32)
  Sedang : Tingkat ancaman sedang (Skor:0.64)
  Tinggi : Tingkat ancaman tinggi (Skor:0.96)

Aset Kritis	Ancaman	Probabilitas			Dampak				Hasil
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya	
Data Keuangan	Data dibaca oleh pihak yang tidak berwenang	0.32	-	-	0.32	-	0.32	-	0.20
	Data diubah oleh pihak yang tidak berwenang	-	0.64	-	0.32	-	0.32	-	0.40
	Rusaknya media penyimpan data (Contoh : hardisk, CD, disket)	-	0.64	-	-	0.32	-	-	0.20
	Hilang/rusaknya dokumen	-	0.64	-	0.32	0.32	0.32	-	0.60
Sistem Rekaman	Data dibaca oleh pihak yang tidak berwenang	0.32	-	-	0.32	-	0.32	-	0.20

Aset Kritis	Ancaman	Probabilitas			Dampak				Hasil
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya	
Data	Data diubah oleh pihak yang tidak berwenang	-	0.64	-	0.32	-	-	-	0.20
	Rusaknya media penyimpan data (Contoh : hardisk, CD, disket)	-	0.64	-	0.32	0.32	0.32	-	0.60
	Hilang/rusaknya dokumen		0.64	-	-	0.32	0.32	-	0.40
Sistem Informasi Akademik	Penyalahgunaan akses	-	0.64	-	-	-	0.64	-	0.40
	Terlalu banyak yang mengakses	-	0.64	-	-	-	0.32	-	0.20
	Masuknya Virus	0.32	-	-	-	-	0.64	-	0.20

Aset Kritis	Ancaman	Probabilitas			Dampak				Hasil
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya	
	Kesalahan memasukkan data	0.32	-	-	-	-	0.64	-	0.20
	Serangan dari luar (DoS)	0.32	-	-	0.64	-	-	-	0.20
	Password aplikasi di ketahui oleh pihak yang tidak berwenang	0.32	-	-	0.64	-	0.32	-	0.30
	Perubahan konfigurasi aplikasi oleh pihak yang tidak berwenang sehingga aplikasi tidak dapat digunakan	-	0.64	-	0.32	-	0.64	-	0.60
	Sharing Password	-	0.64	-	-	-	0.32	-	0.20
	Pencurian kode program	0.32	-	-	-	0.64	-	-	0.20
	Konektivitas	-	0.64	-	-	-	o.32	-	0.20

Aset Kritis	Ancaman	Probabilitas			Dampak				Hasil
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya	
	Ketidakstabilan jaringan area lokal akan menciptakan sebuah backlog	0.32	-	-	-	-	0.32	-	0.10
	Kegagalan operasional software	0.32	-	-	-	-	0.64	-	0.20
	Listrik Padam, banjir dan kejadian eksternal yang dapat mengakibatkan penolakan akses.	0.32	-	-	-	-	-	0.64	0.20
	Membicarakan isu mengenai permasalahan ini ke area publik	0.32	-	-	0.32	-	-	-	0.10

Aset Kritis	Ancaman	Probabilitas			Dampak				Hasil
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya	
Aplikasi Perkantoran	Kesalahan memasukkan data	0.32	-	-	-	-	0.32	-	0.10
	Serangan virus terhadap aplikasi	0.32	-	-	-	-	0.32	-	0.10
	Penyalahgunaan akses oleh pihak yang tidak berwenang	0.32	-	-	-	-	0.32	-	0.10
	Password aplikasi di ketahui oleh pihak yang tidak berwenang	0.32	-	-	-	-	0.32	-	0.10
	Pencurian data keuangan.	0.32	-	-	0.64	-	0.32	-	0.30

Aset Kritis	Ancaman	Probabilitas			Dampak				Hasil
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya	
	Listrik Padam, banjir dan kejadian eksternal yang dapat mengakibatkan penolakan akses.	-	0.64	-	-	-	0.32	-	0.20
	Kegagalan operasional software	0.32	-	-	-	-	0.32	-	0.10
	Membicarakan isu mengenai permasalahan ini ke area publik	0.32	-	-	0.32	-	-	-	0.10
Jaringan	Konfigurasi komponen fisik jaringan oleh pihak yang tidak berkepentingan	0.32	-	-	-	-	0.32	-	0.10

Aset Kritis	Ancaman	Probabilitas			Dampak				Hasil
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya	
	Penyadapan informasi melalui jaringan melalui router, switch, WLAN dll	0.32	-	-	-	-	0.32	-	0.10
	Rusaknya komponen fisik jaringan seperti router, switch, dll	-	0.64	-	-	0.32	0.32	-	0.40
	Pencurian komponen fisik jaringan seperti router, switch, dll	0.32	-	-	-	0.32	-	-	0.10
	Rusaknya modem karena kelebihan beban kerja	0.32	-	-	-	0.32	0.32	-	0.20

Aset Kritis	Ancaman	Probabilitas			Dampak				Hasil
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya	
	Kesalahan dalam konfigurasi firewall (human error)	0.32	-	-	-	-	0.32	-	0.10
	Penyalahgunaan akses jaringan	-	0.64	-	-	-	0.32	-	0.20
Server	Penyalahgunaan akses	0.32	-	-	-	-	0.32	-	0.10
	Masuknya Virus	0.32	-	-	-	-	0.32	-	0.10
	Pencurian Server dan atau komponennya	0.32	-	-	-	0.64	0.32	0.64	0.50
	Kesalahan Konfigurasi dan perawatan Server oleh staf	0.32	-	-	-	-	0.32	-	0.10
	Password Server diketahui oleh orang lain	0.32	-	-	-	-	0.32	-	0.10

Aset Kritis	Ancaman	Probabilitas			Dampak				Hasil
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya	
	Penyadapan informasi penting dari Server melalui jaringan (Contoh : menggunakan ID guess melalui fasilitas telnet	0.32	-	-	-	-	0.32	-	0.10
	Kebakaran pada ruang server	0.32	-	-	-	0.64	0.64	0.64	0.60
	Rusaknya komponen server karena terbakar atau berkarat	0.32	-	-	-	0.32	0.32	0.64	0.40
	Rusaknya Server karena beban kerja yang terlalu tinggi	0.32	-	-	-	-	0.32	0.32	0.20
	Serangan hacker pada server melalui jaringan	0.32	-	-	-	-	0.32	-	0.10
	Matinya aliran listrik	-	0.64	-	-	-	0.32	-	0.20

Aset Kritis	Ancaman	Probabilitas			Dampak				Hasil
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya	
PC	Pencurian PC	0.32	-	-	-	0.64	0.32	-	0.30
	Password PC diketahui oleh orang lain	0.32	-	-	-	-	0.32	-	0.10
	Kesalahan Konfigurasi PC	0.32	-	-	-	-	0.32	-	0.10
	Rusaknya PC karena kurang baiknya perawatan atau human error	0.32	-	-	-	0.32	0.32	-	0.20
	Kebakaran pada ruang PC	0.32	-	-	-	0.32	0.32	0.32	0.30
	Pengguna menghapus file atau software yang ada,	0.32	-	-	-	-	0.32	-	0.10
	Kerusakan software	0.32	-	-	-	-	0.32	-	0.10
	Masuknya Virus	-	-	0.96	-	-	0.32	-	0.30

Aset Kritis	Ancaman	Probabilitas			Dampak				Hasil
		Rendah	Sedang	Tinggi	Reputasi	Keauangan	Produktifitas	Lainnya	
	Listrik padam	-	0.64	-	-	-	0.32	-	0.20
	Bencana alam	0.32	-	-	-	0.64	0.32	0.64	0.50
	Penyalahgunaan akses	0.32	-	-	-	-	0.32	-	0.1

Berdasarkan hasil analisis tersebut, diperoleh 2 macam ancaman yang memiliki tingkat nilai risiko terbesar, yaitu kehilangan/kerusakan, kebakaran dan bencana alam.

4.1.4.2 Mengembangkan Strategi Perlindungan

Proses ini melibatkan pengembangan, pengkajian, dan penerimaan strategi perlindungan organisasi secara menyeluruh, dan rencana mitigasi untuk risiko aset kritis.

Rencana perlindungan yang dibuat berdasarkan hasil analisis risiko difokuskan untuk meningkatkan keamanan seluruh organisasi FTIf. Strategi perlindungan ini Berikut adalah tabel strategi perlindungan yang dapat dikembangkan organisasi.

Strategi Perlindungan Organisasi	
Area Strategi	**Strategi**
Pelatihan, Pendidikan Kesadaran Keamanan	❖ Setiap pendatang baru seharusnya diberikan pelatihan tentang keamanan. ❖ Mengembangkan rencana jangka panjang untuk meningkatkan pelatihan bagi semua personil mengenai keaman secara berkala. ❖ Memberikan pelatihan tahunan keamanan fisik untuk semua pegawai, baik dosen maupun staf. ❖ Meningkatkan pelatihan bagi staf TI. Perbaharui rencana pelatihan dalam enam bulan ke depan termasuk pelatihan formal. ❖ Membuat *remainder* bagi para *user* agar peduli dengan masalah keamanan informasi.
Managemen Keamanan	❖ Mengalokasikan dana untuk sistem keamanan. ❖ Penganggaran tahunan harus

Strategi Perlindungan Organisasi	
Area Strategi	**Strategi**
	mempertimbangkan pengeluaran untuk kebutuhan di masa depan. ❖ Memperjelas peran dan tanggung jawab staf dan mengkomunikasikan ke semua bagian. ❖ Mulai *review* laporan keamanan dalam rapat.
Kebijakan Keamanan dan Peraturan	❖ Membuat Kebijakan dan prosedur keamanan pada semua tingkat dan aktif menegakkan mereka. ❖ Mendokumentasikan, menerbitkan, dan menyebarluaskan spesifikasi sanksi bagi pelanggaran terhadap semua personil. ❖ Memastikan bahwa undang-undang dan peraturan yang dibuat dipahami di semua tingkat organisasi ketika dirilis.
Manajemen Bisnis Berkelanjutan	❖ Membuat rencana terhadap kemungkinan terjadinya ancaman yang tidak diinginkan.
Keamanan Fisik	❖ Menerapkan kebijakan keamanan Fisik ❖ Review, update, dan menerapkan kebijakan pada workstation yang digunakan. ❖ Mengidentifikasi komponen

Strategi Perlindungan Organisasi	
Area Strategi	**Strategi**
	utama sistem lokasi dan memastikan keamanan fisik dari komponen dasar yang berulang (dari kedua staf internal dan eksternal organisasi). ❖ Instalasi perangkat lunak menerapkan prosedur keamanan di semua tingkatan dan memastikan mereka mengikuti baik secara internal maupun eksternal. ❖ Membentuk suatu mekanisme untuk keselamatan panitia untuk memastikan bahwa setiap bagian menyadari kerentanan fisik yang dikenal. Termasuk anggota TI di komite untuk membantu mereka berhubungan dengan sistem computer persyaratan keamanan fisik. ❖ Mendirikan dan berkomunikasi dengan jelas bahwa baik internal maupun eksternal personil yang bertanggung jawab untuk keamanan fisik.
Keamanan Teknologi Informasi	❖ Mengembangkan rencana jangka panjang untuk modernisasi keamanan

Strategi Perlindungan Organisasi	
Area Strategi	**Strategi**
	layanan terkait. Merekomendasikan ini kepada komite eksekutif. ❖ Membuat kebijakan dan prosedur untuk keamanan layanan teknologi informasi. ❖ Membicarakan keamanan dan persyaratan desain jaringan yang sekarang untuk melihat apakah ada cara untuk meningkatkan keamanan tanpa mempengaruhi efisiensi kerja. ❖ Menyelidiki penggunaan profil pengguna untuk membatasi akses ke informasi sensitif selama off-hari dan pekan. ❖ Menerapkan kebijakan password pengguna (misalnya, tidak membagi password).
Keamanan Pegawai	❖ Mendokumentasikan mekanisme dan prosedur untuk identifikasi dan pelaporan kejadian. ❖ Menyediakan "daftar panggilan" untuk menghubungi siapa dan apa yang dapat dilakukan. ❖ Memastikan penyebarluasan dan prosedur "daftar

Strategi Perlindungan Organisasi	
Area Strategi	**Strategi**
	panggilan" ke operator tingkat terendah, dan melakukan latihan kejadian periodik untuk memastikan kepatuhan. ❖ Kejadian manajemen belum ditetapkan.
Isu	❖ Tanpa adanya kebijakan keamanan kemungkinan untuk melakukan kesalahan semakin besar

4.1.4.2.1 *Perencanaan Mitigasi Untuk Aset Kritis*

Mitigasi adalah rencana yang khusus untuk risiko yang terkait dengan aset penting. Perencanaan mitigasi untuk setiap aset kritis direkomendasikan berdasarkan sumber ancaman di profil risiko yang telah dilakukan sebelumnya. Berikut adalah Keempat daerah sumber ancaman:

Aktor manusia yang menggunakan akses jaringan

Aktor manusia yang menggunakan akses Fisik

Permasalahan Sistem

Permasalahan Lain

Penekanan mitigasi ditempatkan pada aset yang dapat mengenali, menolak, dan mengurangi dari risiko ancaman jenis/daerah ini. Selain itu, beberapa ide untuk melacak risiko dan mitigasi rencana juga diidentifikasi. Tabel berikut ini menggambarkan rencana untuk mitigasi aset penting.

Perencanaan mitigasi risiko		
Aset kritis	**Sumber Ancaman**	**Tindakan**
Data Keuangan	Aktor manusia yang menggunakan akses jaringan	Tidak Relevan
	Aktor manusia yang menggunakan akses Fisik	o Mengadakan pelatihan pada pengguna. o Memberikan teguran kepada pelaku jika dijumpai adanya pelanggaran atau kesalahan yang dibuat. o Memberikan tempat penyimpanan yang aman. o Melakukan backup data
	Permasalahan Sistem	Tidak Relevan
	Permasalahan Lain	o Mengingatkan semua staf untuk tidak mendiskusikan permasalahan keamanan yang sensitif dan informasi publik di daerah.
Sistem Rekaman	Aktor manusia yang menggunakan akses jaringan	Tidak Relevan

Perencanaan mitigasi risiko		
Aset kritis	**Sumber Ancaman**	**Tindakan**
Data	Aktor manusia yang menggunakan akses Fisik	○ Mengadakan pelatihan pada pengguna. ○ Memberikan teguran kepada pelaku keuangan jika dijumpai adanya pelanggaran atau kesalahan yang dibuat. ○ Memberikan tempat penyimpanan yang aman. ○ Melakukan backup data
	Permasalahan Sistem	○ Tidak Relevan
	Permasalahan Lain	○ Mengingatkan semua staf untuk tidak mendiskusikan permasalahan keamanan yang sensitif dan informasi publik di daerah.
Sistem Informasi Akademik	Aktor manusia yang menggunakan akses jaringan	○ Pelatihan yang lebih baik bagi pengguna Aplikasi Sistem Informasi Akademik. ○ Menegakkan disiplin terhadap penggunaan password. ○ Penyalahgunaan password dilaporkan ○ Menambah ruang server ○ Menggunakan antivirus yang terupdate
	Aktor manusia yang menggunakan akses Fisik	○ Gunakan *screen saver* atau *time-out* secara default.

Perencanaan mitigasi risiko		
Aset kritis	**Sumber Ancaman**	**Tindakan**
	Permasalahan Sistem	○ Upgrade sistem hardware dan software komputer. Konfigurasi ulang untuk mendukung pengguna. ○ Update kemungkinan rencana.
	Permasalahan Lain	○ Menambahkan keamanan Bangunan FTIf pada rapat untuk melihat apakah sesuatu yang dapat dilakukan tentang *reconfiguring* kerja. ○ Mengingatkan semua staf untuk tidak mendiskusikan permasalahan keamanan yang tidak sensitif dan informasi publik di daerah.
	Pengukuran	○ Mulai ada laporan pelanggaran keamanan internal.
Aplikasi Perkantoran	Aktor manusia yang menggunakan akses jaringan	Tidak Relevan
	Aktor manusia yang menggunakan akses Fisik	○ Pelatihan yang lebih baik bagi pengguna Aplikasi Aplikasi Perkantoran ○ Menegakkan disiplin terhadap penggunaan password. ○ Penyalahgunaan password dilaporkan ○ Gunakan *screen saver* atau *time-out* secara default

Perencanaan mitigasi risiko		
Aset kritis	**Sumber Ancaman**	**Tindakan**
	Permasalahan Sistem	o Upgrade sistem hardware dan software komputer. Konfigurasi ulang untuk mendukung pengguna. o Install operator layar aktivitas pemberitahuan virus. o Update kemungkinan rencana.
	Permasalahan Lain	Tidak Relevan
	Pengukuran	o Mulai ada laporan pelanggaran keamanan internal
Jaringan	Aktor manusia yang menggunakan akses jaringan	o Melakukan monitoring secara terus menerus terhadap aktifitas jaringan.
	Aktor manusia yang menggunakan akses Fisik	o Pelatihan yang lebih baik bagi Staf jaringan o Melakukan perawatan yang terjadwal pada komponen jaringan
	Permasalahan Sistem	o Membatasi akses pada jaringan o Update kemungkinan rencana.
	Permasalahan Lain	o Melakukan perawatan yang terjadwal pada komponen jaringan.
	Pengukuran	o Mulai ada laporan pelanggaran keamanan internal
Server	Aktor manusia yang menggunakan akses jaringan	o Pelatihan yang lebih baik bagi staff IT o Membatasi koneksi lintas subnet

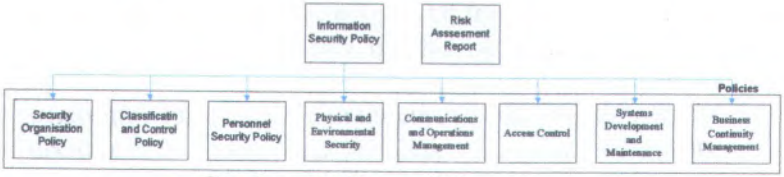
Perencanaan mitigasi risiko		
Aset kritis	**Sumber Ancaman**	**Tindakan**
	Aktor manusia yang menggunakan akses Fisik	○ Kebijakan keamanan server ○ Untuk mendeteksi kebakaran maka ruang server dipasang alat pendeteksi asap ○ Membatasi akses ke ruang server ○ Melakukan perawatan yang terjadwal pada komponen Server
	Permasalahan Sistem	○ Upgrade sistem hardware dan software komputer. Konfigurasi ulang untuk mendukung pengguna. ○ Membatasi akses ke server ○ Menegakkan disiplin terhadap penggunaan password ○ Penyalahgunaan password dilaporkan ○ Update kemungkinan rencana
	Permasalahan Lain	Tidak Relevan
	Pengukuran	○ Mulai ada laporan pelanggaran keamanan internal setelah semua orang telah mengingatkan kebijakan dan sanksi.

Perencanaan mitigasi risiko		
Aset kritis	**Sumber Ancaman**	**Tindakan**
PC	Aktor manusia yang menggunakan akses jaringan	○ Admin jaringan harus mengevaluasi pengguna pribadi dan profil pengguna, dan menggunakan informasi ini untuk meminimalkan akses jaringan PC selama "down time". Hal ini akan meminimalkan risiko jaringan ○ Memeriksa profil operator untuk tugas-tugas sesuai dengan yang dibutuhkan. ○ Password untuk mengkaji kerentanan semua system.
	Aktor manusia yang menggunakan akses Fisik	○ Adanya Kebijakan Keamanan Fisik ○ Melakukan perawatan yang terjadwal pada komponen PC ○ Untuk mendeteksi kebakaran maka fasilitas komputer dipasang alat pendeteksi asap ○ Memberikan Pelatihan pada Staff IT
	Permasalahan Sistem	○ Mendidik pengguna mencegah virus dari yang diperkenalkan ke dalam sistem. ○ Permintaan yang paling aktif virus deteksi perangkat lunak. ○ Install operator layar aktivitas pemberitahuan virus ○ Membatasi akses ke aplikasi

Perencanaan mitigasi risiko		
Aset kritis	**Sumber Ancaman**	**Tindakan**
	Permasalahan Lain	○ Menggunakan UPS untuk mengganti supply listrik ○ Membuat perencanaan bisnis berkelanjutan untuk mengatasi permasalahan yang diakibatkan oleh faktor alam.
	Pengukuran	○ Mulai ada laporan pelanggaran keamanan internal

4.2 Penyusunan Dokumen Kebijakan Keamanan Informasi

Berikut ini adalah Skema dokumen kebijakan keamanan informasi yang disusun berdasarkan ISO 17799. Dokumen kebijakan keamanan merupakan bagian dari implementasi sistem manajemen Keamanan Informasi yang dapat dikembangkan di FTIf ITS. Berdasarkan hasil analisis risiko menunjukkan bahwa FTIf saat ini belum memiliki kebijakan keamanan informasi. Oleh karena itu pada penelitian ini priotitas pembuatan sistem manajemen keamanan informasi FTIf saat ini adalah pada pembuatan kebijakan keamanan.



Gambar 4.2 Skema Dokumen

Analisis Risiko merupakan salah satu acuan yang mendasari dibuatnya kebijakan keamanan informasi, karena kebijakan yang akan dikembangkan merupakan kebijakan yang digunakan untuk mengamankan aset yang rentan/lemah terhadap risiko. Penjelasan terperinci mengenai analisis risiko telah dijelaskan pada sub-bab sebelumnya.

Sistematika penulisan dokumen kebijakan Sekuitas informasi secara umum adalah sebagai berikut:

1. Pendahuluan
   Berisi uraian mengenai tujuan, ruang lingkup dan definisi dan istilah yang digunakan dalam kebijakan keamanan informasi FTIf ITS.

2. Kebijakan Keamanan Organisasi
   Kebijakan ini mengatur tentang keamanan secara global pada organisasi, mengatur dan menjaga integritas sistem informasi internal terhadap keperluan pihak eksternal termasuk pengendalian terhadap pengolahan informasi

yang dilakukan oleh pihak ketiga (*outsourcing*). Dengan adanya kebijakan ini diharapkan dampak negatif yang timbul pada aktifitas tersebut dapat diminimalkan. Berikut adalah salah satu contoh kebijakan yang dibuat:
"*Pengelola harus menekan dampak negatif yang disebabkan oleh insiden yang terjadi pada aktifitas akademik dan non-akademik institut*"

3. Kebijakan Kontrol dan Klasifikasi Informasi
   Kebijakan ini memberikan perlindungan terhadap aset berdasarkan level proteksi yang ditentukan. Dengan adanya kebijakan ini diharapkan data dan informasi yang dihasilkan dapat terlindungi dan aman. Berikut adalah salah satu contoh kebijakan yang dibuat:
   "*Pengelolaan dan pemanfaatan data dan informasi akademik atau non akademik didasarkan atas kriteria informasi yang berkualitas*"

4. Kebijakan Keamanan personal
   Kebijakan ini mengatur tentang pengurangan risiko dari penyalahgunaan fungsi penggunaan atau wewenang akibat kesalahan manusia (*human error*), sehingga mampu mengurangi *human error* dan manipulasi data dalam pengoperasian sistem serta aplikasi oleh user, melalui pelatihan-pelatihan mengenai security awareness agar setiap user mampu menjaga keamanan informasi dan data dalam lingkup kerja masing-masing. Berikut adalah salah satu contoh kebijakan yang dibuat:
   "*Ketentuan pemanfaatan teknologi informasi untuk setiap user diatur sesuai dengan service level agreement yang ditetapkan*"

5. Kebijakan Keamanan Fisik
   Dalam kebijakan ini akan dibahas mengenai ancaman, kerawanan, dan tindakan antisipasi yang dapat dilakukan untuk mengamankan secara fisik seluruh sumber daya

organisasi dan informasi sensitif. Sumber daya ini mencakup seluruh personel, fasilitas tempat bekerja, data, peralatan, sistem pendukung, dan media yang digunakan untuk bekerja. Keamanan fisik sering mengacu pada ukuran-ukuran yang diambil untuk melindungi sistem, bangunan / gedung, dan infrastruktur

Keamanan fisik dapat dicapai melalui konstruksi fasilitas yang layak, perlindungan terhadap kerusakan dan kebakaran, mekanisme anti pencuri dan adanya prosedur keamanan yang diberlakukan. Keamanan fisik berhubungan dengan bagaimana orang dapat masuk secara fisik kedalam lingkungan organisasi, hal ini berbeda dengan keamanan komputer yang berhubungan dengan bagaimana orang dapat masuk kedalam lingkungan melalui port atau modem. Dengan pertimbangan diatas, maka salah satu contoh kebijakan keamanan fisik yang dapat dikembangkan adalah sebagai berikut:
"*Sambungan komunikasi yang vital, server pusat dan penting, serta komponen pokok lainnya harus terletak pada area yang aman secara fisik untuk mengurangi risiko pencurian, sabotase dan kerusakan*"

6. Manajemen Operasional dan komunikasi
menyediakan perlindungan terhadap infrastruktur sistem informasi melalui perawatan dan pemeriksaan berkala, serta memastikan ketersediaan panduan sistem yang terdokumentasi dan dikomunikasikan guna menghindari kesalahan operasional. Pada area ini ada beberapa kebijakan yang dapat dikembangkan, yaitu:
    1. Kebijakan Keamanan Server
    Tujuan dari keamanan server adalah untuk menetapkan standar konfigurasi dasar dari server jaringan yang dimiliki dan dioperasikan oleh FTIf. Pelaksanaan kebijakan server secara efektif akan

meminimalkan akses yang tidak memiliki wewenang terhadap teknologi dan informasi milik FTIf. Selain itu kebijakan keamanan server ini juga mencakup mengenai konfigurasi keamanan minimal yang dibutuhkan untuk semua router dan switch yang terhubung ke jaringan di FTIf.

Aspek keamanan data/informasi atau disebut juga keamanan virtual pada server menyangkut hal-hal sebagai berikut.

- Kontrol akses logikal, menyangkut apa, siapa dan bagaimana data diakses secara virtual. Contohnya seperti password untuk menentukan hak akses.
- Kontrol penyimpan, menyangkut berapa lama data disimpan dan jenis keamanan apa yang digunakan pada media penyimpan dan data yang disimpan. Contohnya sistem backup data yang dipakai dan enkripsi yang digunakan.
- Keamanan jaringan baik jaringan intranet maupun internet terkait dengan konfigurasi jaringan, hak akses jaringan, firewall, intrusion detection dan lainnya.
- Keamanan sistem terkait dengan sistem operasi yang digunakan.

Berikut adalah salah satu kebijakan keamanan server yang dibuat:

"*Data yang terdapat pada server akan di-back-up dalam jangka waktu tertentu*"

2. Kebijakan Backup Data dan Pemulihan

Backup data sangat diperlukan khususnya jika jaringan down, data hilang atau korup hingga user dan manajemen berteriak. Tidak semua data perlu dibackup, jadi ini penting untuk mengidentifikasi data yang kritis, penting dan dengan kata lain perlu dibuat prioritas mengenai apa yang perlu di backup. Saat ini backup data dilakukan oleh masing-masing pegawai

yang mempunyai tanggung jawab terhadap data tersebut. Berikut ini adalah salah satu contoh kebijakan keamanan server yang dapat dikembangkan:
"*Informasi pada setiap sistem harus di backup secara teratur pada CD atau media penyimpanan lainnya*"

7. Akses Kontrol
   Akses Kontrol adalah fitur keamanan yang mengontrol bagaimana pengguna dan sistem berkomunikasi dan berinteraksi dengan sumber daya dan sistem yang lain. Akses kontrol bertujuan untuk melindungi sistem dan sumber daya dari akses yang tidak berwenang dan menentukan tingkat autorisasi setelah prosedur autentikasi berhasil dilaksanakan. Kebijakan akses kontrol yang dibuat pada penelitian ini bertujuan untuk mengendalikan aktifitas user terhada aset informasi yang ada dalam organisasi. Berikut adalah salah satu contoh kebijakan password yang dibuat:
   "*Akses ke kantor, ruang telekomunikasi, server dan wilayah kerja yang berisi informasi sensitif harus dibatasi dan hanya diberikan kepada pengguna yang diijinkan.*"

8. Manajemen Bisnis Berkelanjutan
   siap menghadapi risiko yang akan ditemui didalam aktivitas lingkungan bisnis yang bisa mengakibatkan "*major failure*" atau risiko kegagalan yang utama ataupun "*disaster*" atau kejadian buruk yang tak terduga, sehingga diperlukan pengaturan dan manajemen untuk kelangsungan proses bisnis, dengan mempertimbangkan aspek manajemen bisnis berkelanjutan. Hal ini dikarenakan membangun dan menjaga keamanan sistem manajemen informasi akan terasa jauh lebih mudah dan sederhana dibandingkan dengan memperbaiki sistem

yang telah terdisintegrasi. Berikut adalah salah satu contoh kebijakan keamanan yang dapat dibuat.

"*Untuk mengantisipasi terjadinya bencana, perlu melakukan: Analisis risiko, Manajemen perencanaan, Pengujian perencanaan dan manajemen risiko.*"

4.3 Pemetaan (*Mapping*)

Setelah rancangan kebijakan keamanan informasi telah dibuat, langkah selanjutnya adalah melakukan pemetaan (*mapping*) berdasarkan prinsip *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan) sehingga rancangan kebijakan keamanan yang dibuat dapat sesuai dengan prinsip-prinsip tersebut.

Berikut adalah hasil pemetaan Kebijakan keamanan yang dibuat :

No	ISI DOKUMEN KSI	PRINSIP
1	**PENDAHULUAN**	
1.	Tujuan	Ketersediaan
2.	Ruang Lingkup	Kerahasiaan
3.	Definisi dan Istilah	Ketersediaan
2	**KEAMANAN ORGANISASI**	
1.	Pengelola harus menekan dampak negatif yang disebabkan oleh insiden yang terjadi pada aktifitas akademik dan non-akademik institut.	Ketersediaan, integritas
2.	Pengelola dapat memastikan ketersediaan dan menjaga kualitas layanan Teknologi Informasi pada tingkat terbaik.	Ketersediaan, integritas

3	**KONTROL DAN KLASIFIKASI INFORMASI**	
1.	Pengelolaan dan pemanfaatan data dan informasi institut didasarkan atas kriteria informasi yang berkualitas	Ketersediaan
2.	Kriteria informasi yang berkualitas	Ketersediaan
4.	**KEAMANAN PERSONAL**	
1	Ketentuan pemanfaatan teknologi informasi untuk setiap user diatur sesuai dengan service level agreement yang ditetapkan	Ketersediaan, Kerahasiaan
2	Administrator jaringan berhak membatalkan pemakaian fasilitas komputer dan komunikasi dengan alasan tertentu.	Ketersediaan, integritas
5	**FISIK DAN LINGKUNGAN**	
1	Sambungan komunikasi yang vital, server pusat dan penting, serta komponen pokok lainnya harus terletak pada area yang aman secara fisik untuk mengurangi risiko pencurian, sabotase dan kerusakan.	Ketersediaan
2	Instalasi sambungan komunikasi yang vital, server pusat dan penting, serta komponen pokok lainnya harus memperhatikan bahaya akses secara fisik, bahaya	Ketersediaan

	lingkungan, dan bahaya elektrik.	
3	Komputer portabel harus dilindungi oleh kabel kunci, ditempatkan di lemari terkunci atau diamankan oleh peralatan perlindungan pencuri ketika berada di lingkungan yang tidak dimonitor	Ketersediaan
6	**MANAJEMEN OPERASIONAL DAN KOMUNIKASI**	
6.1	**KEAMANAN SERVER**	
1	Semua server harus menetapkan system registerasi user	Ketersediaan, Kerahasiaan
2	User account pada server harus memiliki password yang memenuhi standar keamanan tersebut, serta habis masa berlakunya dan diperbaharui setiap enam bulan;	Ketersediaan, Kerahasiaan
3	Setiap server harus berada dalam pengawasan administrator; dan	Ketersediaan, Kerahasiaan
4	Data yang terdapat pada server akan di-back-up dalam jangka waktu tertentu.	Ketersediaan
6.2	**BACKUP DATA DAN PEMULIHAN**	
1	Informasi pada setiap sistem harus di *backup* secara teratur pada CD atau media penyimpanan lainnya.	Ketersediaan
2	Untuk multi-user dan sistem	Ketersediaan

	komunikasi, sistem administrator yang bertanggung jawab untuk melakukan *backup* berkala.	
3	Bila diminta, Divisi Teknologi Informasi yang harus menyediakan bantuan teknis untuk instalasi cadangan perangkat keras atau perangkat lunak.	Ketersediaan
4	Semua salinan *Backup* dari informasi kritis atau sensitif harus disimpan dalam sebuah wilayah yang telah disetujui dengan kontrol akses.	Ketersediaan
5	Salinan ini harus dipelihara semata-mata untuk tujuan memulihkan sistem berikut dari infeksi virus komputer, harddisk cacat atau masalah komputer lainnya.	Ketersediaan, Kerahasiaan
6	Sebuah rencana darurat harus dikembangkan untuk semua aplikasi yang menangani informasi penting. Informasi pemilik harus memastikan bahwa rencana ini cukup berkembang, sering *up-date* dan ditinjau secara berkala	Ketersediaan
7	**AKSES KONTROL**	
1	Akses ke kantor, ruang telekomunikasi, server dan wilayah kerja yang berisi	Ketersediaan, kerahasiaan, dan integritas

	informasi sensitif harus dibatasi dan hanya diberikan kepada pengguna yang diijinkan.	
2	Informasi sensitif selalu harus dilindungi terhadap pengungkapan tidak sah.	Ketersediaan, kerahasiaan
3	Hard-copy dokumen yang berisi informasi sensitif harus disimpan di lemari arsip terkunci.	Ketersediaan, kerahasiaan
4	Informasi sensitif harus diamankan di fasilitas terkunci selama non-jam kerja.	Ketersediaan
5	Layar komputer harus diposisikan agar tidak terlihat oleh orang lain.	Ketersediaan, Kerahasiaan
6	Setiap *user* dilarang untuk melakukan akses tanpa hak, atau mengakses di luar kewenangannya, atau memanipulasi data dan informasi, atau memanipulasi perangkat sistem informasi dan komunikasi yang telah disediakan;	Ketersediaan
7	Seorang *user* dari fasilitas komputer dan komunikasi FTIf memiliki hak privasi dan keamanan dari program dan data komputer miliknya;	Ketersediaan, kerahasiaan, integritas
8	Seorang *user* tidak diperbolehkan menggunakan	Ketersediaan, kerahasiaan

	fasilitas komputer dan komunikasi untuk mengganggu atau merugikan pihak lain, atau untuk mengganggu pekerjaan pihak lain tersebut dengan cara apapun. Contoh dari kegiatan mengganggu dan merugikan orang lain ini adalah pengiriman pesan yang bersifat menghina, menipu, mengancam pihak lain, mengandung unsur pornografi, ataupun pesan yang dapat mengganggu kelancaran komunikasi sistem (*spam*);	
9	Seorang *user* tidak diperbolehkan melanggar ketetapan dari persetujuan lisensi perangkat keras dan perangkat lunak tertentu;	Ketersediaan, kerahasiaan
10	Berhubungan dengan halaman *web* yang dibuat dan disimpan pada komputer ataupun fasilitas fakultas, seluruh informasi yang ditampilkan haruslah tidak menyalahi hak cipta pihak lain, termasuk artikel yang berhubungan dengan informasi tersebut. Lebih jauh, *user* yang memiliki *account* sebagai pengelola *web* harus bertanggung	Ketersediaan, kerahasiaan

	jawab atas informasi yang ditampilkan, termasuk halaman *web* yang disebutkan atau terhubung dengan *web* yang dibuat dan disimpan pada komputer tersebut;	
11	Informasi yang disimpan, dikutip, dihubungkan atau diproses dengan fasilitas komputer dan komunikasi universitas haruslah sesuai dengan ketentuan yang berlaku. Seorang *user* tidak diperbolehkan membuat materi visual ataupun materi cetak yang bertentangan dengan kaedah dan etika akademik;	Ketersediaan, kerahasiaan
12	Seorang *user* tidak diperbolehkan menggunakan fasilitas komputer atau komunikasi untuk kepentingan pihak tertentu yang bertujuan untuk mencari keuntungan ataupun bersifat komersial, kecuali diberi ijin secara tertulis oleh pejabat fakultas/jurusan yang berwenang;	Ketersediaan, kerahasiaan
13	Seorang *user* yang telah meminta ijin penggunaan fasilitas tertentu dan belum melakukan pembatalan penggunaan ijin tersebut	Ketersediaan, kerahasiaan

	masih dapat menggunakannya sampai batas waktu ijin tersebut berlaku;	
14	Berhubungan dengan 7.8 dengan ijin dari Dekan atau Ketua Jurusan, seorang administrator yang terkait dapat memeriksa seluruh *file* dalam komputer tersebut di atas dan mengawasi pemakaian komputer untuk menjamin bahwa tidak satupun peraturan dilanggar dan juga untuk menjaga keamanan dan keefektifan pemakaian fasilitas komputer dan komunikasi;	Ketersediaan, Kerahasiaan, dan integritas
15	Berhubungan dengan 7.6 dan 7.8 di atas, seorang administrator berwenang mengambil tindakan-tindakan yang dianggap perlu untuk memastikan penggunaan fasilitas komputer dan komunikasi tidak menyalahi peraturan-peraturan di atas. Tindakan tersebut harus dengan sepengetahuan atasannya, diantaranya adalah mengakses *user account* yang bukan milik pengakses, menghapus satu atau lebih *file*, membuat	Ketersediaan, Kerahasiaan, dan integritas

	back-up, dan/atau mengumpulkan material yang bukan milik pengakses;	
16	Administrator sistem teknologi informasi dan komunikasi harus memperhatikan hak pemakai (*user right*) dari pengguna system.	Ketersediaan
8	**MANAJEMEN BISNIS BERKELANJUTAN**	
1	Pengelola menjamin dan meyakinkan bahwa akan dilakukan pengembalian (*restore*) layanan Teknologi Informasi jika terjadi bencana.	Ketersediaan
2	Untuk mengantisipasi terjadinya bencana, perlu melakukan: Analisis risiko, Manajemen perencanaan, Pengujian perencanaan dan manajemen risiko.	Ketersediaan, integritas
3	Perlu dilakukan pengembangan Disaster Recovery Plan untuk menjamin adanya layanan kontinuitas teknologi informasi	Ketersediaan

BAB V
PENUTUP

Bab ini berisi mengenai simpulan dari rancangan kebijakan keamanan informasi yang telah dibuat dalam tugas akhir ini, dan dilengkapi dengan saran untuk pengembangan kebijakan keamanan informasi bagi perusahaan dan penelitian ke depan.

5.1 Simpulan

Simpulan yang dapat diambil dari pengerjaan tugas akhir ini adalah sebagai berikut:

1. Aset yang berperan dalam keamanan informasi yang harus dilindungi keamanannya di FTIf adalah data Keuangan, sistem rekaman data, aplikasi perkantoran, jaringan, server dan PC.
2. Berdasarkan dari hasil penilaian risiko menggunakan metode octave didapatkan bahwa ancaman yang memiliki nilai risiko terbesar, yaitu risiko kehilangan/kerusakan dan kebakaran. Proses penilaian risiko dijelaskan di bab 4.1.4.1.
3. Rancangan kebijakan keamanan informasi yang mengakomodasikan prinsip-prinsip *Confidentiality* (kerahasiaan), *Integrity* (integritas), dan *Availability* (ketersediaan) dapat dilakukan melalui penilaian risiko dan pemetaan. Proses perancangan kebijakan keamanan informasi secara keseluruhan dijelaskan pada bab 4.1 dan 4.2. Berikut penjelasan singkat mengenai prinsip-prinsip tersebut:
    1. *Confidentiality* (kerahasiaan) dimaksudkan untuk memastikan bahwa kebijakan keamanan informasi yang dibuat menjamin kerahasiaan data atau informasi.
    2. *Integrity (integritas)* dimaksudkan untuk memastikan bahwa kebijakan keamanan informasi yang dibuat menjamin keakuratan dan keutuhan informasi.
    3. *Availability (ketersediaan)* dimaksudkan untuk memastikan bahwa kebijakan keamanan informasi yang dibuat menjamin ketersediaan data saat dibutuhkan.

5.1 Saran

Beberapa hal yang diharapkan dapat dikembangkan di masa mendatang adalah sebagai berikut:

1) Pembuatan kebijakan keamanan informasi ini dibuat berdasarkan analisis risiko menggunakan metode OCTAVE yang hanya mencakup aset yang dianggap penting oleh organisasi sehingga dalam pengembangan selanjutnya diharapkan dapat dibuat kebijakan yang dapat mencakup semua aset yang ada dalam organisasi.
2) Kebijakan keamanan informasi yang dibuat masih dalam tahap pra implementasi sehingga perlu dikembangkan lagi dengan menambahkan metode pasca implementasi

DAFTAR PUSTAKA

[1] Rahardjo, Budi. 2000. Keamanan Sistem Informasi Berbasis Internet. Bandung:PT Insan Komunikasi/Infonesia

[2] Gordon, L., Loeb, M., Lucyshyn, W., & Richardson, R. 2006. CSI/FBI Computer Crime and Security Survey 2006. Computer and Security Institute, 11(1), 1-27.

[3] _____. Capaian Indikator dan Garis Besar Program Kerja (GBPK) FTIf ITS 2007-2011. Kampus ITS Sukolilo, Surabaya. 2009.

[4] Mcleod, R dan Schell, G.P.2007. Management Information System. Prentice Hall.

[5] Wikipedia. Keamanan Informasi <*http://id.wikipedia.org/wiki/Keamanan_informasi*> [8 Oktoberr 2008 jam 13.05 WIB]

[6] Syafrizal, Melvin. 2008. Information Security Management Sistem (ISMS) Menggunakan ISO/IEC 27001:2005. STIMIK AMIKOM YOGYAKARTA.

[7] Whitmann, E. M dan Mattord, J.H. 2006. Management of Information System. Course Technology.

[8] PMII Komisariat UNDIP. Pengertian Kebijakan <*http://pmiikomundip.wordpress.com/2008/06/06/kebijakan-dan-kemiskinan/*>

[9] NIST SP 800-53, Revision 1, "Recommended Security Controls for Federal Information Systems". 2006.

[10] Plasma media. Keamanan Informasi.<http://www.plasmedia.com/secpolicy.htm>

[11] Wikipedia. Keamanan Informasi <*http://id.wikipedia.org/wiki/Keamanan_informasi*> [8 Oktober 2008 jam 13.05 WIB]

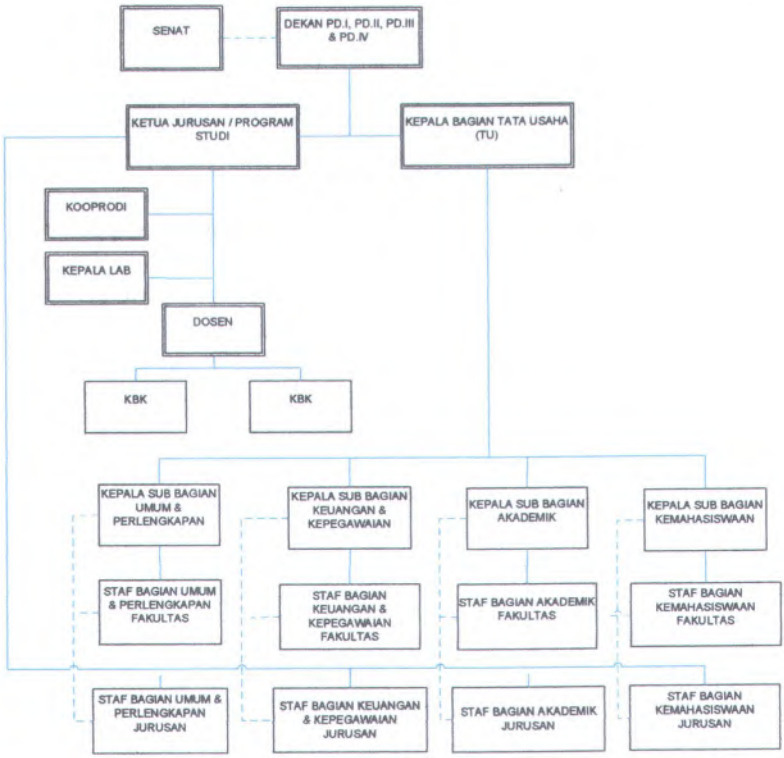
[12] M, Pyka dan P, Januszkiewicz. 2006."The OCTAVE methodology as a risk analysis tool for business resources". Proceedings of the International Multiconference on Computer Science and Information Technology, pp. 485 – 497. Academy of Business in Dąbrowa Górnicza: Poland

[13] ISO/IEC 17799 Information technology – Code of practice for information security management, Reference number ISO/IEC 17799:2002.

[14] Jacquelin Bisson, CISSP & René Saint-Germain. Mengimplementasi kebijakan keamanan dengan standar BS7799 /ISO17799 untuk pendekatan terhadap informasi keamanan yang lebih baik. White Paper, <http://202.57.1.181/~download/linux_opensource/artikel+tutorial/general_tutorials/wp_iso_id.pdf>

LAMPIRAN A
Pengumpulan Data dan Informasi

LAMPIRAN A-1
Struktur Organisasi



Fakultas Teknologi Informasi (FTIf) memiliki 2 (dua) jurusan S1 dan 1(satu) program studi S2 yang secara structural dipimpin oleh seorang Dekan yang dibantu dekan Pembantu I (Bidang Akademik), Pembantu Dekan II (Bidang Administrasi Keuangan dan Kepegawaian), Pembantu Dekan III (Bidang Kemahasiswaan) dan Pembantu Dekan IV (bidang Kerjasama, Alumni, Hukum dan Komunikasi) Dibawah Fakultas terdapat jurusan terdapat ketua jurusan yang diketuai seorang ketua jurusan dibantu sekretaris jurusan dan Koordinator Ruang Baca Fakultas. ketua jurusan membawahi koordinator program studi yang dibantu oleh sekretaris koordinator program studi. Selain itu ketua jurusan juga membawahi koorsinator bidang keahlian,

kepala laboratorium, Koordinator praktikum, Kepala Seksi Pengajaran, dan Kepala Seksi Kerja Praktek.

Sebagai unsur penunjang administrasi terdapat tata usaha fakultas dibawah koordinasi Kepala Bagian (KaBag) yang membawahi 3 Kepala Sub Bagian (KaSubBag), yaitu Kasub-bag Akademik, Kasub-bag kemahasiswaan dan Kasub-bag umum. Tugas dan tanggung jawab pimpinan dalam struktur organisasi fakultas diatur dan ditetapkan sesuai dengan Surat Keputusan Menteri Pendidikan Nasional No 109/0/202 tanggal 12 juli 2002.

Tugas dan tanggung jawab pimpinan dalam struktur organisasi diatur dan ditetapkan dalam organisasi dan tata kelola (OTK) ITS sesuai dengan Kepmendikbud RI No 0186/0/1995 dan statuta ITS Kepmendikbud No. 0443/0/1992. Dan struktur organisasi dan tata kelola Fakultas Teknologi Informasi (FTIf) ITS telah diatur dalam bab II Garis Besar Program Kerja (GBPK) FTIf-ITS tahun 2007-2011. Berikut adalah uraian tugas dan tanggung jawab yang diberikan:

- Dekan
  - Membuat kebijakan yang terkait dengan program kerja dan keuangan di tingkat facultas
  - Menerima laporan keuangan dari pejabat pembuat komitmen Facultas
  - Melakukan verifikasi terhadap kebenaran laporan keuangan tsb
  - Memberikan teguran kepada pelaku keuangan jika dijumpai adanya pelanggaran atau kesalahan yang dibuat.
- PD I

  Mempunyai tugas membantu Dekan dalam memimpin pelaksanaan pendidikan, penelitian dan pengabidian masyarakat.
- PD II

  Mempunyai tugas membantu Dekan dalam pelaksanaan kegiatan dibidang keuangan dan administrasi umum.
- PD III

Mempunyai tugas membantu Dekan dalam pelaksanaan kegiatan dibidang pembinaan serta layanan kesejahteraan masyarakat.

- PD IV
  Mempunyai tugas membantu Dekan dalam pelaksanaan kegiatan dibidang kerjasama, alumni, hukum dan komunikasi.
- Bagian Tata Usaha
  Mempunyai tugas melaksanakan administrasi pendidikan, keuangan, dan kepegawaian, umum, perlengkapan, dan kemahasiswaan.
- Ketua Jurusan
  Mempunyai tugas melaksanakan pendidikan akademik dan /atau profesional dalam sebagian atau satu cabang ilmu pengetahuan dan teknologi. Dalam melaksanakan tugas, ketua jurusan dibantu oleh sekretaris jurusan
- Kepala Lab
  Mempunyai tugas melakukan kegiatan dalam cabang ilmu pengetahuan, teknologi, dan/atau kesenian tertentu sebagai penunjang pelaksanaan tugas pokok jurusan sesuai dengan ketentuan bidang yang bersangkutan.
- Kepala Sub Bagian Pendidikan
  Mempunyai tugas melakukan administrasi pendidikan.
- Kepala Sub Bagian Keuangan dan Kepegawaian
  Mempunyai tugas melakukan administrasi keuangan dan kepegawaian.
- Kepala Sub Bagian Umum dan Perlengkapan
  Mempunyai tugas melakukan urusan tata usaha rumah tangga, dan perlengkapan.
- Kepala Sub Bagian Kemahasiswaan
  Mempunyai tugas melakukan administrasi kemahasiswaan dan alumni.

LAMPIRAN A-2
Data Inventarisasi FTIf

URAIAN	SATUAN	KUANTITAS	KLASIFIKASI
KOMPUTER PC LAB	BUAH	350	FISIK
KOMPUTER PC DOSEN	BUAH	50	FISIK
KOMPUTER PC ADMINISTRASI	BUAH	21	FISIK
KOMPUTER KELAS	BUAH	12	FISIK
KOMPUTER SERVER	BUAH	27	FISIK
NOTEBOOK	BUAH	38	FISIK
LOCAL AREA NETWORK (LAN)	BUAH	3	FISIK
PRINTER	BUAH	34	FISIK
SCANNER	BUAH	6	FISIK
COMPUTER COMPATIBLE	BUAH	4	FISIK
ROUTER	BUAH	11	FISIK
HUB	BUAH	47	FISIK
MODEM	BUAH	6	FISIK
JARINGAN KOMPUTER		1	LAYANAN
JARINGAN ADSL			LAYANAN
JARINGAN TELEPON DI BAWAH TANAH	UNIT	1	LAYANAN

LAMPIRAN A-3
Hasil Wawancara & Survey

Organisasi	:	Fakultas Teknologi Informasi ITS
Nama Pejabat	:	Mustiko Adji, SE
Jabatan	:	KaBag TU Fakultas Teknologi Informasi
Tanggal	:	15 Juni 2009
Topik	:	Identifikasi Aset dan Kebutuhan Keamanan.
Surveyor	:	Rachmawati F.

No	Pertanyaan
1.	Apa aset Penting dalam organisasi anda? Sebutkan 5 aset penting dan berikan alasan mengapa anda memilih aset tersebut? a. Informasi – data terdokumentasi (elektronik/non-elektronik) atau properti intelektual yang digunakan untuk mencapai misi perusahaan. Adapun yang termasuk aset informasi dalam organisasi adalah informasi mahasiswa, informasi nilai, informasi keuangan, informasi b. System – Sistem informasi yang memproses dan menyimpan informasi. Sistem adalah kombinasi dari aset informasi, hardware dan software. Beberapa mesin, clint, server atau jaringan dapat dipertimbangkan sebagai sistem. c. Software – aplikasi software (Sistem operasi, aplikasi database, software jaringan, aplikasi perkantoran, aplikasi lainnya) d. Hardware – Peralatan fisik teknologi informasi (workstations, servers, dll) e. SDM – orang-orang dalam perusahaan yang memiliki skill khusus, pengetahuan, dan pengalaman yang sulit dicari penggantinya.
- Kinerja SDM - Sistem Rekaman Data	

- Informasi, Con: Rapat Yudisium/Pra Yudisium, Nilai TOEFL
- SIM Akademik → Kontinuitas
- Penilaian tentang Akreditasi Dosen
- Aplikasi Perkantoran

2. Kebutuhan keamanan apa sajakah yang digunakan untuk aset tersebut? Berikan penjelasannya!

Aset	Ketersediaan	Integritas	Kerahasiaan
Kinerja SDM	Ada	Ada	Tidak
Sistem rekaman Data	Ada	Ada	Ada
Informasi	Ada	Ada	Ada
Sistem Informasi Akademik	Ada	Ada	Ada
Penilaian tentang akreditasi dosen	Ada	Ada	Ada

Organisasi	:	ITS
Nama Pejabat	:	Yudhi Purwananto, S.Kom. M.Kom.
Jabatan	:	KaJur Teknik Informatika FTIf
Tanggal	:	25 Maret 2009
Topik	:	Identifikasi Aset dan Kebutuhan Keamanan.
Surveyor	:	Rachmawati F.

No	Pertanyaan
1.	Apa aset Penting dalam organisasi anda? Sebutkan 5 aset penting dan berikan alasan mengapa anda memilih aset tersebut? a. Informasi – data terdokumentasi (elektronik/non-elektronik) atau properti intelektual yang digunakan untuk mencapai misi perusahaan. Adapun yang termasuk aset informasi dalam organisasi adalah informasi mahasiswa, informasi nilai, informasi keuangan, informasi b. System – Sistem informasi yang memproses dan menyimpan informasi. Sistem adalah kombinasi dari aset informasi, hardware dan software. Beberapa mesin, clint, server atau jaringan dapat dipertimbangkan sebagai sistem. c. Software – aplikasi software (Sistem operasi, aplikasi database, software jaringan, aplikasi perkantoran, aplikasi lainnya) d. Hardware – Peralatan fisik teknologi informasi (workstations, servers, dll) e. SDM – orang-orang dalam perusahaan yang memiliki skill khusus, pengetahuan, dan pengalaman yang sulit dicari penggantinya.
- Jaringan-→ Karena semua lalu lintas dalam jurusan dilalui	

melalui jaringan
- Server dan data-datanya
- Akses untuk PC2nya
- MONTA
- Sistem Informasi Akademik → Isidentiil
- Tidak ada data yang penting untuk dilindungi

2.	Kebutuhan keamanan apa sajakah yang digunakan untuk aset tersebut? Berikan penjelasannya!

Aset	Ketersediaan	Integritas	Kerahasiaan
Jaringan	Ada	Ada	Ada
Server dan datanya	Ada	Ada	Ada
Akses untuk PCnya	Ada	Ada	Ada
MONTA	Ada	Ada	Ada
Sistem Informasi Akademik	Ada	Ada	Ada

Organisasi	:	ITS
Nama Pejabat	:	Ir. A. Holil Noor Ali M.Kom
Jabatan	:	KaJur Sistem Informasi FTIf
Tanggal	:	15 Juni 2009
Topik	:	Identifikasi Aset dan Kebutuhan Keamanan.
Surveyor	:	Rachmawati F.

No	Pertanyaan
1.	Apa aset Penting dalam organisasi anda? Sebutkan 5 aset penting dan berikan alasan mengapa anda memilih aset tersebut? a. Informasi – data terdokumentasi (elektronik/non-elektronik) atau properti intelektual yang digunakan untuk mencapai misi perusahaan. Adapun yang termasuk aset informasi dalam organisasi adalah informasi mahasiswa, informasi nilai, informasi keuangan, informasi b. System – Sistem informasi yang memproses dan menyimpan informasi. Sistem adalah kombinasi dari aset informasi, hardware dan software. Beberapa mesin, clint, server atau jaringan dapat dipertimbangkan sebagai sistem. c. Software – aplikasi software (Sistem operasi, aplikasi database, software jaringan, aplikasi perkantoran, aplikasi lainnya) d. Hardware – Peralatan fisik teknologi informasi (workstations, servers, dll) e. SDM – orang-orang dalam perusahaan yang memiliki skill khusus, pengetahuan, dan pengalaman yang sulit dicari penggantinya.
-	Informasi Mahasiswa

- Informasi Nilai - Informasi Cash Flow - Informasi Anggaran - Informasi Indikator Capaian	
2.	Siapakah pemilik dari informasi tersebut?
3.	Kebutuhan keamanan apa sajakah yang digunakan untuk aset tersebut? Berikan penjelasannya!

Aset	Ketersediaan	Integritas	Kerahasiaan
Informasi Mahasiswa	Ada	Ada	Ada
Informasi Nilai	Ada	Ada	Ada
Informasi Cash Flow	Ada	Ada	Ada
Informasi Anggaran	Ada	Ada	Ada
Informasi Indikator Capaian	Tidak ada	Ada	Ada

Survey Bagian Manajemen

Nama Pejabat : Mustiko Adji, SE & Yudhi Purwananto, S.Kom. M.Kom.

Jabatan : KaBag TU & KaJur Teknik Informatika Fakultas Teknologi Informasi

Aspek Organisasi	
Pertanyaan	**Praktek?**
Keterangan Y (sudah ada/diimplementasikan) T (Belum ada/belum diimplementasikan) ? (tidak tahu/ragu-ragu)	
KEBIJAKAN KEAMANAN DAN PERATURAN	
Apakah dokumen kebijakan keamanan telah disusun?	T
Apakah sebuah dokumen kebijakan keamanan telah diterbitkan dan dipublikasikan?	T
STRATEGI KEAMANAN	
Sudahkah sebuah forum (steering commite) dibentuk untuk mengawasi dan membahas keamanan informasi?	T
Adakah proses untuk mengkoordinasikan implementasi tindakan keamanan informasi?	Y
Apakah tanggung jawab dan peran untuk memenuhi persyaratan (requirement) tercapainya keamanan informasi telah didefinisikan dengan jelas?	T
Apakah ada proses persetujuan manajemen dari sudut pandang bisnis untuk mengesahkan (otorisasi) fasilitas/layanan IT yang baru?	Y
Apakah kemampuan untuk menyediakan keamanan informasi yang khusus telah dimiliki?	T

Aspek Organisasi	
Pertanyaan	**Praktek?**
KOLABORATIF MANAJEMEN KEAMANAN	
Adakah penghubung (liason) kerjasama dengan personil dan organisasi keamanan informasi eksternal termasuk ahli keamanan industri dan atau pemerintah: provider IT; dan pihak yang berwenang dalam telekomunikasi?	T
Apakah risiko hubungan dengan pihak ketiga telah dianalisa?	Y
Sudahkan persyaratan (requirement) keamanan dari pemilik informasi telah disebutkan dalam kontrak antara pemilik dan organisasi outsource?	?
Apakah telah dilakukan review independent terhadap praktek keamanan informasi untuk memastikan kemampuannya beradaptasi, efektifitasnya, dan kesesuaiannya dengan kebijakan tertulis?	Y
Sudahkah tindakan keamanan telah diidentifikasikan secara khusus untuk menangkal risiko hubungan dengan pihak ketiga?	T
KLASIFIKASI DAN PENGONTROLAN ASET	
Sudahkan dibuat inventarisasi aset-aset utama yang berkaitan dengan sistem informasi?	Y
Sudahkan disusun petunjuk klasifikasi keamanan untuk perlindungan keamanan aset informasi dan yang berindikasi diperlukan dan yang harus diperoleh?	T
Sudahkan ada suatu proses untuk menandai informasi yang memerlukan perlindungan keamanan?	Y
MANAJEMEN KEAMANAN	
Apakah tanggung jawab keamanan disebutkan dalam deskripsi kerja pegawai?	Y

Aspek Organisasi	
Pertanyaan	**Praktek?**
Apakah ada saringan untuk lamaran pekerjan yang memerlukan akses ke informasi sensitive?	Y
Apakah kesepakatan non disclosure diberlakukan untuk tiap pegawai?	T
Apakah butir-butir perjanjian kerja menyertakan tanggung jawab keamanan informasi dan konsekuensi kelalaian untuk memenuhi persyaratan (requirement) tersebut, termasuk setelah pekerja selesai atau berhenti bekerja?	T
Apakah butir-butir perjanjian kerja menyertakan tanggung jawab keamanan informasi dan konsekuensi kelalaian untuk memenuhi persyaratan (requirement) tersebut, termasuk setelah pekerja selesai atau berhenti bekerja?	T
Sebelum mereka diberi akses terhadap fasilitas IT, apakah user telah diberi pelatihan tentang kebijakan dan prosedur keamanan informasi, persyaratan (requirement) keamanan, control bisnis, dan penggunaan fasilitas IT secara benar?	T
Apakah ada pelaporan resmi dan prosedur penanganan insiden untuk mengetahui tindakan apa yang harus dilakukan terhadap laporan insiden yang diterima?	T
Apakah user diminta untuk mencatat dan melaporkan semua kelemahan atau ancaman keamanan terhadap sistem atau jasa yang mereka temukan?	T
Apakah user diminta untuk mencatat dan melaporkan pada IT support jika ada software apapun yang tidak berfungsi dengan baik?	Y
Apakah ada mekanisme yang tersedia untuk memonitor tipe, jumlah dan kerugian karena insiden keamanan dan malfungsi?	Y

Aspek Organisasi	
Pertanyaan	**Praktek?**
Apakah ada proses sanksi formal terhadap pekerja yang melanggar kebijakan dan prosedur keamanan?	?
KETAATAN	
Apakah semua persyaratan legal, peraturan, dan kontrak ditentukan secara spesifik dan didokumentasikan untuk masing-masing sistem informasi?	T
Apakah penggunaan materi dengan hak cipta sudah sesuai dengan ketentuan legal untuk memastikan bahwa yang digunakan hanya software yang dibuat oleh organisasi, atau yang telah memperoleh ijin dan dikeluarkan oleh pengembang untuk organisasi?	T
Apakah catatan organizacional yang penting disimpan dengan aman untuk memenuhi persyaratan hukum maupun untuk mendukung aktifitas bisnis yang penting?	Y
Apakah aplikasi yang memproses data pribadi individu sesuai dengan peraturan proteksi data yang diterapkan?	Y
Apakah fasilitas IT yang digunakan hanya untuk tujuan bisnis?	T
Ketika suatu tindakan terhadap seseorang berkaitan dengan hukum, apakah ketentuan pembuktian telah diikuti agar memperoleh ijin, kualitas, dan kelengkapanyang dikehndaki?	T
Apakah semua wilayah dalam organisasi melakukan peninjauan berkala kesesuaian dengan kebijakan standar keamanan?	T
Apakah fasilitas IT diperiksa secara berkala untuk dilihat kesesuaiannya dengan standar implementasi keamanan?	T

Aspek Organisasi	
Pertanyaan	**Praktek?**
Apakah audit dan aktivitas yang melibatkan pemeriksaan terhadap sistem operasional direncanakan dan diatur secara cermat?	T
Apakah akses ke peralatan audit sistem telah dikontrol?	T
MANAJEMEN BISNIS BERKELANJUTAN	
Apakah proses yang dikelola untuk mengembangkan/mempertahankan keabsahan rencana kesinambungan bisnis seluruh organisasi?	T
Apakah telah diberlakukan strategi untuk menentukan pendekatan menyeluruh terhadap kesinambungan bisnis, dan didukung oleh manajemen?	T
Sudahkah proses perencanaan kesinambungan bisnis mencakup identifikasi dan kesesuaian dengan semua tanggung jawab dan prosedur emergency?	T
Apakah ada sebuah kerangka kerja untuk kesinambungan bisnis yang dipertahankan untuk memastikan bahwa semua tahapan rencana tetap konsisten?	T
Apakah rencana kesinambungan bisnis diuji secara berkala untuk memastikan bahwa mereka tetap actual dan efektif?	T

Survey Bagian Staff

Nama Pejabat : Hermono dan Donny
Jabatan : Staff Teknisi Jaringan SI Dan IF

Aspek Teknis	
Pertanyaan	**Praktek?**
Keterangan Y (sudah ada/diimplementasikan) T (Belum ada/belum diimplementasikan) ? (tidak tahu/ragu-ragu)	
KEAMANAN TEKNOLOGI INFORMASI	
Apakah kontroL akses telah didefinisikan dan didokumentasikan sesuai persyaratan bisnis?	T
Apakah ada prosedur registrasi dan deregistrasi secara formal bagi user untuk memperoleh akses terhadap semua layanan IT multi-user?	Y
Adakah batasan dan control terhadap penggunaan bentuk atau fasilitas apapun dari sistem IT multi-user yang memungkinkan user untuk melanggar control sistem atau control aplikasi?	Y
Apakah proses manajemen password resmi telah dilakukan untuk mengontrol password?	Y
Apakah ada proses formal untuk meninjau hak akses user secara berkala?	Y
Sudahkah user diajari praktek pengamanan yang baik dalam pemilihan dan penggunaan password?	T
Apakah semua user dan kontraktor diberitahu tentang persyaratan dan prosedur keamanan untu melindungi peralatan tanpa awak?	Y

Aspek Teknis	
Pertanyaan	**Praktek?**
Apakah semua user dan kontraktor diberitahu tentang tanggung jawab mereka untuk menerapkan perlindungan semacam itu?	?
Apakah ada proses untuk memastikan bahwa layanan jaringan computer yang bisa diakses perorangan atau dari terminal tertentu itu konsisten dengan kebijakan control akses bisnis?	?
Apakah ada control terkait untuk membatasi rute antara terminal user dengan suatu layanan computer, ketika user tersebut memiliki otorisasi untuk mengakses?	Y
Apakah ada control yang dilakukan user jarak jauh melalui jaringan public atau non-organisasional memakai otentikasi uder untuk mencegah akses tidak sah terhadap aplikasi bisnis?	?
Apakah ada hubungan yang dilakukan oleh sistem computer jarak jauh memakai otentikasi node untuk mencegah akses tidak sah terhadap aplikasi bisnis?	T
Apakah proses untuk mengontrol akses ke diagnostic port yang dirancang untuk penggunaan jarak jauh, oleh para petugas maintenance?	?
Apakah jaringan yang luas telah dibagi-bagi menjadi domain-domain terpisah untuk menekan risiko akses tidak sah terhadap sistem computer dalam jaringan tersebut?	Y
Apakah control telah diterapkan untuk membatasi kemampuan user melakukan koneksi, guna mendukung persyaratan kebijakan akses dari aplikasi bisnis yang melampui batas-batas organisasional?	Y

Aspek Teknis	
Pertanyaan	**Praktek?**
Apakah telah dilakukan control routing terhadap jaringan bersama melewati organisasi, untuk memastikan bahwa koneksi computer dan informasi mengalir sesuai dengan kebijakan akses unit-unit bisnis?	?
Apakah penyedia jaringan telah menjabarkan dengan jelas tentang atribut-atribut keamanan yang digunakan semua layanan, dan menetapkan implikasi keamanan terhadap kerahasiaan, integritas, dan ketersediaan aplikasi bisnis?	?
Akses terhadap computer harus dengan tegas dibatasi hanya melalui penggunaan: ❑ Identifikasi Terminal otomatis ❑ Prosedur log on terminal ❑ User ID ❑ Manajemen password ❑ Alarm bahaya ❑Terminal time out dan waktu connect yang terbatas	
Apakah ada control yang dilakukan user jarak jauh melalui jaringan public atau non-organisasional memakai otentikasi uder untuk mencegah akses tidak sah terhadap aplikasi bisnis?	?
Apakah identifikasi terminal otomatis diterapkan untuk otentifikasi koneksi ke lokasi tertentu (yang spesifik)?	Y
Sudahkan dirancang prosedur untuk logging ke dalam sebuah sistem komputer dengan meminimalkan desempatan akses tidak sah?	Y
Apakah semua user memiliki user ID yang unik, yang haya digunakan oleh mereka saja, untuk memastikan bahwa aktifitas mereka bisa ditelusuri?	Y

Aspek Teknis	
Pertanyaan	**Praktek?**
Apakah sistem manajemen password yang efektif diterapkan untuk otentikasi user?	T
Apakah program sistem utility yang bisa digunakan untuk mengontrol sistem dan aplikasi telah dikontrol secara ketat dan penggunaannya sangat dibatasi?	Y
Berdasarkan assessmen risiko, apakah alarm bahaya disediakan bagi user yang mungkin menjadi sasaran intimidasi?	T
Apakah ada definisi tanggung jawab tidak lanjut alarm bahaya?	T
Apakah terminal-terminal dilokasi berisiko tinggi ada set time out ketika sedang tidak aktif, untuk mencegah akses orang-orang yang tidak berwenang?	T
Apakah ada limit waktu hubungan terminal dengan sistem aplikasi yang sensitive?	T
Apakah akses ke data dan fungsi sistem aplikasi dibatasi sesuai dengan ketetapan kebijakan akses berdasarkan requirement individual?	T
Apakah sistem aplikasi yang sensitive beroperasi di lingkungan pemrosesan terisolasi telah sesuai dengan identifikasi risiko	T
Apakah ada event logging (audit trail) yang berisi berbagai hal abnormal dan peristiwa berkaitan dengan masalah keamanan dan digunakan untuk membantu investigasi dimasa mendatang dan memonitor control akses?	T

Aspek Teknis	
Pertanyaan	**Praktek?**
Apakah sudah ditetapkan prosedur untuk memonitor penggunaan sistem untuk memastikan bahwa user hanya melakukan proses-proses yang telah diotorisasi secara jelas?	T
Untuk memastikan akurasi audit trail, apakah jam pada computer atau alat komunikasi telah disetel sesuai dengan standar yang telah disepakati?	Y
Sudahkan kebijakan formal telah disusun, yang menyebutkan risiko-risiko bekerja dengan fasilitas mobile computing, termasuk pentingnya perlindungan fisik, control akses, teknik kriptografi, backup, dan perlindungan dari viris?	T
Apakah kebijakan dan prosedur telah disusun untuk mengontrol teleworking, mencakup fasilitas yang ada, lingkungan teleworking yang diajukan, pesyaratan keamanan komunikasi, dan ancaman akses tidak sah terhadap peralatan atau jaringan?	?
Apakah prosedur pengoperasian (SOP) sistem komputer benar-benar didokumentasikan untuk menjamin operasi yang tepat dan aman?	T
Adakah sebuah proses untuk mengontrol perubahan fasilitas dan sistem IT, untuk memastikan control yang handal terhadap semua perubahan peralatan, software, atau prosedur?	Y
Apakah tanggung jawab dan prosedur manajemen inciden telah ditetapkan untuk memastikan respon yang cepat, efektif, dan teratur dalam setiap insiden keamanan?	Y

Aspek Teknis	
Pertanyaan	**Praktek?**
Apakah ada pemisahan tugas-tugas sensitive atau wewenang sensitive ? Hal ini untukmenekankan peluang modifikasi yang tidak sah, atau penyalahgunaan data dan jasa?	Y
Apakah fasilitas pengembangan dan operasional dipisah untuk mengurangi risiko perubahan tak sengaja atau akses tidak sah terhadap software operasional dan data bisnis?	Y
Apakah ada monitor proyeksi persyaratan (requirement) kapasitas, dan persyaratan yang akan datang, untuk menekan risiko overload pada sistem?	T
Apakah ada kriteria penerimaan sistem yang baru telah ditetapkan, dan test yang sesuai dilakukan sebelum penerimaannya?	Y
Apakah tindakan pencegahan dan deteksi virus, dan prosedur kewaspadaan user telah diterapkan?	Y
Apakah telah diberlakukan proses untuk membuat backup salinan data bisnis dan software secara berkala untuk menjamin bahwa semuanya bisa di-recover jira terjadi kerusakan komputer atau kegagalan media?	Y
Apakah semua operador komputer diharuskan selalu menjalankan log (membuat daftar otomatis) semua langkah yang mereka lakukan?	T
Apakah ada control yang sesuai untuk memastikan keamanan data dalam jeringan, dan perlindungan terhadap jasa-jasa terkait, dari akses yang tidak sah?	T

Aspek Teknis	
Pertanyaan	**Praktek?**
Apakah ada prosedur yang mengatur pengelolaan media computer yang bisa dipindah-pindahkan seperti tape, disk, kaset, dan print out laporan?	T
Apakah terdapat proses untuk memastikan bahwa media computer dibuang secara aman ketika tidak lagi diperlukan?	Y
Apakah ada prosedur untuk menangani perlindungan data sensitive sehingga terjaga dari kebocoran ke pihak yang tidak sah atau penyalahgunaan	T
Apakah dokumentasi sistem dilindungi dari akses yang tidak sah?	Y
Adakah persetujuan formal escrow (perantara) software jika diperlukan tentang pertukaran data dan software (elektronis maupun manual) antar organisasi?	T
Apakah control keamanan telah diterapkan untuk melindungi electronic commerce (pertukaran data elektronis, email, dan tranksaksi-tranksaksi online di jaringan public seperti internet) dari pencegatan atau modifikasi?	T
Apakah control diterapkan (bila perlu) untuk mengurangi risiko bisnis dan keamanan yang berkaitan dengan e-mail termasuk pencegatan, penyadapan, modifikasi, dan keslahan?	T
Apakah ada kebijakan dan petunjuk yang jelas untuk mengontrol risiko bisnis dan keamanan yang berkaitan demgan sistem office electronic?	T
Apakah ada proses otorisasi formal sebelum informasi disampaikan kepada public?	Y

Aspek Teknis	
Pertanyaan	**Praktek?**
Apakah ada prosedur dan control untuk melindungi pertukaran informasi melalui penggunaan voice, facsimile, dan fasilitas komunikasi video?	T

Survey Bagian Staff

Nama Pejabat : Anis Muslich, SE
Jabatan : Kasubbag Umum & Perlengkapan FTIf

Aspek Fisik	
Pertanyaan	**Praktek?**
Keterangan Y (sudah ada/diimplementasikan) T (Belum ada/belum diimplementasikan) ? (tidak tahu/ragu-ragu)	
KEAMANAN FISIK DAN LINGKUNGAN	
Apakah ada proteksi keamanan fisik dilingkupi perimeter yang telah ditetapkan, melalui penghalang-penghalang yang ditempatkan secara strategis diseluruh organisasi?	Y
Apakah semua pintu masuk semua wilayah aman memastikan (kontrol) hanya pihak berwenang yang memperoleh akses?	Y
Apakah keamanan fisik untuk pusat-pusat data dan ruang computer telah disesuaikan dengan ancaman yang mungkin timbul?	T
Apakah control tambahan digunakan bagi personil atau pihak ketiga yang bekerja diwilayah aman?	T
Apakah wilayah ruang computer atau pusat data yang digunakan untuk mengirim dan meload benar-benar tertutup untuk mencegah akses yang tidak sah?	T
Apakah peralatan ditempatkan secara tepat untuk melindunginya dari bencana alam dan akses tidak sah?	Y

Aspek Fisik	
Pertanyaan	**Praktek?**
KEAMANAN FISIK DAN LINGKUNGAN (lanjutan)	
Apakah peralatan listrik dilindungi dari "mati lampu" dan masalah listrik yang lain-lain?	T
Apakah penataan kabel listrik dan telekomunikasi dilindungi dari sadapan atau kerusakan?	T
Apakah telah ditetapkan prosedur untuk menjaga peralatan IT secara benar, untuk memastikan bahwa peralatan tersebut selalu tersedia dan dalam keadaan baik?	Y
Apakah peralatan yang digunakan diluar lokasi, siapapun pemiliknya, diberikan tingkat perlindungan yang sama sebagaimana peralatan yang digunakan dalam lokasi?	T
Apakah telah diterapkan kebijakan clear desk/clear screen untuk menekan risiko akses tidak sah, kerugian, atau kerusakan di luar jam kerja normal?	T
Apakah ada keharusan mendapatkan otorisasi manajemen tertulis untuk membawa peralatan, data, atau software keluar lokasi?	Y

Halaman ini sengaja dikosongkan

BIODATA PENULIS

Penulis dilahirkan di Surabaya, 30 September 1985. SDN Kedung Cowek 254 Surabaya, SLTPN 31 Surabaya dan SMUN 19 Surabaya. Penulis diterima di Jurusan Sistem Informasi ITS Surabaya tahun 2005 dan terdaftar dengan NRP. 5205100077.

Di jurusan Sistem Informasi penulis mengambil bidang studi Perencanaan dan Pengembangan Sistem Informasi (PPSI). Penulis pernah tergabung dalam tim data entry PSB-online Surabaya pada tahun 2007. Bagi yang ingin berdiskusi lebih lanjut silakan hubungi penulis lewat email : hikma_07@yahoo.co.id

BIODATA PENULIS