TUGAS AKHIR – KS141501

PEMBUATAN DOKUMEN SOP (STANDAR OPERASIONAL PROSEDUR) KEAMANAN ASET INFORMASI YANG MENGACU PADA KONTROL KERANGKA KERJA ISO 27002:2013 (STUDI KASUS : CV CEMPAKA TULUNGAGUNG)

DHENI INDRA RACHMAWAN
NRP 5212 100 178

Dosen Pembimbing I :
Dr. Apol Pribadi S., S.T, M.T

Dosen Pembimbing II :
Eko Wahyu Tyas Darmaningrat, S.Kom., M.BA

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

FINAL PROJECT – KS141501

DEVELOPING STANDARD OPERATIONAL PROCEDURE (SOP) DOCUMENT FOR ASSET INFORMATION SECURITY REFER TO CONTROL ISO27002:2013 FRAMEWORK (CASE STUDY : CV CEMPAKA TULUNGAGUNG)

DHENI INDRA RACHMAWAN
NRP 5212 100 178

Supervisor I :
Dr. Apol Pribadi S., S.T, M.T

Supervisor II :
Eko Wahyu Tyas Darmaningrat, S.Kom., M.BA

INFORMATION SYSTEMS DEPARTMENT
Information Technology Faculty
Institute of Technology Sepuluh Nopember
Surabaya 2017

TUGAS AKHIR – KS141501

PEMBUATAN DOKUMEN SOP (STANDAR OPERASIONAL PROSEDUR) KEAMANAN ASET INFORMASI YANG MENGACU PADA KONTROL KERANGKA KERJA ISO 27002:2013 (STUDI KASUS : CV CEMPAKA TULUNGAGUNG)

Dheni Indra Rachmawan
NRP 5212100178

Dosen Pembimbing I
Dr. Apol Pribadi S., S.T, M.T

Dosen Pembimbing II
Eko Wahyu Tyas Darmaningrat, S.Kom., M.BA

JURUSAN SISTEM INFORMASI
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember
Surabaya 2017

FINAL PROJECT – KS141501

DEVELOPING STANDARD OPERATIONAL PROCEDURE (SOP) DOCUMENT FOR ASSET INFORMATION SECURITY REFER TO CONTROL ISO27002:2013 FRAMEWORK (CASE STUDY : CV CEMPAKA TULUNGAGUNG)

Dheni Indra Rachmawan
NRP 5212100178

Supervisor I
Dr. Apol Pribadi S., S.T, M.T

Supervisor II
Eko Wahyu Tyas Darmaningrat, S.Kom., M.BA

Information Systems Department
Information Technology Faculty
Institut of Technology Sepuluh Nopember
Surabaya 2017

LEMBAR PENGESAHAN

PEMBUATAN DOKUMEN SOP *(STANDARD OPERATIONAL PROCEDURE)* KEAMANAN ASET INFORMASI YANG MENGACU PADA KONTROL KERANGKA KERJA ISO 27002:2013 (STUDI KASUS: CV CEMPAKA TULUNGAGUNG)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh:

DHENI INDRA RACHMAWAN
5212 100 178

Surabaya, Januari 2017

KETUA
JURUSAN SISTEM INFORMASI

Dr. Ir. Aris Tjahyanto, M.Kom
NIP.19650310 199102 1 001

LEMBAR PERSETUJUAN

PEMBUATAN DOKUMEN SOP *(STANDARD OPERATIONAL PROCEDURE)* KEAMANAN ASET INFORMASI YANG MENGACU PADA KONTROL KERANGKA KERJA ISO 27002:2013 (STUDI KASUS: CV CEMPAKA TULUNGAGUNG)

TUGAS AKHIR

Disusun untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer
pada
Jurusan Sistem Informasi
Fakultas Teknologi Informasi
Institut Teknologi Sepuluh Nopember

Oleh :

DHENI INDRA RACHMAWAN
5212 100 178

Disetujui Tim Penguji : Tanggal Ujian : 11 Januari 2017
Periode Wisuda : Maret 2017

Dr. Apol Pribadi S., S.T, M.T **(Pembimbing 1)**

Eko Wahyu Tyas Darmaningrat, S.Kom., M.BA **(Pembimbing 2)**

Ir. Ahmad Holil Noor Ali, M.Kom **(Penguji 1)**

Annisah Herdiyanti, S.Kom., M.Sc., ITIL **(Penguji 2)**

PEMBUATAN DOKUMEN SOP *(STANDARD OPERATIONAL PROCEDURE)* KEAMANAN ASET INFORMASI YANG MENGACU PADA KONTROL KERANGKA KERJA ISO 27002:2013 (STUDI KASUS: CV CEMPAKA TULUNGAGUNG)

Nama Mahasiswa : DHENI INDRA RACHMAWAN
NRP : 5212 100 178
Jurusan : Sistem Informasi FTIF-ITS
Dosen Pembimbing I : Dr. Apol Pribadi S., S.T, M.T
Dosen Pembimbing II : Eko Wahyu Tyas Darmaningrat, S.Kom., M.BA

ABSTRAK

CV Cempaka Tulungagung merupakan perusahaan manufaktur yang bergerak pada industri rokok. Perusahaan ini menggunakan Teknologi Informasi dalam mendukung proses bisnisnya, Tetapi pada perusahaan ini keamanan dari aset informasi tidak begitu diperhitungkan. CV Cempaka belum memiliki peraturan maupun prosedur mengenai keamanan aset informasi sehingga berdampak sering terjadinya permasalahan kehilangan data dan kerusakan pada beberapa komputer perusahaan yang mengakibatkan proses bisnis terhambat.

Dalam memenuhi kebutuhan keamanan aset informasi tersebut maka diperlukan adanya sebuah tata kelola dalam bentuk dokumen SOP (Standard Operating Procedure) keamanan aset informasi untuk mengurangi adanya ancaman dan risiko serta untuk mendukung penyelarasan pencapaian tujuan organisasi dalam proses bisnisnya. Metode penelitian yang digunakan

yaitu OCTAVE sebagai pengolah hasil informasi yang didapatkan dari wawancara dan FMEA digunakan untuk menghitung seberapa tinggi dampak untuk perusahaan jika risiko itu terjadi dan membuat ranking prioritas untuk masing-masing risiko. Kemudian acuan dalam pengendalian risikoyang telah diidentifikasi dengan menggunakan kerangka kerja ISO/IEC:27002:2013.

Dalam penelitian ini, hasil akhir yang didapatkan adalah sebuah dokumen SOP yang sesuai dengan kebutuhan keamanan informasi bagi perusahaan CV Cempaka dengan acuan kontrol pada kerangka kerja ISO27002:2013, Selain SOP yang dihasilkan adapula dokumen pendukung seperti kebijakan, formulir dan instruksi kerja untuk mendukung implementasi dari SOP keamanan aset informasi.

Kata kunci: Keamanan Aset, Standard Operating Procedure, Risiko, Manajemen Risiko, ISO27002:2013

DEVELOPING STANDARD OPERATIONAL PROCEDURE (SOP) DOCUMENT FOR ASSET INFORMATION SECURITY REFER TO CONTROL ISO27002:2013 FRAMEWORK (CASE STUDY : CV CEMPAKA TULUNGAGUNG)

Name	**: DHENI INDRA RACHMAWAN**
NRP	**: 5212 100 178**
Department	**: Information Systems FTIF -ITS**
Supervisor I	**: Dr. Apol Pribadi S., S.T, M.T**
Supervisor II	**: Eko Wahyu Tyas Darmaningrat, S.Kom., M.BA**

ABSTRACT

.CV Cempaka Tulungagung is a manufacturing company engaged in the tobacco industry. The company uses information technology in support of business processes, but the company is the security of information assets is not taken into consideration. CV Cempaka not yet have rules or procedures regarding the security of information assets so the impact is often the problem of data loss and damage to several computer companies that resulted in a business process is inhibited.

In meeting the security needs of the information assets of the necessary existence of a governance document in the form of SOP (Standard Operating Procedure) the security of their information assets to mitigate threats and risks as well as to support the achievement of organizational goals in the alignment of business processes. The method used is OCTAVE

as the processing result of information obtained from interviews and FMEA is used to calculate how high the risk of impact to the company if it happens and rank priorities for each risk. Then the reference in risikoyang control have been identified by using the framework of ISO / IEC: 27002: 2013.

In this study, the final result obtained is an SOP documents that match the security needs of information for the company's CV Cempaka with reference to the control in the framework of ISO27002: 2013, the addition of SOP produced unisex supporting documents such as policies, forms and work instructions to support the implementation of SOP security of information assets.

Keywords: Asset Security, Standard Operating Procedure, Risk, Risk Mangement, ISO27002:2013

Buku ini dipersembahkan untuk kedua orang tua, serta kakak perempuan tercinta yang selalu medoakan dan memberi dukungan

Halaman ini sengaja dikosongkan

KATA PENGANTAR

Alhamdulillah.

Puji syukur penulis panjatkan ke hadirat Allah SWT karena hanya berkat hidayah, rahmat, dan karunia-Nya penulis dapat menyelesaikan laporan tugas akhir yang berjudul **"PEMBUATAN DOKUMEN SOP *(STANDAR OPERASIONAL PROSEDUR)* KEAMANAN ASET INFORMASI YANG MENGACU PADA KONTROL KERANGKA KERJA ISO 27002:2013"**. Laporan tugas akhir ini disusun sebagai syarat kelulusan pada Jurusan Sistem Informasi Institut Teknologi Sepuluh Nopember Surabaya.

Selama pengerjaan dan penulisan laporan tugas akhir ini, tentunya banyak pihak yang telah memberikan bantuan sehingga dapat terselesaikan dengan baik dan tepat waktu. Oleh karena itu penulis ingin mengucapkan terima kasih kepada :

1. Bapak Dr. Apol Pribadi Subriadi, S.T, M.T selaku Dosen Pembimbing I yang bersedia meluangkan waktunya dan membimbing penulis dalam pengerjaan tugas akhir ini.
2. Ibu Eko Wahyu Tyas Darmaningrat, S.Kom., M.BA selaku Dosen Pembimbing II yang selalu sabar membimbing dan memberi nasehat nasehat kepada penulis.
3. Bapak Ir. Ahmad Holil Noor Ali, M.Kom dan Ibu Annisah Herdiyanti, S.Kom., M.Sc., ITIL selaku dosen penguji. Terimakasih atas kritikan dan masukan yang bersifat membangun untuk peningkatan kualitas penelitian ini.
4. Bapak Dr. Aris Tjahyanto, M.Kom selaku Ketua Jurusan Sistem Informasi ITS, yang telah memberikan dan menyediakan fasilitas terbaik untuk kebutuhan panelitian ini.
5. Bapak Hermono selaku laboran yang membantu menjadwalkan seminar dan sidang tugas akhir.
6. Ibu Ida Wahyu Yuniarti, S.H. selaku Kepala Divisi Personalia CV Cempaka yang selalu memberikan informasi,

pengetahuan serta dukungan yang sangat baik selama peneitian.

7. Rahma Permatasari yang selalu ada untuk mebantu, menghibur, menyemangati dan memberikan inspirasi serta selalu mendoakan kelancaran pengerjaan Tugas Akhir ini.
8. Anggota MK 56 yang selalu memberikan dukungan dan motivasi kepada penulis dalam segala proses penelitian
9. Teman-teman Sola12is dan seluruh anggota HMSI yang saling mendukung selama masa tugas belajar ini.
10. Seluruh pihak yang telah membantu penulis baik secara langsung maupun tidak langsung dan telah memberikan dukungan sehingga tugas akhir ini dapat terselesaikan dengan baik.

Penulis menyadari bahwa masih banyak kekurangan pada tugas akhir ini, maka penulis mohon maaf atas segala kekurangan dan kekeliruan yang ada di dalam tugas akhir ini. Penulis membuka pintu selebar-lebarnya bagi pihak-pihak yang ingin memberikan kritik dan saran bagi penulis untuk menyempurnakan tugas akhir ini. Semoga tugas akhir ini dapat bermanfaat bagi seluruh pembaca.

Surabaya, 05 Januari 2017

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

Halaman Sengaja Dikosongkan

BAB I
PENDAHULUAN

Pada bab ini, akan dijelaskan tentang Latar Belakang Masalah, Perumusan Masalah, Batasan Masalah, Tujuan Tugas Akhir, Manfaat Kegiatan Tugas Akhir dan Relevansi dengan laboratorium MSI.

1.1. Latar Belakang

Teknologi informasi mampu membantu melakukan kegiatan operasional secara efektif dan efisien untuk mempertahankan eksistensinya, sehingga mampu memberikan nilai tersendiri dan mampu untuk menciptakan keunggulan kompetitif. Oleh karena penggunaan teknologi informasi telah menjadi salah satu faktor kunci keberhasilan suatu perusahaan ataupun organisasi. Hal ini membuat keamanan aset sebuah informasi menjadi salah satu aspek penting dari digunakanya teknologi informasi pada sebuah organisasi, tetapi sangat disayangkan masalah keamanan ini seringkali kurang mendapat perhatian dari para pemilik dan pengelola teknologi informasi. Seringkali masalah keamanan berada di urutan kedua, atau bahkan diurutan terakhir dalam daftar hal-hal yang dianggap penting. Pada survey yang dilakukan oleh IBM melalui internet, 92 % dari bisnis yang dilakukan tidak memiliki persiapan apapun apabila terjadi bencana terkait teknologi informasi [1]. Survey ini dilakukan pada 224 pimpinan perusahaan di seluruh dunia. Menurut pembelajaran yang sudah dilakukan pada perusahaan atau organisasi yang pernah mengalami bencana, 40% dari organisasi atau perusahaan tersebut lumpuh terkena dampak dari bencana sehingga tidak dapat melanjutkan operasi bisnisnya lagi dan hanya 25% dari organisasi tersebut yang dapat menjalankan [2]. Keamanan informasi secara

tidak langsung menjadi salah satu perhatian bagi perusahaan jika ingin melanjutkan proses bisnisnya. Oleh karena itu, perlu adanya standarisasi yang diterapkan atau diimplementasikan dalam perusahaan sebagai panduan yang memberikan arahan dalam menjaga asset penting seperti informasi yang dianggap penting dalam menjalankan proses bisnis bagi perusahaan tersebut.

Dalam era global ini berbagai perusahaan industri telah memanfaatkan teknologi komputer untuk menghasilkan informasi yang akan digunakan, sebagai dasar dalam pengambilan keputusan-keputusan penting. Salah satunya perusahaan CV Cempaka Tulungagung yang merupakan perusahaan manufaktur yang bergerak pada industri rokok. Perusahaan ini menggunakan Teknologi Informasi dalam proses bisnisnya antara lain dalam melakukan perencanaan perhitungan bahan baku, penjadwalan produksi, pengelolaan inventori, pemeriksaan kalitas produk, pencatatan pegawai, pencatatan fasilitas kantor, pencatatan distributor, pencatatan piutang, laporan bulanan, pencatatan aktiva dan lain sebagainya, tetapi pada perusahaan ini keamanan aset informasi tidak begitu diperhitungkan dampak dari ancaman yang mungkin maupun sudah terjadi antara lain sering terjadinya kehilangan data perhitungan dalam penjadwalan produksi dan penyediaan bahan baku, pernah hilangnya beberapa data distributor dan karyawan, dan sering terjadi konsleting pada beberapa komputer perusahaan sehingga mengakibatkan proses bisnis terhambat. Hal ini menunjukan bahwa risiko hilangnya maupun rusaknya aset informasi menjadi salah satu perhatian yang harus segera diatasi. Dengan adanya permasalahan tersebut, keamanan aset informasi harus dapat dikelola dengan baik sehingga dapat memperkecil risiko yang menyebabkan terganggunya proses bisnis.

Dengan demikian, salah satu bentuk dukungan dalam menjaga keamanan aset informasi yang dapat diimplementasikan pada perusahaan CV Cempaka adalah dengan membuat sebuah prosedur yang terdokumentasi dengan baik dalam bentuk sebuah dokumen SOP (*Standard Operational Procedure*) mengenai kemanan aset informasi agar risiko dari keamanan informasi dapat dikurangi atau dihindari. SOP dapat berguna untuk mendefinisikan seluruh konsep, teknik, dan persyaratan dalam menjalankan suatu proses yang dituliskan ke dalam suatu dokumen yang langsung dapat digunakan oleh pegawai maupun karyawan yang bersangkutan dalam melaksanakan tugas dalam proses bisnisnya [3]. Metode penelitian yang digunakan yaitu OCTAVE sebagai pengolah hasil informasi yang didapatkan dari wawancara dan FMEA digunakan untuk menghitung seberapa tinggi dampak untuk perusahaan jika risiko itu terjadi dan membuat ranking prioritas untuk masing-masing risiko. Kemudian basis yang digunakan dalam membuat prosedur kendali akses aset informasi sebagai manajemen risiko adalah kerangka kerja ISO/IEC:27002:2013.

Sebelumnya sudah ada penelitian serupa mengenai pembuatan Dokumen SOP yang menggunakan kerangka kerja 27002:2013. Namun berdasarkan analisis penelitian terdahulu, belum ada yang melibatkan perusahaan dibidang industri rokok seperti halnya CV Cempaka. Juga terdapat beberapa kelemahan dalam dokumentasi tindakan, instruksi kerja dan kebijakan yang masih minim. Sehingga diperlukan adanya pembuatan dokumen SOP untuk mengatur dan membuat proses TI di CV Cempaka lebih terstruktur, juga dapat meningkatkan kualitas keamanan informasi yang ada.

Pada proses pembuatan dokumen SOP ini, kerangka kerja ISO/IEC 27002:2013 berfungsi sebagai acuan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan [4]. ISO/IEC27002 tidak mengharuskan bentuk-bentuk kontrol yang tertentu tetapi menyerahkan kepada pengguna untuk memilih dan menerapkan kontrol yang tepat sesuai kebutuhannya, dengan mempertimbangkan hasil analisa risiko yang telah dilakukan.

1.2. Rumusan Permasalahan

Berdasarkan latar belakang yang telah dijabarkan di atas, maka didapatkan perumusan masalah yang akan dijadikan acuan dalam pembuatan tugas akhir ini adalah sebagai berikut :

1. Apakah hasil analisis risiko untuk keamanan aset informasi yang terkait dengan proses operasional bisnis pada CV Cempaka ?
2. Bagaimana hasil pembuatan dokumen SOP *(Standard Operational Procedure)* untuk keamanan aset informasi pada CV Cempaka yang mengacu pada kontrol kerangka kerja ISO27002:2013 ?
3. Apakah hasil dokumen SOP *(Standard Operational Procedure)* keamanan aset informasi sudah sesuai dengan kebutuhan keamanan pada CV Cempaka ?

1.3. Batasan Masalah

Dari perumusan masalah yang telah dipaparkan sebelumnya, dalam pengerjaan tugas akhir ini ada beberapa batasan masalah yang harus diperhatikan adalah sebagai berikut :

1. Aset Informasi pada penelitian ini hanya mencakup aset informasi kritis pada CV Cempaka Tulungagung.
2. Analisis risiko yang dilakukan adalah terbatas kepada analisis risiko aset informasi kritis pada CV Cempaka Tulungagung.
3. Analisa dan penilaian risiko dilakukan dengan menggunakan pendekatan metode OCTAVE *(Operationally Critical Threat, Asset, and Vulnerability)* dan FMEA *(Failure Modes and Effecs Analysis)*
4. Penelitian ini berfokus pada keamanan aset informasi yang bernilai *high* dan *very high*.
5. Penelitian ini menggunakan standard ISO27002:2013 sebagai acuan pembuatan kontrol dalam pembuatan SOP.

1.4. Tujuan Tugas Akhir

Tujuan tugas akhir yang dibuat oleh peneliti adalah :

1. Menghasilkan identifikasi dan penilaian risiko aset informasi yang dapat mengancam proses bisnis yang berkaitan dan mengetahui tindakan yang harus dilakukan untuk mengatasi risiko pada CV Cempaka Tulungagung
2. Menghasilkan dokumen SOP *(Standard Operating Procedure)* keamanan aset informasi pada CV Cempaka Tulungagung yang berdasarkan hasil analisis risiko dan sesuai dengan kerangka kerja ISO/IEC 27002:2013
3. Mengetahui hasil verifikasi dan validasi dari dokumen SOP sehingga dapat digunakan oleh CV Cempaka Tulungagung untuk mendukung pengelolaan keamanan aset informasi.

1.5. Manfaat Tugas Akhir

Manfaat yang dapat diperoleh dari pengerjaan tugas akhir ini adalah sebagai berikut:

Bagi akademisi :

1. Peneliti menjadi mengerti aset informasi penting pada perusahaan manufaktur khususnya pada industri rokok
2. Peneliti menjadi mengerti risiko apa saja yang terjadi pada aset informasi pada perusahaan manufaktur khususnya pada industri rokok
3. Peneliti berkontribusi dalam penyusunan dokumen SOP (*Standard Operating Procedure*) terkait keamanan aset informasi pada perusahaan manufaktur khususnya pada industri rokok

Bagi Perusahaan :

1. Perusahaan mendapatkan informasi terkait risiko teknologi informasi yang dapat muncul di CV Cempaka Tulungagung
2. Perusahaan mendapatkan Dokumen SOP (*Standard Operating Procedure*) terkait keamanan aset informasi yang dapat digunakan sebagai panduan atau langkah dasar untuk melakukan proses keamanan aset informasinya.

1.6. Relevansi

Topik pada tugas akhir ini mengenai Pembuatan Dokumen SOP (*Standard Operational Procedure*) Keamanan Aset Informasi Mengacu pada Kontrol ISO27002:2013 (*Studi Kasus : CV Cempaka Tulungagung*). Topik tersebut berkaitan dengan mata kuliah manajemen risiko serta tata kelola Teknologi dan sistem informasi yang berada dalam roadmap pada laboratorium Manajemen Sistem Informasi (MSI).

BAB II
TINJAUAN PUSTAKA

Sebelum melakukan penelitian tugas akhir, penulis melakukan tinjauan terhadap tulisan dari beberapa penelitian sebelumnya yang sesuai dengan tema yang diambil. Hasil tinjauan tersebut adalah sebagai berikut.

2.1 Studi Sebelumnya

Dalam mengerjakan tugas akhir ini terdapat beberapa penelitian yang digunakan sebagai acuan referensi, berikut merupakan informasi singkat mengenai penelitian-penelitian berikut :

JUDUL	***PROTEKSI ASET SISTEM INFORMASI; ANALISIS DAN DESAIN MODEL PROTEKSI TERHADAP ASET SISTEM INFORMASI TERINTEGRASI***
Nama Peneliti	Ali Masjono
Tahun Penelitian	2010
Hasil Penelitian	Desain model dari SIM-Integrasi Security Management dan SOP untuk meyakinkan bahwa SIM-Integrasi PNJ memiliki Standar Security Policy dan procedure yang memadai
Hubungan dengan Tugas Akhir	Kaitan antara tugas akhir dengan penelitian ini adalah terletak pada SOP yang dibuat mengenai keamanan aset informasi yang dimiliki oleh suatu organisasi

JUDUL	***EVALUASI RISK MANAGEMENT PADA PARA PENGEPUL TEMBAKAU DI KECAMATAN BAURENO KABUPATEN BOJONEGORO***
Nama Peneliti	Vina Erviana Yenny Sugiarti, S.E. M.Ak., QIA.
Tahun Penelitian	2014
Hasil Penelitian	Menghasilkan rekomendasi kepada para pengepul untuk mengatasi risiko secara umum dengan melakukan reduction. Rekomendasi ini berguna bagi badan usaha untuk mengelola risiko yang ada pada usahanya
Hubungan dengan Tugas Akhir	Kaitan antara tugas akhir dengan penelitian ini adalah terletak pada cara pengelolaan risiko yang ada pada pabrik rokok tingkat menengah yang mampu dijadikan pedoman bagi penulis

JUDUL	***KAJIAN STRATEGI PENGAMANAN INFRASTRUKTUR SUMBER DAYA INFORMASI KRITIS***
Nama Peneliti	Ahmad Budi Setiawan
Tahun Penelitian	2015
Hasil Penelitian	Masukan untuk kebijakan dan kerangka kerja pengamanan infrastruktur kritis khususnya sektor TIK. Kajian ini dilakukan dengan metode gabungan kuantitatif dan kualitatif yang mengkombinasikan hasil penilaian risiko

	pada obyek riset dengan pendapat pengambil kebijakan, akademisi, pakar dan praktis
Hubungan dengan Tugas Akhir	Kaitan antara tugas akhir dengan penelitian ini adalah mengenai strategi yang dapat digunakan untuk mengamankan sumber daya informasi kritis yang ada di sebuah perusahaan. Strategi tersebut dapat digunakan sebagai referensi oleh peneliti

JUDUL	***PEMBUATAN DOKUMEN SOP (STANDART OPERATING PROCEDURE) KEAMANAN DATA YANG MENGACU PADA KONTROL KERANGKA KERJA COBIT 5 DAN ISO 27002:2013 (STUDI KASUS : STIE PERBANAS)***
Nama Peneliti	Aulia Nur Fatimah
Tahun Penelitian	2015
Hasil Penelitian	Penelitian ini menghasilkan dokumen SOP mengenai keamanan data dan juga rekomendasi mitigasi risiko yang ada pada STIE PERBANAS
Hubungan dengan Tugas Akhir	Kaitan antara tugas akhir dengan penelitian ini adalah metodologi yang digunakan hampir sama dan juga penentuan kontrolnya dilakukan berdasarkan pemetaan kerangka kerja terlebih dahulu berdasarkan pada hasil penilaian risiko yang memiliki nilai paling tinggi.

Dari studi literatur diatas bisa diketahui bahwa terdapat peneliti sebelumnya yang melakukan pembuatan *standart operating procedure (SOP)* dalam sebuah organisasi. Pada penelitian ini akan menyusun *standart operating procedure (SOP)* pada perusahaan yang bergerak di bidang industri rokok, khususnya perusahaan rokok CV Cempaka Tulungagung.

2.2 Dasar Teori

Pada bagian ini, akan dijelaskan mengenai teori-teori yang digunakan untuk mendukung pengerjaan tugas akhir. Teori tersebut yaitu mengenai : aset, keamanan data, risiko, metode manajemen risiko yaitu OCTAVE dan FMEA, kerangka kerja Cobit dan ISO27002:2013 serta SOP (*Standard Operating Procedure*).

2.2.1 Aset

Aset merupakan sumber daya yang dimiliki oleh perusahaan atau semua hak yang dapat digunakan dalam perusahaan. Aset juga termasuk didalamnya pembebanan yang ditunda yang dinilai dan diakui sesuai dengan prinsip ekonomi yang berlaku. [5]

Sementara menurut FASB (*Financial Accounting Standards Boards)* menjelaskan aset adalah kemungkinan keuntungan ekonomi yang diperoleh atau dikuasai di masa yang akan datang oleh perusahaan sebagai akibat transaksi atau kejadian yang sudah berlalu.

2.2.2 Aset Informasi

Aset informasi adalah sepotong informasi yang terdefinisi, disimpan dengan cara apapun, tidak mudah untuk diganti, keahlian, waktu, sumber daya dan kombinasinya serta diakui sebagai sesuatu yang berharga bagi organisasi. Aset informasi pada penelitian ini akan mengacu pada definisi komponen Sistem

Informasi. Komponen sistem informasi dibangun berdasarkan komponen-komponen pendukung yang meliputi : sumber daya manusia *(people)*, perangkat keras *(hardware)*, perangkat lunak *(software)*, data dan jaringan *(network).*

Komponen Sistem Informasi sendiri tersebut saling berinteraksi satu dengan yang lain membentuk suatu kesatuan untuk mencapai sasaran. Komponen tersebut yaitu sebagai berikut :

1. Komponen *hardware.*

   Hardware adalah semua peralatan yang digunakan dalam memproses informasi, misalnya komputer, dapat disimpulkan bahwa hardware dapat bekerja berdasarkan perintah yang telah ditentukan, atau yang juga disebut dengan istilah *instruction set*. Dengan adanya perintah yang dapat dimengerti oleh hardware tersebut, maka hardware tersebut dapat mekakukan berbagai kegiatan yang telah ditentukan oleh pemberi perintah.
2. Komponen *Software*

   Perangkat Lunak *(software)* adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya. perangkat lunak ini merupakan catatan bagi mesin komputer untuk menyimpan perintah, maupun dokumen serta arsip lainnya. *Software* ini mengatur sedemikian rupa sehingga logika yang ada dapat dimengerti oleh mesin komputer. Secara umum, perangkat lunak *(software)* dapat dibagi menjadi tiga bagian, yaitu Sistem Operasi, Bahasa Pemrograman dan Perangkat Lunak Aplikasi.
3. Data

   Data adalah kumpulan dari catatan-catatan, atau potongan dari pengetahuan. Sebuah basis data memiliki penjelasan terstruktur dari jenis fakta yang tersimpan di dalamnya:

penjelasan ini disebut skema. Skema menggambarkan obyek yang diwakili suatu basis data, dan hubungan di antara obyek tersebut. Basis data berperan sebagai penyedia informasi dalam tujuannya untuk mendukung perusahaan melakukan kegiatan operasional.

4. Jaringan *(Network)*
   Jaringan komputer merupakan sistem yang terdiri dari gabungan beberapa perangkat komputer yang didesain untuk dapat berbagi sumber daya, berkomunikasi dan akses informasi dari berbagai tempat antar komputer yang satu dengan komputer yang lain. Beberapa manfaat dari jaringan komputer adalah : Berbagi sumber daya / pertukaran data, mempermudah berkomunikasi/ bertransaksi, membantu akses informasi, dan mampu memberikan akses informasi dengan cepat dan *up-to-date*
5. Sumber Daya Manusia
   Sumber daya manusia ini meliputi pemakai akhir dan pakar sistem. Pemakai akhir adalah orang yang menggunakan informasi yang dihasilkan sistem informasi. Sedangkan pakar sistem informasi adalah orang yang mengembangkan dan mengoperasikan sistem informasi, misalnya *system analyst*, *developer*, operator sistem dan staf administrasi lainnya. Dimensi utama yang harus diperhatikan dengan aset SDM: keahlian teknis, pengetahuan bisnis, dan orientasi pada pemecahan masalah. Dalam penelitian ini Sumber daya manusia yang berperan adalah staff TI dan Non TI serta pihak manajemen perusahaan CV Cempaka.

Seluruh infrastruktur teknologi informasi, termasuk didalamnya perangkat keras *(hardware)* dan perangkat lunak *(software)* merupakan asset perusahaan yang diperguna kan secara bersama-sama. Infrastruktur teknologi informasi ini sangat esensial bagi

perusahaan karena merupakan tulang punggung *(backbone)* untuk terciptanya sistem yang terintegrasi dengan biaya seefektif mungkin, baik untuk keperluan pengembangan, operasional, maupun pemeliharaan.

2.2.3 Aset Informasi Kritis

Aset Informasi Kritis merupakan fasilitias, sistem, dan *tools* yang jika hancur atau rusak akan memiliki dampak yang signifikan terhadap realibility dan operasional proses bisnis di perusahaan.

Dampak yang diakibatkan akan membuat perusahaan menerima kerugian, baik kerugian dari segi waktu pemulihan maupun dari segi keuangan perusahaan.

2.2.4 Keamanan Informasi

Informasi adalah salah satu aset bagi sebuah perusahaan atau organisasi, yang sebagaimana aset lainnya memiliki nilai tertentu bagi perusahaan atau organisasi tersebut sehingga harus dilindungi, untuk menjamin kelangsungan perusahaan atau organisasi, meminimalisir kerusakan karena kebocoran sistem keamanan informasi, mempercepat kembalinya investasi dan memperluas peluang usaha.

Keamanan sistem mengacu pada perlindungan terhadap semua sumberdaya informasi organisasi dari ancaman oleh pihak-pihak yang tidak berwenang. Institusi/organisasi menerapkan suatu program keamanan sistem yang efektif dengan mengidentifikasi berbagai kelemahan dan kemudian menerapkan perlawanan dan perlindungan yang diperlukan. Keamanan sistem dimaksudkan untuk mencapai tiga tujuan utama yaitu; kerahasiaan, ketersediaan dan integritas. [6]

Keamanan sistem Informasi terdiri dari perlindungan terhadap aspek-aspek berikut:

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.
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).

Berdasarkan uraian pengertian keamanan informasi menururt beberapa ahli di atas, dapat disimpulkan bahwa keamanan informasi adalah perlindungan karakteristik informasi *(confidentiality, integrity, availability dan accountability)* baik itu dalam memperoses informasi, menyimpan serta mengirimkanya dalam upaya untuk menjaga keberlangsungan dan memperluas kesempatan bisnis.

2.2.5 Risiko

Pengertian risiko adalah sebagai suatu keadaan yang belum pasti terjadi, dan yang merupakan satu keadaan yang dihadapi oleh manusia dalam setiap kegiatannya dan risiko adalah suatu ketidakpastian dimasa yang datang tentang kerugian.

Definisi ini jelas memandang bahwa risiko berbeda dengan ketidakpastian. Ketidakpastian cenderung mengakibatkan dampak negative yang mana berbeda dengan risiko yang mampu

membawa dampak negatif, positif, dan netral. Semua risiko adalah suatu ketidakpastian, namun tidak semua ketidakpastian merupakan risiko. Pemahaman ini perlu agar tidak terjadi kerancuan. Bila risiko atas rugi dapat diperhitungkan maka jelas bukan lagi ketidakpastian, oleh karena itu penting bagi pihak perusahaan untuk memperhitungkan risiko yang mungkin dapat terjadi.

Para ahli risiko, [7] membedakan risiko statis dan risiko dinamis. Risiko statis adalah risiko dari ketidakpastian atas terjadinya sesuatu dan Risiko dinamis adalah risiko yang timbul karena terjadinya perubahan dalam masyarakat.

2.2.6 Risiko Teknologi Informasi

Menurut [8], kategori risiko TI antara kehilangan informasi potensial dan pemulihannya adalah sebagai berikut. Pertama adalah keamanan. Risiko yang informasinya diubah atau digunakan oleh orang yang tidak berotoritas. Ini termasuk kejahatan komputer, kebocoran internal, dan terorisme cyber. Kedua adalah ketersediaan. Risiko yang datanya tidak dapat diakses seperti setelah kegagalan sistem, karena kesalahan manusia, perubahan konfigurasi, kurangnya pengurangan arsitektur atau akibat lainnya. Ketiga adalah daya pulih. Risiko di mana informasi yang diperlukan tidak dapat dipulihkan dalam waktu yang cukup, setelah sebuah kejadian keamanan atau ketersediaan seperti kegagalan perangkat lunak atau keras, ancaman eksternal, atau bencana alam. Keempat adalah performa. Risiko di mana informasi tidak tersedia saat diperlukan, yang diakibatkan oleh arsitektur terdistribusi, permintaan yang tinggi,

dan topografi informasi teknologi yang beragam. Kelima adalah daya skala.

2.2.7 Manajemen Risiko

Manajemen risiko adalah sebuah bidang ilmu yang membahas bagaimana sebuah perusahaan atau organisasi dapat menerapkan ukuran dalam melakukan pemetaan permasalahan dengan pendekatan manajemen secara komprehensif dan sistematis. Berdasarkan ISO 31000:2009, manajemen risiko adalah aktivitas yang terkoordinir untuk menjalankan dan mengawasi sebuah perusahaan atau organisasi dengan pendekatan risiko.

Institute of Risk Management (IRM) menjelaskan bahwa manajemen risiko adalah sebuah proses yang bertujuan untuk membantu organisasi atau perusahaan dalam memahami, mengevaluasi dan mengambil tindakan untuk risiko-risiko yang muncul, dengan meningkatkan kemungkinan untuk berhasil dan mengurangi kemungkinan kegagalan.

Manajemen risiko adalah sebuah proses yang meliputi identifikasi, penilaian dan menentukan risiko , pengambilan tindakan untuk melakukan mitigasi atau antisipasi serta pemantauan dan melakukan *review* progres dari setiap tahapan yang ada.

Business Continuity Institute menjelaskan bahwa manajemen risiko adalah sebuah budaya, proses dan struktur yang ditempatkan untuk mengelola kesempatan potensial secara efektif dan mencegah efek buruk yang dapat terjadi pada perusahaan atau organisasi.

Oleh karena itulah, dapat disimpulkan bahwa manajemen risiko adalah sebuah proses pengelolaan risiko pada sebuah perusahaan atau organisasi tertentu, yang memiliki tujuan untuk meminimalisasi risiko yang mungkin muncul

2.2.8 Manajemen Risiko Teknologi Informasi

Menurut [9], manajemen risiko merupakan suatu proses yang logis dan sistematis dalam mengidentifikasi, menganalisa, mengevaluasi, mengendalikan, mengawasi, dan mengkomunikasikan risiko yang berhubungan dengan segala aktivitas, fungsi atau proses dengan tujuan perusahaan mampu meminimasi kerugian dan memaksimumkan kesempatan. Implementasi dari manajemen risiko ini membantu perusahaan dalam mengidentifikasi risiko sejak awal dan membantu membuat keputusan untuk mengatasi risiko tersebut.

Teknologi dan Sistem Informasi hampir dapat dipastikan telah diimplementasikan pada setiap perusahaan untuk membantu proses bisnis operasional dan pengambilan keputusan perusahaan. Teknologi dan Sistem Informasi yang berkembang begitu pesat dapat mendatangkan kesempatan sekaligus ancaman bagi perusahaan itu sendiri. Hal ini dibuktikan dengan tingginya kebocoran informasi internal perusahaan dan serangan yang mengancam sistem keamanan komputer perusahaan. Berdasarkan hal-hal itulah perlu diimplementasi sebuah pengelolaan risiko dalam hal teknologi informasi.
Manajemen risiko teknologi informasi adalah pengelolaan risiko teknologi informasi /sistem informasi pada sebuah organisasi atau perusahaan tertentu yang memiliki tujuan untuk meminimalisasi

risiko yang mungkin muncul dengan solusi yang berhubungan dengan aspek teknologi informasi/sistem informasi. [10]

2.2.9 ISO / IEC : 27002 : 2013

ISO 27002 memberikan best practice bagi organisasi dalam mengembangkan dan mengelola standard keamanan dan bagi manajemen untuk meningkatkan keamanan informasi dalam organisasi.

ISO 27002:2005 sangat berhubungan dengan 27001:2005 yaitu ISO / IEC 27001 secara resmi mendefinisikan persyaratan wajib untuk Sistem Manajemen Keamanan Informasi (SMKI). Menggunakan ISO / IEC 27002 untuk menunjukkan kontrol keamanan informasi yang sesuai dalam ISMS, tapi karena ISO / IEC 27002 hanyalah kode praktek / pedoman daripada standar sertifikasi, organisasi bebas untuk memilih dan menerapkan kontrol lain, atau memang mengadopsi alternatif suite lengkap keamanan informasi kontrol seperti yang mereka lihat cocok untuk dipakai.

Tujuan pengendalian dan kontrol dalam ISO / IEC 27002:2005 dimaksudkan untuk diterapkan untuk memenuhi persyaratan diidentifikasi oleh penilaian risiko. ISO / IEC 27002:2005 ini dimaksudkan sebagai dasar umum dan pedoman praktis untuk mengembangkan standar keamanan organisasi dan praktek manajemen keamanan yang efektif, dan untuk membantu membangun kepercayaan dalam kegiatan antar-organisasi. Banyak sistem informasi belum dirancang untuk menjadi aman. Keamanan yang dapat dicapai melalui cara-cara teknis terbatas, dan harus didukung oleh manajemen yang tepat dan prosedur.

Mengidentifikasi yang mengontrol harus di tempat membutuhkan perencanaan yang matang dan perhatian terhadap detail. [11]

Sebelum mengimplementasikan ISO 27002 perlu dilakukan penilaian risiko keamanan informasi pada suatu organisasi. ISO 27002 mengatur mengenai penilaian risiko ini. Penilaian risiko sebaiknya mengidentifikasi, menghitung dan memprioritaskan risiko terhadap kriteria untuk risiko yang bisa diterima dan tujuan yang relevan dengan organisasi. Hasil penilaian risiko sebaiknya memberikan petunjuk dan menetapkan tindakan manajemen yang tepat dan prioritas untuk mengelola risiko keamanan informasi dan untuk mengimplementasikan kontrol yang dipilih untuk melindungi terhadap risiko ini. Proses penilaian risiko dan pemilihan kontrol mungkin membutuhkan sejumlah tindakan untuk mencakup bagian sistem informasi yang berbeda-beda dari individu atau organisasi.

2.2.8.1 Kontrol Standard ISO27002:2013

Kontrol merupakan pedoman pengimplementasian yang menyediakan detail informasi untuk mendukung sebuah sitem dapat tetap berjalan. Berikut ini merupakan kontrol yang ada pada ISO27002:2013 :

5 Information security policies

5.1 Management direction for information security

Kontrol untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi sesuai dengan kebutuhan bisnis dan hukum dan peraturan yang relevan.

6 Organization of information security

6.1 Internal organization

Kontrol untuk membangun kerangka kerja manajemen untuk memulai dan mengontrol pelaksanaan dan Operasi keamanan informasi dalam organisasi.

6.2 Mobile devices and teleworking

Kontrol untuk menjamin keamanan teleworking dan penggunaan perangkat mobile.

7 Human resource security

7.1 Prior to employment

Untuk memastikan bahwa karyawan dan kontraktor memahami tanggung jawab mereka dan cocok melakukan peran yang diterima.

7.2 During employment

Untuk memastikan bahwa karyawan dan kontraktor menyadari dan memenuhi tanggung jawab keamanan informasi mereka.

7.3 Termination and change of employment

Untuk melindungi kepentingan organisasi sebagai bagian dari proses perubahan atau pengakhiran kerja.

8 Asset management

8.1 Responsibility for assets

Kontrol untuk mengidentifikasi aset organisasi dan menentukan tanggung jawab perlindungan yang tepat.

8.2 Information classification

Kontrol untuk memastikan kesesuaian tingkat perlindungan dengan pentingnya informasi bagi organisasi.

8.3 Media handling

Kontrol untuk mencegah tidak sah pengungkapan, modifikasi, penghapusan atau perusakan informasi yang tersimpan pada media.

9 Access control

9.1 Business requirements of access control

Untuk membatasi akses ke fasilitas pengolahan informasi dan informasi.

9.2 User access management

Untuk memastikan akses pengguna yang berwenang dan untuk mencegah akses tidak sah ke sistem dan layanan.

9.3 User responsibilities

Kontrol untuk membuat pengguna bertanggung jawab dan menjaga informasi otentikasi mereka.

10 Cryptography

10.1 Cryptographic controls

Untuk memastikan penggunaan yang tepat dan efektif kriptografi untuk melindungi kerahasiaan, keaslian dan/atau integritas informasi.

11 Physical and environmental security

11.1 Secure areas

Untuk mencegah akses yang tidak sah, kerusakan dan gangguan untuk informasi dan pengolahan informasi fasilitas organisasi.

11.2 Equipment

Kontrol untuk mencegah kehilangan, kerusakan, pencurian dan gangguan pada aset operasional pada perusahaan.

12 Operations security

12.1 Operational procedures and responsibilities

Untuk memastikan operasi yang benar dan aman fasilitas pengolahan informasi.

12.2 Protection from malware

Untuk memastikan bahwa informasi dan informasi mengelola fasilitas dilindungi malware.

12.3 Backup

Untuk melindungi terhadap hilangnya data.

12.4 Logging and monitoring

Untuk merekam peristiwa dan menghasilkan bukti.

12.5 Control of operational software

Untuk memastikan integritas sistem operasional.

12.6 Technical vulnerability management

Untuk mencegah eksploitasi kerentanan teknis.

12.7 Information systems audit considerations

Kontrol untuk meminimalkan dampak dari kegiatan audit pada sistem operasi.

13 Communications security

13.1 Network security management

Untuk menjamin perlindungan informasi dalam jaringan dan mendukung fasilitas pengolahan informasinya.

13.2 Information transfer

Untuk menjaga keamanan informasi ditransfer dalam suatu organisasi dan dengan setiap entitas eksternal.

14 System acquisition, development and maintenance

14.1 Security requirements of information systems

Untuk memastikan bahwa keamanan informasi merupakan bagian integral dari sistem informasi di seluruh siklus hidup. Ini juga mencakup persyaratan untuk sistem informasi yang menyediakan layanan melalui jaringan publik.

14.2 Security in development and support processes

Untuk memastikan bahwa keamanan informasi dirancang dan dilaksanakan dalam siklus hidup pengembangan sistem informasi

14.3 Test data

Untuk menjamin perlindungan data yang digunakan untuk pengujian.

15 Supplier relationships

15.1 Information security in supplier relationship

Untuk memastikan perlindungan aset organisasi yang dapat diakses oleh pemasok.

15.2 Supplier service delivery management

Untuk menjaga tingkat disepakati keamanan informasi dan pelayanan sesuai dengan perjanjian pemasok.

16 Information security incident management

16.1 Management of information security incidents and improvements

Kontrol untuk memastikan konsistensi dan efektifitas pendekatan pengelolaan gangguan terkait keamanan informasi

17 Information security aspects of business continuity management

17.1 Information security continuity

Kontrol yang terkait kontinuitas keamanan informasi harus tertanam dalam sistem manajemen kelangsungan bisnis organisasi.

17.2 Redundancies

Kontrol untuk memastikan ketersediaan fasilitas pengolahan informasi.

18 Compliance

18.1Compliance with legal and contractual requirements

Kontrol untuk menghindari pelanggaran hukum, undang-undang, peraturan atau kontrak kewajiban yang terkait dengan keamanan informasi dan persyaratan keamanan.

18.2 Information security reviews

Kontrol untuk memastikan bahwa keamanan informasi diimplementasikan dan dioperasikan sesuai dengan kebijakan dan prosedur organisasi.

2.2.10 OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation merupakan sebuah perangkat alat, teknik dan metode untuk melakukan penilaian terhadap sistem keamanan informasi berbasis Risiko pada perusahaan. Metode ini memiliki sebuah pendekatan dimana digunakan untuk melakukan sebuah penilaian dalam kebutuhan keamanan informasi dari perusahaan. Metode OCTAVE merupakan metode yang pertama kali dikeluarkan sebelum ada kembangan lainnya seperti OCTAVE-S dan OCTAVE allegro. Metode OCTAVE ini lebih ditunjukkan kepada perusahaan yang memiliki lebih dari 300 karyawan [12].

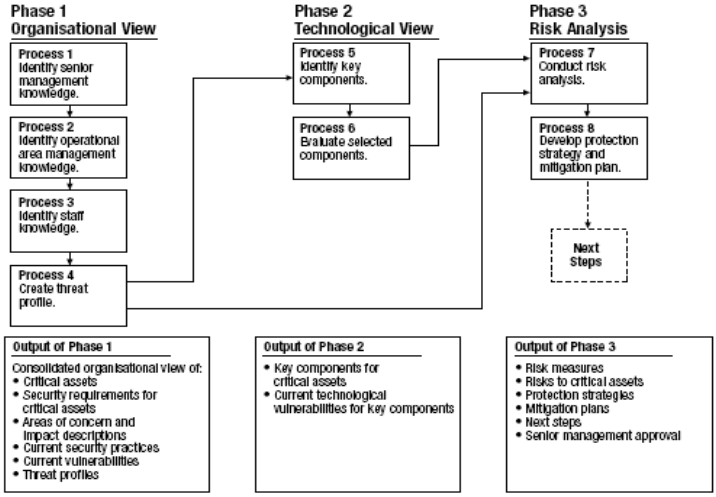
Karakter dari OCTAVE adalah :

1. *Self-directed :* disini seluruh elemen atau divisi yang terdapat pada perusahaan bekerjasama dengan kepala divisi sebagai

penanggung jawab teknologi informasi sehingga kebutuhan dari keamanan dapat terdefinisikan

2. *Flexible :* Setiap metode yang digunakan dapat menyesuaikan dengan lingkungan bisnis perusahaan, tujuan keamanan dan ketahanan dan tingkat kemampuan perusahaan
3. *Evolved :* Metode ini menggerakkan perusahaan untuk lebih mengutamakan keamanan informasi dalam konteks bisnis.

OCTAVE melihat semua aspek Risiko keamanan informasi dari fisik, teknis dan sudut pandang orang. Dengan metode ini akan digunakan waktu untuk mempelajari proses, Sehingga membantu organisasi untuk lebih memahami aset, ancaman, kerentanan dan risiko . Sehingga dapat membuat keputusan yang lebih baik tentang bagaimana untuk menangani risiko tersebut. Terdapat beberapa fase pada metode Octave, dijelaskan pada gambar 2.1



Gambar 2.1 Bagan OCTAVE

Fase 1 : Melihat dari sisi organisasi

a. Proses

- Mengidentifikasi berdasarkan pengetahuan pihak manajemen senior
- Mengidentifikasi berdasarkan pengetahuan pihak manajemen wilayah operasional
- Mengidentifikasi berdasarkan pengetahuan staff
- Membuat Profil ancaman

b. Output

- Melakukan *list* aset penting pada organisasi
- Kebutuhan keamanan bagi aset penting
- *List* upaya untuk melindungi aset informasi penting
- *List* ancaman terhadap aset kritis
- *List* kelemahan kebijakan pada organisasi

Fase 2: Melihat sisi teknologi

a. Proses

- Melakukan identifikasi komponen kunci
- *Evaluate* Infrastruktur komponen

b. Output

- *List* Komponen utama dan infrastruktur
- Mendapatkan Identifikasi kerentanan teknologi pada organisasi

Fase 3: Menganalisa risiko teknologi informasi

a. Proses

- Melakukan analisa risiko
- Mengembangkan strategi keamanan

b. Output

- Daftar Risiko terhadap aset kritis

- Hasil Pengukuran tingkat Risiko
- Strategi keamanan berdasarkan implementasi Octave
- Rencana-rencana dari pengurangan atau mitigasi risiko

2.2.11 FMEA *(Failure Mode and Effect Analysis)*

Failure Mode and Effect Analysis (FMEA) adalah suatu prosedur terstruktur untuk mengidentifikasikan dan melakukan pencegahan sebaik mungkin terhadap mode kegagalan. FMEA digunakan untuk mengidentifikasi berbagai sumber dan penyebab dari suatu masalah kualitas. Suatu mode kegagalan merupakan apa saja yang termasuk berbagai hal negatif (biasanya out of scope) [13].

Terdapat beberapa tahapan dari FMEA yaitu:

1. Menentukan komponen terlebih dahulu dari sistem yang akan dianalisis.
2. Mengidentifikasi kegagalan yang paling potensial dari sistem yang dianalisis
3. Melakukan identifikasi terhadap akibat dari potensial kegagalan dari sistem
4. Melakukan identifikasi terhadap penyebab dari kegagalan ketika sistem sedang berjalan
5. Melakukan brainstorming dan menetapkan nilai dalam bentuk
   - *Severity :* dampak dari kesalahan pada system
   - *Occurence :* Frekuensi dari kesalahan yang terjadi
   - *Detection :* Kemampuan pengendalian Risiko yang terjadi
   - *Risk Potential Number :* Penilaian terhadap potensi yang memiliki Risiko yang paling tinggi.

2.2.12 SOP *(Standart Operating Procedure)*

Standard Operating Procedure (SOP) adalah serangkaian instruksi tertulis yang dibakukan (terdokumentasi) mengenai

berbagai proses penyelenggaraan administrasi perusahaan, bagaimana dan kapan harus dilakukan, dimana dan oleh siapa dilakukan.

Standar Operasional Prosedur merupakan suatu pedoman atau acuan untuk melaksanakan tugas pekerjaan sesuai dengan fungsi dan alat penilaian kinerja instansi pemerintah berdasarkan indikator!indikator teknis, administratif dan prosedural sesuai tata kerja, prosedur kerja dan sistem kerjapada unit kerja yang bersangkutan.

2.2.11.1 Kriteria dan Format SOP

Dalam membuat SOP, diperlukan adanya kriteria dan format yang berfungsi sebagai standarisasi dokumen. Tidak adanya aturan mengenai batasan panjang pendeknya SOP memberikan kemudahan bagi organisasi dalam membuat SOP karena dapat disesuaikan dengan kebutuhan organisasi. Namun, SOP yang ringkas akan memudahkan para pengguna SOP. Penentuan kriteria dan format dalam SOP juga dapat disesuaikan dengan kebutuhan organisasi. Yang perlu diperhatikan dalam penyusunan SOP adalah terdapat langkah-langkah yang jelas, terstruktur dan terperinci. Hilangnya salah satu langkah penting akan menyebabkan penyimpangan dalam menjalankan prosedur. Terdapat tujuh kriteria SOP yang dapat digunakan sebagai acuan, yaitu [14]:

1. Spesifik
2. Lengkap
3. Mudah dipahami
4. Mudah diaplikasikan
5. Mudah dikontrol dan diubah
6. Mudah diaudit

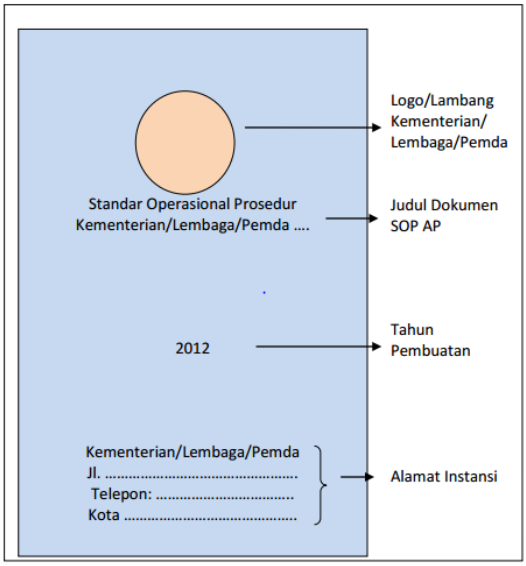
2.2.11.2Dokumen SOP

Dalam penyusunan dokumen SOP, menurut perturan pemerintah (Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 35 Tahun 2012 Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan) didasarkan pada format SOP yang telah disusun. Namun ketidakbakuan format SOP menyebabkan organisasi dapat menyusun dokumen SOP sesuai dengan kebutuhannya masing-masing. Format SOP dipengaruhi oleh tujuan pembuatan SOP. Sehingga apabila tujuan pembuatan SOP maka format SOP juga dapat berbeda .

Sesuai dengan anatomi dokumen SOP yang pada hakekatnya berisi prosedur-prosedur yang distandarkan dan membentuk satu kesatuan proses, maka informasi yang dimuat dalam dokumen SOP terdiri dari 2 macam unsur, yaitu Unsur Dokumentasi dan Unsur Prosedur. Adapun informasi yang terdapat dalam Unsur Dokumentasi dan Unsur Prosedur adalah [15]:

1. Unsur Dokumentasi
   Unsur dokumentasi merupakan unsur dari dokumen SOP yang berisi hal-hal terkait dalam proses pendokumentasian SOP sebagai sebuah dokumen. Adapun unsur dokumen SOP antara lain:
   a. Halaman Judul (*Cover*)
      Merupakan halaman pertama sebuah dokumen SOP. Halaman judul berisi informasi mengenai:
      - Judul SOP
      - Instansi / Satuan Kerja
      - Tahun pembuatan
      - Informasi lain yang diperlukan

Halaman judul dapat disesuaikan sesuai dengan kebutuhan organisasi. Berikut adalah contoh halaman judul sebuah dokumen SOP yang dapat dilihat pada Gambar 2.2 :



Gambar 2.2 Bagan Penyusunan SOP
(Sumber: Pedoman Penyusunan SOP Administrasi Pemerintahan, 2012)

b. Keputusan Pimpinan Kementrian / Lembaga / Pemda
Setelah halaman judul, maka disajikan keputusan Pimpinan Kementrian / Lembaga / Pemda terkait ketetapan dokumen SOP ini. Hal ini bertujuan sebagai dasar hukum yang berlaku dan sifatnya adalah mengikat. Selain itu keputusan pimpinan dalam dokumen SOP merupakan pedoman bagi semua pegawai untuk melaksanakan SOP.

c. Daftar isi dokumen SOP

Daftar isi dibutuhkan untuk membantu pencarian informasi secara lebih cepat dan tepat. Selain itu di dalam daftar isi terdapat pula informasi mengenai perubahan / revisi yang dibuat untuk bagian tertentu dari SOP

d. Penjelasan singkat penggunaan

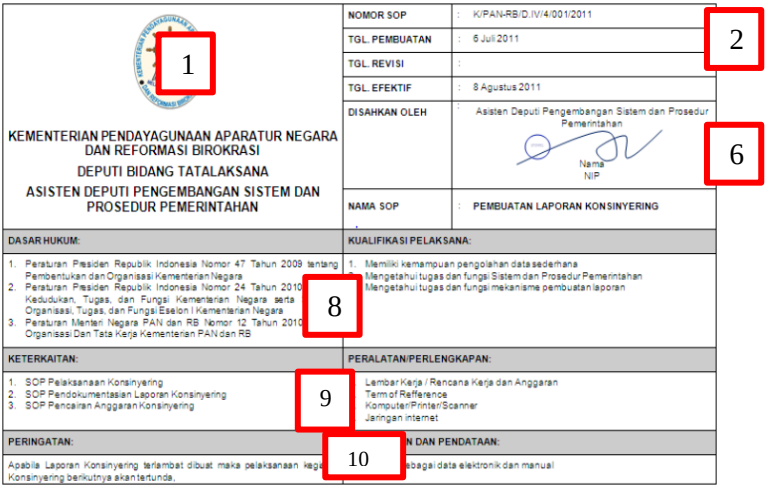
Sebagai sebuah dokumen yang menjadi manual, maka dokumen SOP hendaknya memuat penjelasan bagaimana membaca dan menggunakan dokumen tersebut. Di dalam bagian ini terdapat informasi mengenai Ruang Lingkup yang berisi penjelasan tujuan pembuatan prosedur, Ringkasan yang berisi ringkasan singkat mengenai prosedur, dan Definisi/Pengertian-pengertian umum yang berisi beberapa definisi yang terkait dengan prosedur yang distandarkan.

2. Unsur Prosedur

Unsur prosedur merupakan unsur dari dokumen SOP yang berisi hal-hal inti dari dokumen SOP. Unsur prosedur dibagi dalam dua bagian, yaitu Bagian Identitas dan Bagian *Flowchart*. Adapun penjelasan unsur prosedur adalah:

a. Bagian Identitas

Berikut adalah contoh bagian identitas SOP yang dapat dilihat pada Gambar 2.3 :



Gambar 2.3 Contoh Bagian SOP
(Sumber: Pedoman Penyusunan SOP Administrasi Pemerintahan, 2012)

Di dalam bagian identitas berisi hal-hal yang tertulis pada tabel 2.1 berikut :

Tabel 2.1 Penjelasan Identitas SOP

No.	Bagian Identitas	Penjelasan
1.	Logo dan Nama Instansi/ Unit Kerja	Nomenklatur unit organisasi pembuat
2.	Nomor SOP	Nomor prosedur yang di-SOP-kan sesuai dengan tata naskah dinas yang berlaku di Kementerian/Lembaga/Pemda
3.	Tanggal Pembuatan	Tanggal pertama kali SOP dibuat berupa tanggal selesainya SOP dibuat bukan tanggal dimulainya pembuatannya

No.	Bagian Identitas	Penjelasan
4.	Tanggal Revisi	Tanggal SOP direvisi atau tanggal rencana ditinjau ulangnya SOP yang bersangkutan
5.	Tanggal Efektif	Tanggal mulai diberlakukan SOP atau sama dengan tanggal ditandantanganinya dokumen SOP
6.	Pengesahan oleh pejabat yang berkompeten pada tingkat satuan kerja	Item pengesahan berisi nomenlektur jabatan, tanda tangan, nama pejabat yang disertai dengan NIP serta stempel/cap instansi
7.	Judul SOP	Judul prosedur yang di-SOP-kan dengan kegiatan yang sesuai dengan tugas dan fungsi yang dimiliki
8.	Dasar Hukum	Berupa peraturan perundang-undangan yang mendasari prosedur yang diSOP-kan berserta aturan pelaksanaannya
9.	Keterkaitan	Penjelasan mengenai keterkaitan prosedur yang distandarkan dengan prosedur lain distandarkan
10.	Peringatan	Penjelasan mengenai kemungkinan-kemungkinan yang terjadi ketika prosedur dilaksanakan atau tidak dilaksanakan

No.	Bagian Identitas	Penjelasan
11.	Kualifikasi Pelaksana	Penjelasan mengenai kualifikasi pelaksana yang dibutuhkan dalam melaksanakan perannya pada prosedur yang distandarkan
12.	Peralatan dan Perlengkapan	Penjelasan mengenai daftar peralatan utama (pokok) dan perlengkapan yang dibutuhkan yang terkait secara langsung dengan prosedur yang di-SOP-kan
13.	Pencatatan dan Pendanaan	Berisi informasi mengenai hal-hal yang perlu didata dan dicatat oleh pejabat tertentu. Dalam kaitan ini, perlu dibuat formulir-formulir tertentu yang akan diisi oleh setiap pelaksana yang terlibat dalam proses

b. Bagian *Flowchart*

Di dalam bagian *flowchart* ini berisi uraian mengenai langkah-langkah (prosedur) kegiatan beserta mutu baku dan keterangan yang diperlukan. Bagian ini berisi langkah-langkah secara sistematis. Adapun isi bagian ini adalah Nomor kegiatan; Uraian kegiatan yang berisi langkah-langkah (prosedur); Pelaksana yang merupakan pelaku kegiatan; Mutu baku yang berisi kelengkapan, waktu, output, dan keterangan.

Berikut adalah contoh bagian *flowchart* SOP yang dapat dilihat pada gambar 2.4.

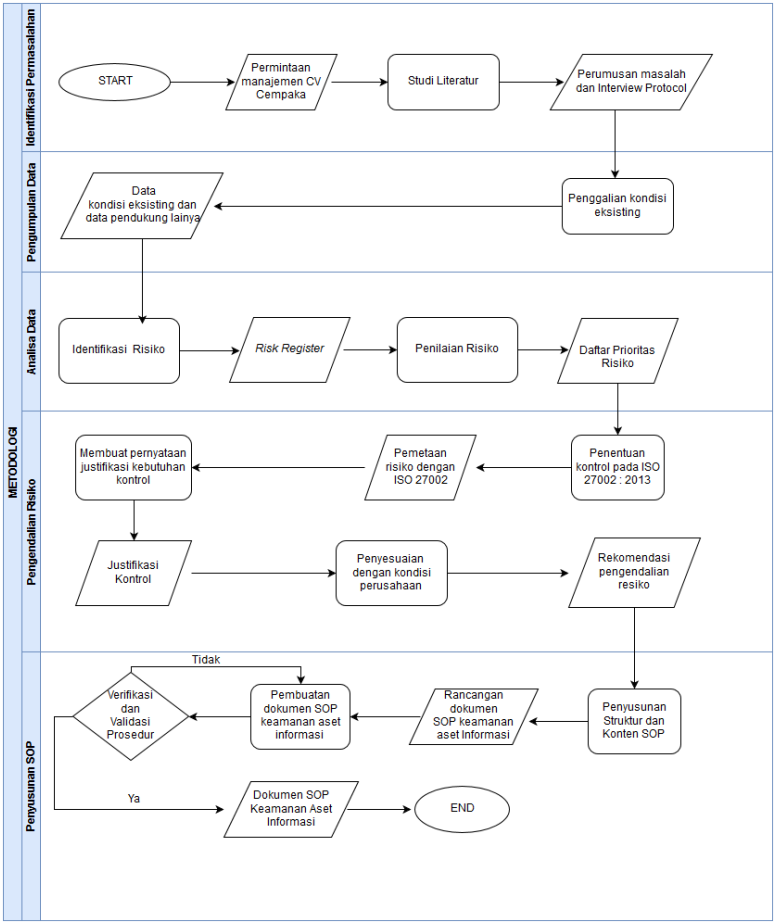
No.	Kegiatan	Pelaksana				Mutu Baku			Keterangan
		Kabid	Kasubid	Analis	Asdep	Kelengkapan	Waktu	Output	
1.	Menugaskan Kasubid untuk mempersiapkan konsep laporan konsinyering					Agenda Kerja	15 menit	Disposisi	
2.	Memerintahkan analis untuk mengumpulkan bahan laporan konsinyering					Disposisi	15 menit	Disposisi	
3.	Mengumpulkan dan menyerahkan bahan konsinyering kepada Kasubid					Disposisi	1 hari	Bahan Laporan, Disposisi	SOP Pengumpul-an Bahan
4.	Mengonsep laporan konsinyering dan menyerahkan kepada Kabid					Bahan Laporan	2 jam	Konsep Laporan, Disposisi	
5.	Memeriksa konsep laporan konsinyering. Jika setuju menyampaikan kepada Asdep. Jika tidak setuju menyerahkan kepada Kasubid untuk diperbaiki.		Tidak / Ya			Konsep Laporan	1 jam	Draft Laporan, Disposisi	
6.	Memeriksa draft laporan konsinyering. Jika setuju menandatangani dan menyerahkan kepada Kabid. Jika tidak setuju mengembalikan kepada Kabid untuk diperbaiki.				Tidak / Ya	Draft Laporan	1 jam	Laporan, Disposisi	
7.	Menyerahkan laporan konsinyering kepada Kasubdit untuk didokumentasikan.					Laporan	10 menit	Disposisi	
8.	Menyerahkan laporan konsinyering kepada Analis untuk didokumentasikan.					Laporan	10 menit	Disposisi	
9.	Mendokumentasikan Laporan Konsinyering.					Laporan	15 menit	Laporan, Bukti Dokumentasi	

Gambar 2.4 Contoh Bagian Flowchart SOP
(Sumber: Pedoman Penyusunan SOP Administrasi Pemerintahan, 2012)

Berkaitan dengan penelitian tugas akhir ini, kriteria dan format dokumen SOP dapat menjadi acuan dalam penyusunan dokumen SOP manajemen akses di CV Cempaka Tulungagung. Dengan adanya dokumen SOP ini maka pengguna SOP dapat melakukan prosedur dengan sistematis dan adanya dasar hukum dalam penggunaan SOP. Selain itu, SOP juga merupakan salah satu bentuk kegiatan tata kelola pada suatu organisi.

BAB III
METODOLOGI

Bab ini menggambarkan metodologi yang akan digunakan selama penelitian berlangsung pada gambar 3.1, termasuk tahapan yang dilakukan dalam menyusun dokumen SOP.



Gambar 3.1 Metodologi Penelitian

3.1 Tahap Identifikasi Permasalahan

Tahapan ini merupakan langkah awal untuk memulai penyusunan tugas akhir ini. Masukkan dari permasalahan yang ada adalah datang dari permintaan manajemen perusahaan, mengenai pentingnya keamanan aset informasi serta daftar kelemahan sistem yang dapat menimbulkan ancaman di CV Cempaka.
Pada tabel 3.1 berikut merupakan detail dari tahap identifikasi permasalahan :

Tabel 3.1 Penjelasan Identifikasi Permasalahan

Input	Proses	Output
Permintaan manajemen CV Cempaka Tulungagung	Studi Literatur	• Rumusan permasalahan • Latar belakang

Proses identifikasi permasalahan ini didukung dengan adanya studi literatur yang dilakukan untuk memperkuat data dan sebagai referensi untuk memberikan aspek integritas pada penelitian ini. Studi literatur dilakukan dari buku, jurnal, paper, dan informasi yang ada di internet. Tahapan ini akan menghasilkan rumusan permasalahan, latar belakang penelitian pada perusahaan yang dijadikan sebagai bahan dasar untuk memulai penelitian ini dan membuat interview protokol untuk proses selanjutnya.

3.2 Tahap Pengumpulan Data

Pada tahap ini dilakukan pengumpulan data dan informasi kondisi eksisting yang dapat digunakan sebagai dasar penelitian Tugas Akhir ini. Aktivitas dijelaskan pada tabel 3.2 sebagai berikut:

Tabel 3.2 Pengumpulan data

Input	Proses	Output
• Rumusan permasalahan • Latar belakang	1. Wawancara 2. Analisa Dokumen	• Aset informasi penting perusahaan • Kebutuhan keamanan pada aset • Risiko terkait teknologi informasi • Sumberdaya yang terkait • Praktik keamanan yang dilakukan perusahaan

Proses pengumpulan data dilakukan dengan cara wawancara terstruktur dan tidak terstruktur, serta mempelajari prosedur, kebijakan dan laporan tahunan perusahaan yang telah dilakukan sebelumnya. Validasi kepada pihak perusahaan penting untuk dilakukan, dengan tujuan untuk menunjang aspek kebenaran (*correctness*) dan integritas dari sebuah penelitian.

Wawancara dilakukan kepada departemen perusahaan yang aset informasinya terkait dengan proses bisnis, untuk menggali data dan informasi atas penelitian yang dilaksanakan. Sedangkan proses observasi ini dilakukan mengumpulkan data melalui studi lapangan langsung untuk menganalisis risiko. Selain itu observasi

ini dilakukan untuk mengamati Teknologi Informasi yang digunakan perusahaan untuk menentukan aset dan sumberdaya yang terkait risiko dalam proses bisnis perusahaan. Dokumen perusahaan juga dipelajari terkait peraturan pemerintah yang berkaitan dengan perusahaan, kebijakan, prosedur dan laporan tahunan, hal ini dilakukan untuk membuat penelitian ini sesuai dengan kebutuhan dan kondisi perusahaan.

3.3 Tahap Analisa data

Tahap menganalisa informasi identifikasi risiko merupakan aktivitas analisa dan penilaian risiko dengan menggunakan metode Octave dan FMEA. Pada tabel 3.3 merupakan detail pada tahap analisa informasi teridentifikasi :

Tabel 3.3 Analisa data

Input	Proses	Output
• Aset informasi penting perusahaan • Kebutuhan keamanan pada aset • Ancaman yang pernah terjadi terkait TI • Praktik keamanan yang dilakukan perusahaan • Sumberdaya terkait	1. Identifikasi 2. Penilaian risiko	• Risk Register • Daftar prioritas risiko

3.3.1 Identifikasi risiko

Tahapan proses identifikasi risiko ini menggunakan framework Octave, risiko tersebut akan diidentifikasi untuk melihat dan meastikan hal yang menjadi ancaman bagi operasional perusahaan, selain itu untuk mengidentifikasi praktek pengamanan yang telah dilakukan serta fungsi yang terlibat didalamnya, seberapa sering risiko terjadi beserta penyebab dan dampaknya. Identifikasi risiko ini terjadi pada komponen perangkat keras, perangkat lunak, manusia, dan data.

3.3.2 Penilaian risiko

Setelah itu dilanjutkan dengan melakukan penilaian menggunakan metode FMEA *(Failure Mode and Effect Analysis).* Dengan metode ini akan dilihat kecenderungan, dampak, dan deteksi yang diberikan pada setiap risiko TI/SI yang ada. Selanjutnya dilakukan proses perhitungan skor prioritas risiko (kecenderungan x dampak x deteksi). Setelah dilakukan perhitungan prioritas risiko maka akan muncul risiko yang berada pada kondisi high dan very high yang digunakan dalam pembentukan SOP.

Pada proses ini akan menghasilkan tabel risk register dan daftar prioritas risiko yang dapat dijadikan bahan dalam melakukan analisis pembuatan dokumen SOP keamanan aset informasi untuk CV Cempaka.

3.4 Tahap Pengendalian risiko

Hasil dari analisis dan penilaian risiko akan digunakan sebagai masukan dalam tahap penentuan pengendalian risiko. Dalam tahap pengendalian risiko dilakukan penentuan tujuan kontrol

berdasarkan kerangka kerja ISO27002:2013. Penentuan tujuan kontrol tersebut dilakukan dalam dua tahap yaitu pemetaan risiko dan penentuan pengendalian dengan kontrol pada kerangka ISO27002:2013. Pada tabel 3.4 merupakan detail dari tahap perlakuan risiko :

Tabel 3.4 Pengendalian risiko

Input	Proses	Output	Verifikasi
• Risk Register • Daftar Prioritas Risiko	1. Menentukan kontrol yang dibutuhkan pada ISO 27002 :2013 2. Membuat pernyataan justifikasi kebutuhan kontrol 3. Melakukan penyesuaian dengan perusahaan	• Pemetaan risiko dengan kontrol ISO 27002 :2013 • Justifikasi kontrol • Rekomendasi pengendalian risiko	

3.4.1 Penentuan Kontrol yang Dibutuhkan pada ISO 27002:2013

Setelah di dapatkan hasil penilaian risiko yang akan menentukan seluruh kontrol yang dibutuhkan untuk mengimplementasikan opsi pegendalian risiko yang telah ditentukan. Penentuan tujuan kontrol akan didasarkan pada kontrol yang ada pada kontrol yang ada pada kerangka kerja ISO27002:2013. Dalam proses penentuan tujuan kontrol, setiap risiko akan dipetakan langsung kedalam kontrol yang relevan dan sesuai dengan kebutuhkan..

3.4.2 Pernyataan Justifikasi Kebutuhan Kontrol

Dalam bagian ini, merupakan proses membuat sebuah pernyataan dari kebutuhan kontrol yang telah dipilih. akan dibuat sebuah daftar risiko, rekomendasi pengendalian risiko dan justifikasi dari masing masing kontrol. Hasil luaran tersebut adalah sebuah tabel yang berisikan justifikasi kontrol.

3.4.3 Penyesuaian dengan kondisi perusahaan

Dalam bagian ini, merupakan proses penyesuaian kontrol yang sudah ditentukan dengan kondisi pada perusahaan yaitu menyesuaikan aktifitas-aktifitas yang dilakukan dalam suatu kontrol agar dapat diimplementasikan sepenuhnya oleh perusahaan. Sehingga mendapatkan rekomendasi pengendalian risiko yang tepat

3.5 Tahap Penyusunan SOP

Pada tahap penyusunan SOP ini terdapat tiga aktivitas yang dilakukan oleh penulis. Pada tabel 3.5 merupakan detail penjelasan :

Tabel 3.5 Penyusunan SOP

Input	Proses	Output	Verifikasi dan Validasi
• Rekomendasi pengendalian risiko • Pemetaan risiko dengan kontrol ISO 27002 :2013 • Justifikasi kontrol	1. Penyusunan struktur dan konten SOP 2. Pembuatan dokumen SOP keamanan aset informasi	Perancangan dokumen SOP keamanan aset informasi	Verifikasi dan validasi kepada pihak manajemen CV Cempaka

Proses pembuatan dokumen SOP adalah proses pengembangan dari perancangan konten dokumen SOP. Dokumen SOP yang dibuat akan disesuaikan dengan konten dokumen yang sudah divalidasi terhadap pihak CV Cempaka. Pembuatan dokumen SOP akan didasarkan pada standard pembuatan dokumen SOP dan kontrol yang ada didalamnya.

Untuk memastikan kesesuaian prosedur yang dibuat maka dilakukan verifikasi pada pihak CV cempaka dengan melakukan beberapa pengujian prosedur, menanyakan keterangan dengan pihak yang berhubungan dengan prosedur SOP dan hasil dari pengujian serta status untuk menunjukan penerimaan atau ketepatan prosedur. Setelah melakukan verifikasi dilakukan validasi dokumen SOP yang dibuat sehingga dokumen ini sudah sesuai dan dapat digunakanperusahaan CV Cempaka.

BAB IV
PERANCANGAN KONSEPTUAL

Bab ini menjelaskan tentang perancangan konseptual dalam pengerjaan tugas akhir ini, yaitu perancangan secara detail dari setiap tahapan pengerjaan yang telah dijerlaskan pada Bab III. Dalam tahap perancangan, terdapat tiga proses utama yaitu penentuan subjek dan objek penelitian, pembuatan daftar pertanyaan dalam bentuk *interview protocol* untuk wawancara pengalian data dan perancangan penilaian risiko serta perancangan SOP.

4.1 Objek Penelitian

Penelitian ini dilakukan pada perusahaan yang bergerak dibidang produksi rokok, yaitu CV Cempaka. Objek yang akan diteliti adalah keamanan aset informasi pada CV Cempaka. Objek keamanan aset informasi dalam CV Cempaka merupakan salah satu bagian dari keamanan informasi yang sedang dikembangkan. Dimana dengan terkelolanya keamanan aset informasi dengan baik pada CV Cempaka dapat meningkatkan keefektifan proses bisnis yang berjalan.

Proses perbaikan keamanan data untuk CV Cempaka dalam penelitian ini akan dikembangkan dari segi manajamen yaitu dengan membuat sebuah prosedur berdasarkan kerangka kerja ISO27002:2013.

4.1.1 Profil dan Sejarah CV Cempaka

CV. Cempaka merupakan perusahaan swasta yang sudah ada sejak tahun 1982 di Indonesia. Yang mana core bisnisnya adalah bisnis rokok. Dengan core bisnis pada bisnis rokok, CV Cempaka memiliki berbagai produk terkait dengan bisnis yang mereka geluti sekarang ini. CV Cempaka dan afiliasinya memproduksi, memasarkan dan mendistribusikan rokok di Indonesia, yang

meliputi cempaka super long size, cempaka super, cempaka filter light dll.

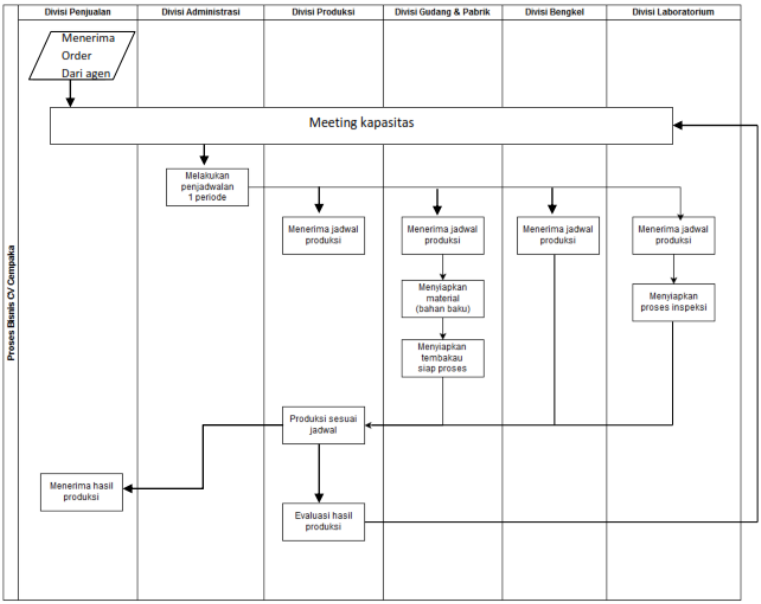
Pada tanggal 1 April 1982 yaitu sejak dikeluarkan surat ijin usaha dengan dengan nomor : B 79/B2/HO/KDH/AA oleh pemerintahan Daerah Tingkat II Tulungagung, serta ijin produksi dari Bea Cukai nomor : 00481/F maka berdirilah perusahaan rokok dengan nama "PR Cempaka" di tulungagung dengan bentuk CV.

Seiring makin berkembangnya perusahaan, maka cempaka berusaha mendapatkan ijin usaha lain yaitu ijin tempat usaha berdasarkan undang-undang gangguan (HO) nomor 530.08/08/445.14/1985 yang disahkan oleh Bupati KDH Tingkat II Tulungagung. Sehingga berdirilah perusahaan rokok baru "Cempaka" pada tahun 1982.

Peningkatan produksi yang dicapai mempengaruhi juga perubahan inventaris dan jumlah tenaga kerja. Dengan perkembangan yang semakin bertambah maju, sampai sekarang ini perusahaan mempunyai ribuan tenaga kerja dan hasil produksi telah disebarkan ke pelosok tanah air.

4.1.2 Proses Bisnis Inti CV Cempaka

Pada gambar 4.1 berikut merupakan gambaran proses bisnis pada CV Cempaka:



Gambar 4.1 Bagan proses bisnis cempaka

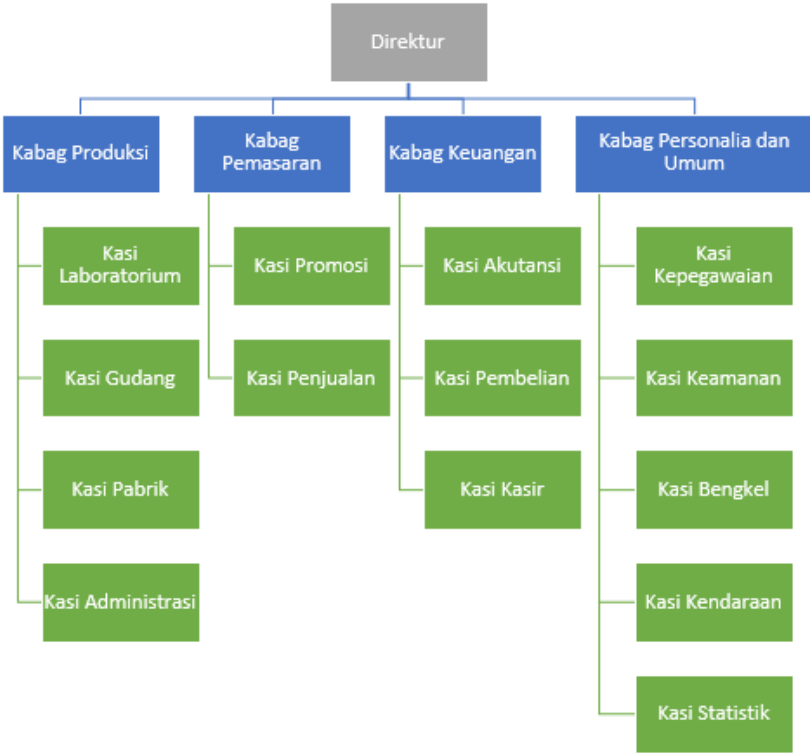
Proses Bisnis di CV Cempaka bermula dari divisi penjualan yang menerima order dari agen. Kemudian dari divisi penjualan mengadakan meeting dengan bagian produksi yaitu divisi pabrik, divisi administrasi, dan divisi gudang dan bagian personalia yaitu divisi bengkel. Dari hasil meeting tersebut akan digunakan untuk perencanaan dan penjadwalan seminggu ke depan guna memenuhi order tersebut. Administrasi PPIC (Production Planning and Inventory Control) akan merencanakan dan menjadwalkan produksi. Dalam kegiatan produksi tersebut terdapat banyak elemen yang harus dipertimbangkan dari masing-masing bagian. Misalkan pada divisi gudang sanggup atau tidak

dalam memenuhi kebutuhan tembakau pada divisi pabrik. divisi gudang merupakan divisi yang berkewajiban untuk menyuplai tembakau ke divisi pabrik. Untuk bagian bengkel dimungkinkan terjadi perawatan berkala terhadap mesin.

Hal tersebut memungkinkan menganggu pemenuhan order atau tidak. Divisi gudang masih memiliki stok material pendukung atau tidak. Divisi laboratorium juga harus merencanakan berapa sampel yang harus diambil pada setiap kali inspeksi. Perencanaan dan penjadwalan tersebut juga dapat berubah secara mendadak misalkan terdapat kejadian insidental. Sebagai contoh, ketika terjadi banjir di pihak supplier dan tidak dimungkinkan untuk mengirim material ke CV Cempaka atau mungkin terjadi kerusakan mesin secara mendadak. Hal tersebut biasanya diatasi dengan meeting darurat seketika itu juga. Pada akhir produksi, produk rokok tersebut akan dikirim ke divisi penjualan sebelum nantinya rokok tersebut akan dipasarkan.

4.1.3 Struktur Organisasi CV Cempaka

Fungsional bisnis pada CV Cempka digambarkan dalam sebuah struktur organisasi yang akan dijelaskan pada subab struktur organisasi dan proses bisnis yang berjalan dalam CV Cempaka yang akan dijelaskan adalah proses bisnis yang berkaitan dalam penelitian pada gambar 4.2 merupakan struktur organisasi pada CV Cempaka.



Gambar 4.2 Struktur Organisasi CV Cempaka

4.1.4 Proses Bisnis yang menggunakan teknologi informasi

Adapun beberapa proses bisnis yang terkait dengan penelitian dan berpengaruh dengan proses bisnis inti yang di tulis pada tabel 4.1 berikut :

Tabel 4.1 Fungsional Bisnis CV Cempaka

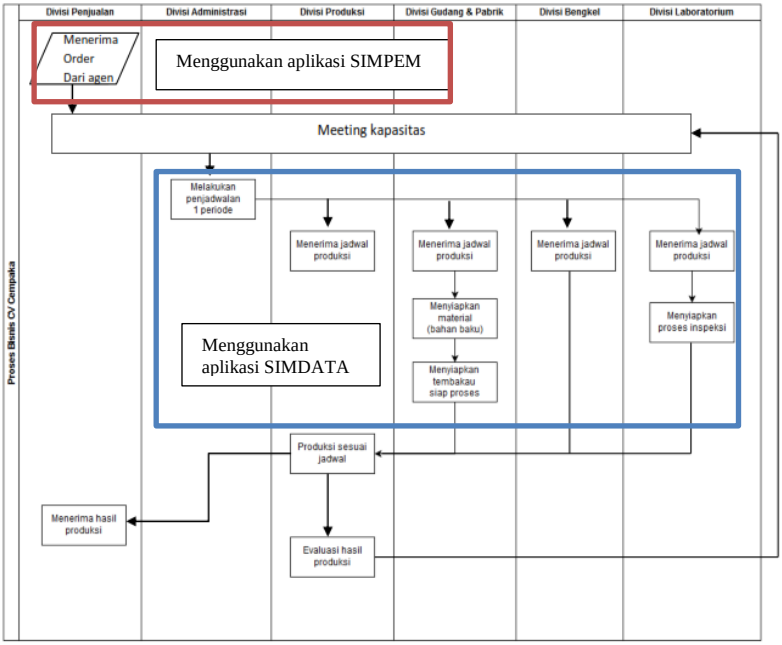
Fungsional Bisnis	Proses Bisnis Terkait Sistem Informasi	Aset TI digunakan
Pemasaran	Perencanaan kegiatan pemasaran dan penjualan	• Sistem aplikasi • Server • PC • Kabel Lan
	Pencatatan distributor	
	Promosi produk	
Akutansi Keuangan	Laporan Keuangan	• Sistem aplikasi • Server • PC • Kabel Lan
	Pencatatan piutang	
	Pencatatan aktiva tetap	
	Pengelolaan perkiraan kas	
Personalia dan Umum	Pengadaan tenaga kerja	• Sistem aplikasi • Server • PC • Kabel Lan
	Pengaturan jam kerja karyawan	
	Pencatanan pegawai	
	Pencatatan Fasilitas Kantor	
Produksi	Penyediaan bahan baku	• Sistem aplikasi • Server • PC • Kabel Lan
	Penjadwalan produksi	
	Pemeriksaan kualitas produk	
	Pengelolaan inventori	

Dalam proses melakukan perencanaan perhitungan bahan baku, penjadwalan produksi, pengelolaan inventori, pemeriksaan

kualitas produk, pencatatan pegawai, pencatatan fasilitas kantor, pencatatan distributor, pencatatan piutang, laporan bulanan, pencatatan aktiva, dan lain lain pada CV Cempaka menggunakan sistem informasi, yang mana keamanan aset informasi masih belum begitu diperhitungkan dampaknya. Sehingga bagian personalia selaku penanggung jawab harus memastikan keamanan aset informasi yang dimiliki agar proses bisnis perusahaan tidak terganggu.

4.1.5 Hubungan proses bisnis inti dan dukungan IT

Pada gambar 4.3 berikut merupakan gambaran penggunaan IT dalam proses bisnis inti Cempaka



Gambar 4.3 Hubungan proses bisnis inti dengan sistem informasi

Dalam proses penerimaan order dari agen maupun untuk melakukan penjadwalan sebuah produksi diperlukan adanya

sebuah sistem informasi untuk mendukung proses bisnis utama yaitu memproduksi rokok. SIMPEM (sistem informasi pemasaran) ini digunakan untuk melakukan setiap pencatatan pemasaran dan penjualan produk dimana data dari simpem ini sangatlah penting dan rahasia selain itu dalam proses bisnis CV cempaka menggunakan SIMDATA (Sistem informasi penjadwalan dan pendataan) digunakan untuk setiap kegiatan penjadwalan produksi maupun cek gudang ada pada aplikasi ini data dari simpem ini sangatlah penting dan rahasia, sehingga keamanan dari aset informasi sangatlah penting untuk dijaga agar proses bisnis tidak terganggu. Selain kedua aplikasi tersebut juga digunakan aplikasi SISKA (Sistem informasi Akuntansi) dan SIADMIN (Sistem informasi administrasi) juga penting dalam melakukan perhitungan dan pedataan akuntansi keuangan dan administrasi perusahaan. Keempat sustem informasi tersebut juga berhubungan dengan beberapa aset informasi yang dinilai kritis antara lain :

- Server
- PC
- Kabel Lan
- Karyawan/Administrator
- Wifi
- Router

Aset diniliai kritis karena jika aset diatas tidak berfungsi maka sistem tidak dapat digunakan dan secara tidak langsung akan menghambat proses bisnis yang berlangsung.

4.2 Pengumpulan Data dan Informasi

Pengumpulan data dengan teknik wawancara, yang akan dilaksanakan terhadap Bagian Personalia dan umum CV Cempaka selaku perwakilan yang memiliki wewenang dalam teknologi informasi. Pada tabel 4.1 adalah perancangan proses dari pengumpulan data dan informasi.

Tabel 4. 1. Deskripsi perancangan proses pengumpulan data dan informasi

Nama Proses	Pengumpulan Data dan Informassi
Teknik	**Wawancara** Proses memperoleh keterangan untuk tujuan penelitian dengan cara tanya jawab sambil bertatap muka antara si penanya atau pewawancara dengan si penjawab atau responden dengan menggunakan alat yang dinamakan interview protocol. Wawancara dilakukan secara sistematis, telah terencana, dan mengacu pada tujuan penelitian yang dilakukan
Objek	Keamanan Aset Informasi pada CV Cempaka Tulungagung
Kebutuhan proses	*Interview protocol*
Strategi pelaksanaan	untuk memperoleh pangetahuan yang mendalam dengan mendengar sekelompok orang dari pasar sasaran yang tepat untuk membicarakan isu yang diamati dengan peneliti melalui wawancara, maka perlu dirumuskan strategi pelaksanaan agar pada saat wawancara berlangsung tidak ditemui hambatan. Strategi wawancara tresebut adalah sebagai berikut : • Menetapkan tujuan wawancara • Membuat Interview Protocol • Menentukan narasumber

1. Tujuan Wawancara

Tujuan wawancara pada tabel 4.2 ditetapkan untuk mendapatkan informasi yang tepat dari narasumber yang terpercaya dan menjadi acuan dalam perumusan pertanyaan wawancara.

Tabel 4.2 Tujuan Wawancara

Wawancara Ke-	Narasumber	Tujuan Wawancara
1	Kabag Produksi	Penggalian informasi mengenai proses bisnis inti dalam CV.Cempaka dan fungsi fungsi yang ada didalamnya
2	Kabag Personalia dan Umum	Penggalian informasi mengenai implementasi teknologi infomasi dalam CV.Cempaka termasuk didalamnya gambaran umum penggunaan teknologi informasi, fungsionalnya, pengelolaan aset sistem informasi, teknis mengenai penggunaan hardware, software, database dan jaringan, kelemahan teknologi informasi, risiko keamanan yang pernah terjadi dan sering terjadi.

2. Pembuatan *Interview Protocol*

Pada tabel 4.3, instrumen wawancara disediakan dalam interview protocol yaitu kumpulan data instrumen yang termasuk di dalamnya adalah items wawancara, kategori respon, instruksi dan lainnya. Interview protocol ini merupakan tulisan yang ditulis oleh peneliti dan dibaca oleh interviewer kepada responden atau ditampilkan untuk wawancara melalui. Interviewer juga mencatat

dan merekam respon dari responden pada interview protocol tersebut.

Tabel 4.3 Detail Ringkas Pertanyaan dalam Interview Protocol

No	Tujuan pertanyaan	Detail ringkas pertanyaan
1	Penggalian informasi mengenai proses bisnis dalam CV.Cempaka dan fungsi fungsi yang ada didalamnya, gambaran umum penggunaan teknologi informasi, kebutuhan keamanan data, pengelolaan aset sistem informasi, risiko keamanan yang pernah terjadi dan sering terjadi.	• Proses bisnis inti dalam proses bisnis CV.Cempaka • Penggunaan IT dalam operasional bisnis • Data struktur organisasi dan peran fungsi yang terlibat dalam proses bisnis • Praktek pengamanan yang telah dilakukan • Identifikasi risiko keamanan aset informasi • Seberapa sering risiko terjadi beserta penyebab dan dampaknya

3. Menentukan Narasumber

Penentuan narasumber dilakukan untuk memudahkan proses pengumpulan data. Dalam penetapan pihak narasumber, yang harus diperahtikan adalah kapasitas objek dalam kewenangannya memberi informasi yang valid, dan apakah pertanyaan yang dirumuskan relevan dengan pengetahuan pihak narasumber. Pada tabel 4.4 berikut adalah profil narasumber dalam penelitian.

Tabel 4.4 Narasumber Penelitian

Nama	Jabatan
Pak Dadang	Kepala bagian produksi
Bu Ida Wahyu Juniarti	Kepala divisi personalia

4.3 Analisa data

Dalam melakukan analisa data akan dilakukan analisa dan penilaian risiko, penelitian menggunakan pendekatan *risk assessment* kerangka kerja ISO27002:2013 dengan metode OCTAVE *(Operationally Critical Threat, Asset, and Vulnerability)* dan FMEA (*Failure Modes and Effecs Analysis*). Dimana dalam pendekatan *risk assessment* tersebut terdapat beberapa proses dalam melakukan penilaian risiko yaitu menetapkan dan mengelola kriteria, mengidentifikasi risiko, menganalisa risiko dan mengevaluasi risiko.

4.3.1 Identifikasi risiko

Dalam Identifikasi risiko akan berdasarkan dengan metode pada *framework* Octave yaitu dengan mengidentifikasi terlebih dahulu aset penting yang dimiliki organisasi, kebutuhan keamanan organisasi, praktek keamanan terkini yang telah atau sedang dilakukan, aset kritis dan kelemahan infrastruktur TI yang ada saat ini. Hasil dari identifikasi risiko kemudian akan dilanjutkan pada proses identifikasi pemilik risiko. Hasil luaran dari proses mengidentifikasi risiko adalah sebuah daftar risiko. Daftar risiko tersebut selanjutnya akan menjadi masukan untuk proses analisis risiko.

4.3.2 Penilaian risiko

Dalam penilaian risiko, metode yang digunakan dalam penelitian adalah metode FMEA. Dalam metode FMEA terdapat keiteria dalan melakukan penilaian risiko yaitu berdasarkan pada nilai dampak (*severity*), nilai kemungkinan (*occurence*) dan nilai deteksi (*detection*). Berikut adalah kriteria perhitungan untuk masing masing nilai.

a. Penentuan Nilai Dampak (*Severity* = S)

Pengukuran nilai dampak akan dilihat dari seberapa besar intensitas suatu kejadian atau gangguan dapat mempengaruhi aspek aspek penting dalam organisasi. Berikut merupakan penjelasan dari masing masing nilai dampak pada tabel 4.5 merupakan kriteria nilai dampak (severity).

Tabel 4.5 Kriteria Nilai Dampak

Dampak	Dampak dari Efek	Rank
Akibat Berbahaya	Gangguan dapat menghentikan proses bisnis	10
Akibat Serius	Gangguan menyebabkan kerugian secara finansial dan proses bisnis sangat terganggu serta penurunan kinerja	9
Akibat Ekstrim	Gangguan menyebabkan kerugian secara finansial dan sangat menghambat proses bisnis serta penurunan kinerja	8
Akibat Major	Gangguan menyebabkan kerugian secara finansial dan menghambat proses bisnis	7
Akibat Signifikan	Gangguan menyebabkan penurunan kinerja sehingga proses bisnis terhambat	6
Akibat Moderat	Ganguan menyebabkan kerugian finansial	5
Akibat Minor	Ganguan menyebabkan sedikit kerugian	4
Akibat Ringan	Gangguan menyebabkan gangguan kecil pada proses bisnis yang dapat diatasi tanpa kehilangan sesuatu	3
Akibat Sangat Ringan	Tanpa disadari dan memberikan dampak kecil pada proses bisnis	2
Tidak Ada Akibat	Tanpa disadari dan tidak mempengaruhi proses bisnis sama sekali	1

b. Penentuan Nilai Kemungkinan (*Occurrence* = O)

Nilai kemungkinan merupakan pengukuran terhadap tingkat frekuensi atau keseringan terjadinya masalah atau gangguan yang dapat menghasilkan kegagalan. Pada tabel 4.6 berikut merupakan penjelasan dari nilai kemungkinan.

Tabel 4.6 Kriteria Nilai Kemungkinan

Kemungkinan Kegagalan	Probablitas	Ranking
Very High: Kegagalan hampir/tidak dapat dihindari	Lebih dari satu kali tiap harinya	10
Very High: Kegagalan selalu terjadi	Satu kali setiap 3-4 hari	9
High: Kegagalan terjadi berulang kali	Satu kali dalam seminggu	8
High: Kegagalan sering terjadi	Satu kali dalam sebulan	7
Moderatly High : Kegagalan terjadi saat waktu tertentu	Satu kali setiap 3 bulan	6
Moderate : Kegagalan terjadi sesekali waktu	Satu kali setiap 6 bulan	5
Moderate Low : Kegagalan jarang terjadi	Satu kali dalam setahun	4
Low: Kegagalan terjadi relative kecil	Satu kali dalam 1-3 tahun	3
Very Low: Kegagalan terjadi relative kecil dan sangat jarang	Satu kali dalam 3 - 6 tahun	2
Remote: Kegagalan tidak pernah terjadi	Satu kali dalam 6 - 50 tahun	1

c. Penentuan Nilai Deteksi (*Detection* = D)

Pengkuruan nilai deteksi merupakan penilaian terhadap kemampuan organisasi dalam melakukan kontrol dan kendali terhadap terjadinya suatu gangguan atau kegagalan yang akan terjadi. Pada tabel 4.7 berikut adalah penjelasan nilai deteksi dan metode deteksi terhadap risiko.

Tabel 4.7 Kriteria Nilai Deteksi

Deteksi	Kriteria Deteksi	Ranking
Hampir tidak mungkin	Tidak ada metode deteksi	10
Sangat Kecil	Metode deteksi yang ada tidak mampu memberikan cukup waktu untuk melaksanakan rencana kontingensi	9
Kecil	Metode deteksi tidak terbukti untuk mendeteksi tepat waktu	8
Sangat Rendah	Metode deteksi tidak andal dalam mendeteksi tepat waktu	7
Rendah	Metode deteksi memiliki tingkat efektifitas yang rendah	6
Sedang	Metode deteksi memiliki tingkat efektifitas yang rata-rata	5
Cukup Tinggi	Metode deteksi memiliki kemungkinan cukup tinggi untuk dapat mendeteksi kegagalan	4
Tinggi	Metode deteksi memiliki kemungkinan tinggi untuk dapat mendeteksi kegagalan	3
Sangat Tinggi	Metode deteksi sangat efektif untuk dapat mendeteksi dengan waktu yang cukup untuk melaksanakan rencana kontingensi	2
Hampir Pasti	Metode deteksi hampir pasti dapat mendeteksi dengan waktu yang cukup	1

Setelah melakukan penetuan nilai dampak (*severity*), nilai kemungkinan (*occurence*) dan nilai deteksi (*detection*) selanjutnya adalah melakukan kalkulasi nilai prioritasi risiko (Risk Priority Number) yang didapatkan dari formulasi berikut :

RPN = S x O x D

RPN : *Risk Priority Number*, perhitungan nilai risiko
S : *Severity*, nilai dampak
O : *Occurrence*, niai kemungkinan
D: *Detection*, nilai deteksi

4.3.3 Kriteria dalam Penerimaan Risiko

Penentuan kriteria penerimaan risiko didasarkan pada hasil penilaian risiko, dimana setelah ditentukan nilai RPN dari masing masing risiko, selanjutnya ditentukan level risiko berdasarkan skala RPN. Risiko dengan tingkat *very high* dan *high* kemudian akan dialakukan analisis lebih lanjut untuk menentukan perlakuan risiko. Pada tabel 4.8 berikut ini adalah skala penentuan nilai RPN berdasarkan pada metode FMEA.

Tabel 4.8 Penerimaan Risiko (sumber: FMEA)

Level Risiko	Skala Nilai RPN
Very High	> 200
High	< 200
Medium	< 120
Low	< 80
Very Low	< 20

4.4 Pengendalian Risiko

Hasil dari analisis dan penilaian risiko serta penerimaan risiko kemudian akan menjadi masukan dalam tahap pengendalian risiko. Dalam tahap ini dilakukan terlebih dahulu penentuan tujuan kontrol berdasarkan kerangka kerja ISO27002:2013, kemudian dilakukan penyesuaian kontrol dengan perusahaan setelah itu dilakukan perumusan rekomendasi pengendalian risiko.

4.4.1 Pemetaan Risiko dan Kontrol ISO27002:2013

Pemetaan ini dilakukan dengan tujuan untuk menentukan tujuan kontrol ISO27002:2013 yang dibutuhkan dalam melakukan mitigasi terhadap risiko. Pada tabel 4.10 berikut adalah tabel pemetaan risiko dengan kategori keamanan data dan kontrol ISO27002:2013.

Tabel 4.9 Contoh pemetaan risiko dengan kontrol ISO 27002

Kategori	Aset Informasi Kritis	Potensi Kegagalan	Potensi Penyebab	Kontrol ISO 27002	Justifikasi

Dan setelah pemetaan kontrol dengan kerangka kerja ISO27002:2013 kemudian dibuat daftar rekomendasi mitigasi risiko. Hasil rekomendasi mitigasi risiko inilah yang akan menjadi bahan pertimbangan untuk usulan perancangan prosedur.

4.4.2 Rekomendasi Pengendalian Risiko

Setelah memetakan risiko dengan ISO27002:2013 selanjutnya adalah melakukan penyesuaian aktivitas dalam kontrol dengan kondisi pada perusahaan untuk mendapatkan rekomendasi pengendalian risiko. Hasil dari rekomendasi pengendalian risiko ini adalah mengidentifikasi sebuah prosedur yang diperlukan untuk memastikan risiko tidak berulang.

4.5 Perancangan SOP

Dalam penyusunan dokumen SOP tidak terdapat suatu format baku yang dapat dijadikan acuan, hal ini dikarenakan SOP merupakan dokumen internal yang kebiijakan pembuatannya disesuaikan oleh masing masing organisasi, begitu pula dengan penyunan format dari dokumen SOP tersebut. Format langkah-langkah dalam SOP akan dibuat dalam bentuk *flowchart* untuk memudahkan penggambaran aktivitas. Berikut merupakan penjelasan dari format SOP yang akan dikembangkan dan juga *flowchart* penggambaran aktivitas prosedur.

Format SOP akan dikembangkan sesuai dengan struktur standard dengan acuan dari peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia mengenai pedoman penyusunan standar operasional prosedur nomor 35 tahun 2012. Berdasarkan panduan tersebut, pada tabel 4.11 berikut merupakan penjelasan struktur dan konten yang akan dimasukkan dalam dokumen SOP penelitian.

Tabel 4.10 Format Konten SOP

Struktur Bab	Sub-Bab	Deskripsi
Pendahuluan	Tujuan	Berisi tujuan dari dibuatnya dokumen SOP
	Ruang Lingkup	Merupakan ruang lingkup dari prosedur-prosedur yang akan dimuat dalam dokumen
	Overview Keamanan Aset Informasi	Berisi penjelasan singkat mengenai keamanan aset informasi
	Evaluasi Penilaian Risiko	Berisikan penjelasan dan hasil dari penilaian risiko

Struktur Bab	Sub-Bab	Deskripsi
Prosedur	Deskripsi Umum	Merupakan pendefinisian tujuan, ruang lingkup, referensi kontrol dan pendefinisian istilah lain yang terkait dalam prosedur
	Rincian Prosedur	Berisi penjabaran aktivitas-aktivitas yang perlu dilakukan dan ditampilkan dalam bentuk *flowchart*
	Bagan Alur SOP	Semua formulir yang diperlukan untuk menjalankan prosedur akan dijelaskan cara penggunaannya

4.6 Perancangan proses Verifikasi dan Validasi

Pengujian SOP dilakukan melalui dua cara yakni verifikasi dan validasi. Verifikasi dilakukan dengan cara wawancara untuk memastikan kebenaran informasi yang terkandung dalam SOP, sedangkan validasi dilakukan dengan simulasi untuk mengetahui ketepatan SOP ketika implementasi dalam kasus nyata. Pada tabel 4.12 merupakan penjelasan metode pengujian SOP yang akan dilakukan.

Tabel 4.11 Metode Pengujian SOP

	Tujuan	Metode	Sasaran
Verifikasi	Untuk melakukan verifikasi terhadap dokumen untuk memastikan kebenaran dari informasi-informasi yang didefinisikan dan termuat di dalam dokumen SOP	Wawancara	Pihak yang memiliki kedudukan paling tinggi pada bagian Personalia dan umum yaitu Kepala bagian personalia dan umum CV Cempaka
Validasi	Untuk melakukan validasi dokumen dengan melihat apakah SOP dapat berjalan sesuai dengan kondisi yang ada dan untuk menemukan kekurangan dari SOP yang telah dibuat sehingga dapat dilakukan koreksi dan selanjutnya dapat diterapkan	Simulasi Pengujian dokumen SOP	Pelaksana SOP, yakni : Fungsional bisnis perusahaan yang terlibat

4.6.1 Verifikasi

Verifikasi dilakukan dengan tujuan memastikan kebenaran dari informasi yang termuat dalam dokumen SOP dan kesesuaiannya dengan kondisi CV.Cempaka . Metode yang digunakan dalam melakukan verifikasi adalah melakukan wawancara dengan bagian CV.Cempaka sebagai pihak yang memiliki kewenangan dalam keamanan teknologi informasi. Berikut adalah tahapan yang dilakukan dalam melakukan verifikasi pengujian SOP.

1. Penulis menyerahkan dokumen SOP kepada bagian personalia umum dan menjelaskan isi dokumen dengan detil.
2. Bagian personalia umum melakukan review dokumen SOP.
3. Penulis mengadakan wawancara secara langsung setelah Bagian personalia umum selesai mereview dokumen. Pertanyaan yang dilontarkan terkait struktur SOP, konten SOP, serta istilah yang digunakan dalam SOP.
4. Bagian personalia umum akan memberikan review dan revisi dokumen jika ada yg kurang dengan dokumenya
5. Penulis melakukan pembenahan dokumen SOP sesuai saran dari Bagian personalia umum.
6. Penulis menyerahkan ulang hasil revisi pada bagian personalia umum.
7. Bagian personalia umum menyetujui dokumen SOP yang telah diperbaiki.

4.6.2 Validasi

Validasi dilakukan untuk memastikan dokumen SOP dapat berjalan sesuai dengan kondisi yang ada pada CV.Cempaka dan untuk menemukan ketidaksesuaian dan kekurangan SOP sehingga dapat dibenahi sesuai kondisi yang ada. Metode yang digunakan adalah dengan pengujian SOP dengan pelaksana SOP yaitu pihak manajemen CV. Cempaka. Berikut merupakan tahapan yang dilakukan dalam melakukan validasi pengujian SOP.

1. Penulis menyerahkan dokumen SOP yang telah diperbaiki pada tahap verifikasi.

2. Penulis memberikan arahan penggunaan dokumen SOP dan menjelaskan beberapa skenario yang akan diuji.
3. Pelaksana SOP mensimulasikan SOP dengan menggunakan case yang asli yang masuk pada catatan *service desk* CV cempaka
4. Setelah simulasi selesai, penulis meminta *feedback* dan *review* dari pelaksana.
5. Penulis melakukan perbaikan dokumen jika terdapat ketidaksesuaian pada proses simulasi
6. Setelah selesai, dokumen SOP dapat dinyatakan valid dan dapat diterapkan.

BAB V
IMPLEMENTASI

Bab ini menjelaskan tentang implementasi setiap tahapan dan proses-proses di dalam metodologi tugas akhir yang dapat berupa hasil, waktu pelaksanaan dan lampiran terkait yang memuat pencatatan tertentu dengan implementasi proses.

5.1 Proses Pengumpulan Data

Pengumpulan data yang dilakukan dalam penelitian bertujuan untuk mengidentifikasi dan menganalisa risiko yang berkaitan dengan keamanan asset informasi pada CV Cempaka. Dalam melakukan pengumpulan data, dilakukan wawancara menggunakan *interview protocol* dan oservasi dokumen dengan bagian personalia umum CV Cempaka. Hasil dari wawancara dapat dilihat pada Lampiran A.

5.1.1 Identifikasi Aset teknologi informasi

Penentuan aset TI ini dilakukan dengan observasi dokumen aset perusahaan dimana aset yang diidentifikasi merupakan aset yang digunakan dalam mendukung proses bisnis dan berada pada kantor CV Cempaka Tulungagung. Dari hasil observasi maka disimpulkan dalam tabel 5.1 berikut ini.

Tabel 5.1 Identifikasi aset

Kategori aset	Daftar aset
Hardware	Server
	PC
	Laptop
	Camera CCTV
	Printer
	IP Telepon

Kategori aset	Daftar aset
	Mesin Fotocopy
	LCD Proyektor
	Scanner
Jaringan	Wifi
	Router
	Switch
	Kabel
Software	Sistem Informasi Keuangan (SISKA)
	Sistem Informasi Administrasi (SIADMIN)
	Sistem Informasi Pendataan dan penjadwalan (SIMDATA)
	Sistem Informasi Pemasaran (SIMPEM)
Data	Data keuangan
	Data produksi
	Data Kepegawaian
	Data Aset
	Data Pemasaran

Dari hasil observasi akan di analisa kembali dalam mengidentifikasi aset informasi kritis yang akan digunakan dalam proses penelitian selanjutnya.

5.1.2 Identifikasi Aset Informasi kritis

Penentuan aset kritis dilakukan melalui pengumpulan informasi berdasarkan sudut pandang pihak CV Cempaka yaitu Kasie Personalia umum dan dilakukan analisa dari hasil wawancara dan observasi aset yang digunakan dimana aset kritis ini merupakan aset yang sangat berpengaruh dalam keberlangsungan proses bisnis CV Cempaka jika terjadi gangguan ataupun ancaman pada aset tersebut perusahaan akan mengalami hambatan dalam operasional, bahkan sebuah kerugian. Dari hasil wawancara yang terlampir pada Lampiran A maka dapat disimpulkan bahwa dalam masing masing kategori Aset TI terdapat aset kritis yang dijelaskan dalam tabel 5.2 berikut ini.

Tabel 5.2 Daftar Aset kritis

Aset TI	Daftar Aset Kritis	Alasan/Sebab
Hardware	Server	Hardware menjadi pendukung dalam proses bisnis perusahaan. Server menjadi aset kritis untuk memastikan data dan sistem selalu dapat diakses selain itu komputer juga digunakan untuk proses operasional dan juga sebagai media untuk mengakses data
	PC	
Software	Sistem Informasi Keuangan (SISKA)	SISKA yang berhubungan dengan kegiatan akuntansi dan juga penghitungan keuangan, SIADMIN sistem informasi ini berhubungan dengan bagian personalia, atau HR, SIMDATA digunakan pada bagian
	Sistem Informasi Administrasi (SIADMIN)	
	Sistem Informasi Pendataan dan	

Aset TI	Daftar Aset Kritis	Alasan/Sebab
	penjadwalan (SIMDATA)	produksi untuk mendata persediaan tembakau, kertas, cengkeh dan lainya, selain itu untuk mencatat penjadwalan produksi perusahaan, SIMPEM digunakan untuk melakukan pencatatan penerimaan pesanan dari pihak distributor dan juga untuk melakukan pencatatan penjualan dan pengiriman produk. Dan ke empat sistem ini saling berhubungan
	Sistem Informasi Pemasaran (SIMPEM)	
Data	Data keuangan	Seluruh data sangat penting bagi perusahaan karena terkait dengan keberlangsungan bisnis perusahaan sehingga keamanan dari setiap data sangat penting
	Data produksi	
	Data Kepegawaian	
	Data Aset	
	Data Pemasaran	
Jaringan	Wifi	Jaringan digunakan untuk mengakses informasi, seperti mengakses database dan mengakses internet.
	Kabel	
	Router	
	Switch	
Sumber Daya	Karyawan	Suatu aset yang penting dalam sebuah organisasi

Aset TI	Daftar Aset Kritis	Alasan/Sebab
Manusia	Satuan pengamanan	karena SDM yang memiliki kompetensi dapat mendukung proses bisnis berjalan dengan lancer.

5.1.3 Identifikasi Kebutuhan Kemanan Aset Kritis

Kebutuhan keamanan merupakan bentuk perlindungan terhadap ancaman yang mungkin terjadi dalam upaya untuk untuk memastikan keberlangsungan proses bisnis, meminimalisir risiko bisnis. Kebutuhan keamanan tiap-tiap aset juga memiliki lebih dari satu kebutuhan. Justifikasi kebutuhan keamanan aset kritis ini juga dilakukan dengan cara melakukan observasi secara langsung dan diskusi dengan pihak yang terkait. Aspek keamanan aset informasi tersebut akan menjadi kategori dalam mengidentifikasi kebutuhan keamanan aset kritis. Pada tabel 5.3 berikut adalah daftar kebutuhan keamanan aset kritis pada CV Cempaka.

Tabel 5.3 Daftar Kebutuhan Keamanan Aset Kritis

Aset Kritis	Kebutuhan Kemanan	Narasumber
Server	Dapat diakses 24 jam dalam 7 hari	Bagian personalia
	Konfigurasi server dilakukan dengan benar	Bagian personalia
	Adanya sumber listrik cadangan	Bagian personalia
	Adanya kontrol keamanan untuk ruang fisik server	Bagian personalia

Aset Kritis	Kebutuhan Kemanan	Narasumber
	Adanya pembatasan hak akses	Bagian personalia
	Server tidak boleh diakses oleh pihak yang tidak berwenang	Bagian personalia
PC	Dapat berfungsi selama jam kerja organisasi	Bagian personalia
	Adanya sumber listrik cadanagn	Bagian personalia
	Adanya Antivirus	Bagian personalia
	Adanya pembatasan hak akses	Bagian personalia
	Data yang terdapat didalam pc harus lengkap dan aman	Bagian personalia
Sistem Informasi Keuangan (SISKA)	Dapat berfungsi selama jam kerja organisasi	Bagian personalia
	Data yang dimasukan pada aplikasi harus lengkap	Bagian personalia
	Adanya pembatasan hak akses	Bagian personalia
Sistem Informasi Administrasi (SIADMIN)	Dapat berfungsi selama jam kerja organisasi	Bagian personalia
	Data yang dimasukan pada aplikasi harus lengkap	Bagian personalia

Aset Kritis	Kebutuhan Kemanan	Narasumber
	Adanya pembatasan hak akses	Bagian personalia
Sistem Informasi Pendataan dan penjadwalan (SIMDATA)	Dapat berfungsi selama jam kerja organisasi	Bagian personalia
	Data yang dimasukan pada aplikasi harus lengkap	Bagian personalia
	Adanya pembatasan hak akses	Bagian personalia
Sistem Informasi Pemasaran (SIMPEM)	Dapat berfungsi selama jam kerja organisasi dan sesuai	Bagian personalia
	Data yang dimasukan pada aplikasi harus lengkap dan sesuai	Bagian personalia
	Adanya pembatasan hak akses	Bagian personalia
Data keuangan	Adanya backup data secara rutin	Bagian personalia
	Adanya pembatasan hak akses	Bagian personalia
Data Produksi	Adanya backup data secara rutin	Bagian personalia
	Adanya pembatasan hak akses	Bagian personalia
Data Kepegawaian	Adanya backup data secara rutin	Bagian personalia
	Adanya pembatasan hak akses	Bagian personalia

Aset Kritis	Kebutuhan Kemanan	Narasumber
Data Aset	Adanya backup data secara rutin	Bagian personalia
	Adanya pembatasan hak akses	Bagian personalia
Data Pemasaran	Adanya backup data secara rutin	Bagian personalia
	Adanya pembatasan hak akses	Bagian personalia
Wifi	Tersedia selama jam operasional kerja organisasi	Bagian personalia
	Terdapat sumber listrik cadangan	Bagian personalia
	Adanya kontrol rutin	Bagian personalia
	Adanya anti netcut	Bagian personalia
Kabel	Tersedia selama jam operasional kerja organisasi	Bagian personalia
	Adanya kontrol rutin	Bagian personalia
	Kabel dilakukan pelabelan untuk mempermudah pengorganisasian	Bagian personalia
Router Dan Switch	Tersedia selama jam operasional kerja organisasi	Bagian personalia

Aset Kritis	Kebutuhan Kemanan	Narasumber
	Adanya kontrol rutin	Bagian personalia
	Memonitoring jaringan untuk memastikan keaslian data	Bagian personalia

5.1.4 Identifikasi Ancaman Aset Kritis

Ancaman aset kritis merupakan hal yang mungkin terjadi dan pernah terjadi pada aset dan mengakibatkan terganggunya proses bisnis. Identifikasi ancaman pada aset kritis dikategorikan kedalam ancaman dari lingkungan, ancaman dari manusia dan ancaman Hardware dan jaringan atau infrastruktur. Daftar Ancaman berikut ini didapatkan dari hasil wawancara kepada narasumber. Pada tabel 5.4 berikut adalah daftar ancaman aset kritis pada CV Cempaka.

Tabel 5.4 Daftar Ancaman Aset Kritis

Ancaman dari Lingkungan	
1.	Gempa Bumi
2.	Tsunami dan Badai
3.	Banjir
4.	Kebakaran
5.	Kerusakan Pada Bangunan
6.	Perubahan Regulasi
Ancaman dari Manusia	
7.	Kesalahan input data
8.	Data Corrupt/Rusak
9.	Pencurian Data
10.	Memberitahukan Password penting
11.	Sabotase Jaringan (hacking)
12.	Kelalaian Pegawai
13.	Penurunan Loyalitas Pegawai

Ancaman dari Infrastruktur	
Hardware	
14.	Kerusakan Komputer
15.	Kerusakan Server
16.	Kerusakan pada Genset dan UPS
17.	Kesalahan Konfigurasi Hardware
18.	Pencurian Komponen Hadware
Software	
19.	Bug pada Software
20.	Serangan virus
21.	Kesalahan Konfigurasi dan input data pada Sistem
22.	Pembobolan sistem
Jaringan	
23.	Gangguan pada Router
24.	Kerusakan Kabel
25.	Gangguan Koneksi Internet
26.	Hilangnya Komponen

5.1.5 Identifikasi Praktik Keamanan yang telah dilakukan Organisasi

Pada tabel 5.5 berikut ini merupakan daftar praktik keamanan yang telah dilakukan CV Cempaka dalam memastikan keamanan aset teknologi informasi yang mendukung berjalannya proses bisnis.

Tabel 5.5 Daftar Praktik Keamanan yang telah dilakukan Organisasi

Praktik Keamanan Organisasi	Pihak yang Bertanggung Jawab
Adanya antivirus dan diupdate secara berkala	Bagian personalia
Adanya update patch dan firewall secara berkala	Bagian personalia
Tidak dapat menginstal aplikasi lain dalam PC selain admin	Bagian personalia

Praktik Keamanan Organisasi	Pihak yang Bertanggung Jawab
Adanya Camera CCTV yang bekerja 24 jam	Bagian personalia
Dilakukan backup data Camera CCTV selama 1 bulan 2 kali	Bagian personalia
Telah dipasang pendingin pada ruang server untuk mengurangi terjadinya overheat	Bagian personalia
Adanya fire extinguisher untuk memadamkan api saat terjadi kebakaran	Bagian personalia
Adanya genset dan ups untuk mengatasi saat tidak mendapat aliran listrik	Bagian personalia
Dilakukan pengecekan kerusakan ruangan setiap 1 bulan sekali	Bagian personalia
Telah dilakukan dokumentasi data dalam bentuk laporan cetak pada setiap sistem yang dimiliki	Bagian personalia Bagian Keuangan Bagian Produksi Bagian Pemasaran
Telah dilakukan backup server 2 hari sekali	Bagian personalia
Ada penguncian/penggembokan pada ruang server sehingga tidak dapat sembarang orang bisa masuk	Bagian personalia
Data hanya bisa dimasukkan, diganti atau dihapus oleh database administrator saja	Bagian personalia
Dilakukan maintenance rutin setiap 6 bulan sekali setiap perangkat TI	Bagian personalia
Dilakukan maintenance Wifi setiap 2 minggu sekali	Bagian personalia
Membedakan role atau hak akses untuk masing masing pegawai sesuai dengan unit kerja dan fungsinya	Bagian personalia
Pengaturan kabel dengan melakukan	Bagian personalia

Praktik Keamanan Organisasi	Pihak yang Bertanggung Jawab
pelabelan untuk masing masing fungsi kabel	
Adanya log setiap aktivitas dalam sistem informasi yang dimiliki	Bagian personalia
Adanya pergantian password secara berkala	Bagian personalia Bagian Keuangan Bagian Produksi Bagian Pemasaran
Adanya anggota satuan keamanan yang berkeliling selama 24 jam penuh	Bagian personalia

5.1.6 Identifikasi Kerentanan pada Teknologi

Pada tabel 5.6 berikut merupakan daftar kerentanan pada teknologi yang dibagi kedalam masing masing aset kritis.

Tabel 5.6 Daftar Kerentanan pada Teknologi

Server	
System of Interest	2 Server pada kantor CV Cempaka
Komponen Utama	**Kemungkinan Ancaman**
• Sistem Operasi • Processor • RAM • Harddisk • Listrik • Keamanan Jaringan • Genset • UPS • Kabel	• Tidak mendapatkan aliran listrik karena terjadi pmadaman listrik • Genset tidak dapat berfungsi karena mengalami kerusakan • RAM mengalami kelebihan memori • Kinerja Procesor menurun akibat terlalu banyak kapasitas data • Tempat penyimpanan (Harddisk) penuh • Keamanan jaringan dapat ditembus • UPS tidak berfungsi • Ruang Server kurang diberi pengamanan • Komponen dicuri karena kelalaian pihak

• Pendingin ruangan • Ruang Server	keamanan
PC	
System of Interest	PC yang ada pada kantor CV Cempaka
Komponen Utama	**Kemungkinan Ancaman**
• CPU • Monitor, Keyboard dan Mouse • Kabel LAN • Antivirus • Sistem Operasi • Software • Listrik • UPS • Genset • Firewall	• Monitor, Keyboard ataupun mouse mengalami kerusakan • Firewall ditembus oleh bagian yang tidak berwenang • Kabel LAN putus akibat hewan pengerat • Tidak mendapatkan aliran listrik karena terjadi pemadaman pada PLN • UPS tidak berfungsi • Virus yang menyerang tidak dapat tertangani oleh antivirus • Komponen di curi karena kelalaian pihak keamanan
Data	
System of Interest	Seluruh data yang dimiliki perusahaan
Komponen Utama	**Kemungkinan Ancaman**
• Database • Server • Listrik • PC • Firewall • Database Administrator (DBA)	• Tidak dapat mendapatkan aliran listrik karena terjadi pemadaman pada PLN • Firewall ditembus oleh bagian yang tidak berwenang • PC berhenti beroperasi karena terserang virus • Database Admnistrator salah dalah melakukan pengolahan data (ubah dan hapus) • Data dicuri karena Database Administrator kurang melakukan kontrol keamanan

Perangkat Lunak	
System of Interest	Sistem informasi keuangan, sistem informasi administrasi, sistem pendataan dan penjadwalan, Sistem pemasaran
Komponen Utama	**Kemungkinan Ancaman**
• Firewall • Server • Antivirus	• Firewall ditembus oleh bagian yang tidak berwenang • Virus yang menyerang tidak dapat tertangani oleh antivirus • Server mengalami kerusakan sehingga sistem tidak dapat diakses
Wifi	
System of Interest	2 wifi yang terpasang pada bagian personalia, 2 wifi pada bagian produksi, 2 wifi pada bagian pemasaran dan keuangan semua berada dalam 1 kantor
Komponen Utama	**Kemungkinan Ancaman**
• Listrik • Kabel • Keamanan Jaringan	• Tidak mendapatkan aliran listrik karena terjadi pemadaman • Kabel rusak akibat gigitan hewan • Keamanan jaringan dapat ditembus oleh pihak yang tidak berwenang
Router	
System of Interest	4 Router pada kantor CV Cempaka
Komponen Utama	**Kemungkinan Ancaman**
• Listrik • Kabel • Keamanan Jaringan	• Tidak mendapatkan aliran listrik karena terjadi pemadaman • Kabel rusak akibat digigit hewan pengerat • Komponen dicuri karena kelalaian pihak keamanan

5.1.7 Hubungan antara Aset Kritis, Kebutuhan Kemanan, Ancaman dan Praktik Keamanan Organisasi

Berdasarkan hasil analisis terkait aset kritis. Maka perlu dilakukan pemetaan hubungan antara masing masing aset dengan identifikasi kebutuhan keamanan dan ancaman serta praktik keamanan yang telah dilakukan. Pemetaan hubungan tersebut berfugsi untuk menganalisis lebih dalam kondisi kekinian dari praktik keamanan yang telah dilakukan oleh CV Cempaka untuk mengatasi adanya ancaman untuk setiap aset kritis. Pada tabel 5.7 berikut adalah hubungan antara aset kritis dan masing masing kebutuhan keamanan, ancaman serta praktik keamanan yang telah diimplementasikan.

Tabel 5.7 Hubungan aset kritis, kebutuhan keamanan, ancaman dan praktik keamanan organsiasi

Kategori Aset	Aset Kritis	Kebutuhan Keamanan	Ancaman	Praktik Keamanan Organisasi
Hardware	Server	Dapat diakses 24 jam dalam 7 hari	• Kerusakan Komputer • Kerusakan Server • Kerusakan Genset dan UPS • Kesalahan konfigurasi	• Dilakukan maintenance rutin setiap 6 bulan sekali untuk perangkat TI • Telah dilakukan backup server 2 hari sekali • Adanya Camera CCTV yang bekerja 24 jam
		Konfigurasi server dilakukan dengan benar		
		Adanya sumber listrik cadangan		
		Adanya kontrol keamanan untuk ruang fisik server		

Kategori Aset	Aset Kritis	Kebutuhan Keamanan	Ancaman	Praktik Keamanan Organisasi
		Adanya pembatasan hak akses	• Pencurian Komponen Hadware	• Telah dipasang pendingin pada ruangan untuk mengurangi terjadinya overheat • Telah ada fire extinguisher untuk memadamkan api saat terjadi kebakaran • Ada penguncian pada ruang server sehingga tidak sembarang orang bisa masuk • Dilakukan backup data Camera CCTV selama sebulan 2 kali • Adanya anggota satuan keamanan yang berkeliling selama 24 jam penuh
		Server tidak boleh diakses oleh usb atau pihak yang tidak berwenang		
	PC	Dapat berfungsi selama jam kerja organisasi		
		Adanya sumber listrik cadanagn		
		Adanya Antivirus		
		Adanya pembatasan hak akses		
		Data-data yang terdapat didalam pc harus lengkap dan aman		

Kategori Aset	Aset Kritis	Kebutuhan Keamanan	Ancaman	Praktik Keamanan Organisasi
Software	Sistem Informasi Keuangan (SISKA) Sistem Informasi Administrasi (SIADMIN)	• Dapat berfungsi selama jam kerja organisasi • Data yang dimasukan pada aplikasi harus lengkap dan sesuai • Adanya pembatasan hak akses	• Bug pada software • Serangan virus • Kesalahan konfigurasi dan input data pada sistem • Pembobolan sistem	• Adanya antivirus dan di update secara berkala • Tidak dapat menginstal aplikasi lain dalam PC selain admin • Membedakan role dan hak akses untuk masing masing pegawai sesuai dengan unit kerja • Adanya log setiap

Kategori Aset	Aset Kritis	Kebutuhan Keamanan	Ancaman	Praktik Keamanan Organisasi
	Sistem Informasi Pendataan dan penjadwalan (SIMDATA)			aktivitas dalam sistem informasi yang dimiliki
	Sistem Informasi Pemasaran (SIMPEM)			
Data	Data keuangan	• Adanya backup data secara rutin • Adanya pembatasan hak akses	• Kesalahan input data • Data corrupt/rusak • Pencurian data • Sharing password	• Telah dilakukan back up server 2 hari sekali • Telah dilakukan dokumentasi data dalam bentuk cetak pada setiap sistem
	Data Produksi			
	Data Kepegawaian			
	Data Aset			

Kategori Aset	Aset Kritis	Kebutuhan Keamanan	Ancaman	Praktik Keamanan Organisasi
	Data Pemasaran			yang dimiliki • Data hanya dapat dimasukkan, diganti dan dihapus oleh database administrator saja • Adanya perbedaan role atau hak akses pada data untuk masing masing fungsi
Jaringan	Wifi	Tersedia selama jam operasional kerja organisasi	• Gangguan pada router • Kerusakan kabel • Gangguan koneksi internet • Sabotase jaringan internet	• Telah dipasang anti netcut untuk keamanan wifi • Dilakukan maintenance rutin setiap 6 bulan sekali untuk setiap perangkat TI
		Adanya sumber listrik cadangan		
		Adanya kontrol rutin		
		Adanya anti netcut		
	Kabel	Tersedia selama jam operasional kerja		

Kategori Aset	Aset Kritis	Kebutuhan Keamanan	Ancaman	Praktik Keamanan Organisasi
		organisasi		• Dilakukan maintenance WIFI setiap 2 minggu sekali • Pengaturan kabel dengan melakukan pelabelan untuk sesuai fungsi kabell
		Adanya kontrol rutin		
		Kabel dilakukan pelabelan untuk mempermudah pengorganisasian		
	Router	Tersedia selama jam operasional kerja organisasi		
		Adanya kontrol rutin		
		Memonitoring jaringan untuk memastikan keaslian data		

Berdasarkan dari hasil identifikasi aset kritis, kebutuhan keamanan, ancaman dari masing masing aset dan praktik keamanan yang telah dilakukan oleh organisasi, maka selanjutnya adalah menganalisa risiko yang mungkin timbul dari masing masing aset. Risiko tersebut dianalisis untuk setiap aset TI yaitu perangkat keras (*hardware),* perangkat lunak *(software)*, data, jaringan dan sumber daya manusia.

5.2 Analisis Data

Analisa data yang bertujuan untuk mendeskripsikan data sehingga bisa di pahami, lalu untuk membuat kesimpulan atau menarik kesimpulan mengenai karakteristik populasi berdasarkan data yang didapatkan dari sampel ini didasarkan pada hasil identifikasi kebutuhan keamanan, ancaman dan juga praktik keamanan dari masing masing aset informasi yang telah diidentifikasikan sebelumnya. Analisis risiko dilakukan berdasarkan pada metode FMEA. Dalam melakukan analisis risiko, terlebih dahulu dilakukan identifikasi potensi penyebab kegagalan dan potensi dampak kegagalan untuk setiap risiko. Setalah daftar risiko beserta penyebab dan dampak diidentifikasi, selanjutnya adalah melakukan penilaian risiko berdaarkan kriteria penilaian risiko pada metode FMEA. Penilaian risiko yang dilakukan secara meyeluruh dan didasarkan pada seluruh komponen sistem informasi yaitu *hardware, software*, jaringan, data dan sumber daya manusia. Sehingga dalam tahap analisis risiko akan dihasilkan luaran sebuah *risk register* dan hasil penilaian risiko.

5.2.1. Risk Register

Pada tabel 5.8 berikut merupakan *risk register* untuk risiko keamanan aset informasi yang terkait pada hilangnya kerahasiaan, integritas dan keutuhan data. Dan untuk keseluruhan daftar risiko dapat dilihat pada lampiran B.

Tabel 5.8 Risk Register Keamanan aset informasi

Kategori Aset	Aset Informasi Kritis	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
Data	• Data keuangan, • Data	Manipulasi data	Username dan password diketahui oleh pengguna lain	• Kerugian secara finansial maupun non-finansial • Hilangnya	Bagian personalia
			Adanya Hacker yang memanipulasi data		

Kategori Aset	Aset Informasi Kritis	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
	Produksi, • Data Kepegawaian , • Data Aset • Data Pemasaran		Penurunan loyalitas karyawan sehingga data dimanipulasi	kepercayaan antar *stakeholder* • Terhambatnya proses bisnis	
		Pencurian data	Kelalaian Karyawan	• Kebocoran data penting dan rahasia sehingga berdampak kerugian secara non-finansial • Penuruan reputasi perusahaan	Bagian personalia
			Adanya hacker yang mampu membobol sistem keamanan server		

Kategori Aset	Aset Informasi Kritis	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
		Data Hilang	Server rusak	• Kerugian secara finansial maupun non-finansial • Terhambatnya proses bisnis	Bagian personalia
Hardware	Server	Kerusakan server	Kesalahan Konfigurasi	• Kerugian secara finansial • Terhambatnya proses bisnis	Bagian personalia
			Tegangan listrik tidak stabil		
			Server overheat		

Kategori Aset	Aset Informasi Kritis	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
		Sever tidak berfungsi (mati)	Adanya Pemadaman listrik Kerusakan pada Genset dan UPS	Terhambatnya proses bisnis	Bagian personalia
		Server hilang	Kelalaian satuan keamanan	• Kerugian secara finansial • Terhambatnya proses bisnis	Bagian personalia
	PC	Kerusakan PC	Kesalahan Konfigurasi	• Kerugian secara finansial • Terhambatnya proses bisnis	Bagian personalia
			Tegangan listrik tidak stabil		
			PC overheat		

Kategori Aset	Aset Informasi Kritis	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
			Kelalaian karyawan		
		PC Hilang	Kelalaian satuan keamanan	• Kerugian secara finansial • Terhambatnya proses bisnis	Satuan Keamanan
Software	• Sistem Informasi Keuangan (SISKA) • Sistem Informasi Administrasi	Sistem tidak dapat diakses	Pembobolan sistem	• Kebocoran data penting dan rahasia sehingga berdampak kerugian secara finansial maupun non-	Bagian personalia
			Username dan password diketahui oleh pengguna lain		

Kategori Aset	Aset Informasi Kritis	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
	(SIADMIN) • Sistem Informasi Pendataan dan penjadwalan (SIMDATA) • Sistem Informasi Pemasaran (SIMPEM)			finansial • Terhambatnya proses bisnis	
		Sistem tidak berjalan normal (error)	Serangan virus	• Kerugian secara finansial dan non finansial • Terhambatnya proses bisnis	Bagian personalia
			Kesalahan Konfigurasi pada Sistem		
			Bug pada Software		
Jaringan	Wifi	Gangguan koneksi	Kesalahan Konfigurasi wifi	penurunan kinerja sehingga proses bisnis terhambat	Bagian personalia

Kategori Aset	Aset Informasi Kritis	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Potensi Dampak Kegagalan	Pemilik Risiko
	Kabel	Kerusakan kabel	Kurangnya kontrol pengamanan kabel	penurunan kinerja sehingga proses bisnis terhambat	Bagian personalia
	Router	Router mengalami gangguan	Kesalahan Konfigurasi router	penurunan kinerja sehingga proses bisnis terhambat	Bagian personalia
Sumber Daya Manusia	Karyawan	Data yang ada tidak valid	Kesalahan input data	penurunan kinerja dan sedikit kerugian	Semua bagian pada perusahaan

5.2.2. Penilaian Risiko dengan Metode FMEA

Sesuai dengan kriteria penilaian risiko berdasarkan metode FMEA. Pada tabel 5.9 berikut ini merupakan hasil penilaian untuk risiko keamanan data dengan tingkat level *very high* hingga *Low*. Sedangkan untuk keseluruhan penilaian risiko dapat dilihat pada lampiran B.

Tabel 5.9 Hasil Penilaian Risiko

Level Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	RPN
Very High	Data Hilang	Kelalaian administrator	240
High	Kerusakan Server	Kesalahan konfigurasi server	140
	PC rusak	Kesalahan konfigurasi PC	140
	Sistem tidak dapat diakses	Username dan password diketahui oleh pengguna lain	140
	Manipulasi data	Username password diketahui orang lain	140
	Data Hilang	Server rusak	120
	Kerusakan kabel LAN	Kurangnya kontrol pengamanan kabel	144
	Password shared	Kelalaian pegawai	140
	Data tidak sesuai	Kesalahan input data	120

Level Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	RPN
Medium	Kerusakan Hardware	Banjir	105
		Kerusakan pada bangunan (bocor)	105
		Overheat	105
	Sistem tidak dapat diakses	Server Down	112
		Pembobolan sistem	84
	Manipulasi data	Adanya hacker	84
	Data tidak dapat diakses	Server Down	90
	Gangguan koneksi	Kesalahan Konfigurasi wifi	96
	Internet mati	Listrik mati	108
Low	PC rusak	Gempa bumi	63
	Pencurian data	Adanya hacker	72
	Sistem tidak berjalan normal (error)	Kesalahan Konfigurasi pada Sistem	70

Level Risiko	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	RPN
	Hilangnnya komponen TI	Kelalaian pegawai	72
	Penyalahgua an data organisasi	Penurunan Loyalitas Pegawai	54
	Pelanggaran hak akses	Penurunan Loyalitas Pegawai	54

5.2.3. Evaluasi Risiko

Dalam evaluasi risiko akan dibuat sebuah tabel daftar prioritas risiko yang didasarkan pada level risiko dan yang paling berpengaruh dalam proses bisnis perusahaan yang dapat dilihat pada tabel 5.10 Level risiko yang akan diprioritaskan merupakan yang berada pada level risiko *very high, high.*

Hasil dari evaluasi risiko berikut ini yang nantinya akan dilakukan analisis pengendalian risiko yang berupa sebuah pengimplementasian kontrol kebijakan, praktek dan prosedur. Berikut ini merupakan tabel daftar tingkat prioritas tertinggi dilihat dari nilai RPN yang tinggi.

Tabel 5.10 Daftar Prioritas Risiko

Aset Informasi Kritis	Level Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan
Server	High	Kerusakan Server	Kesalahan konfigurasi server
PC	High	PC rusak	Kesalahan konfigurasi PC
Data keuangan, Data Produksi, Data penjualan, Data Kepegawaian	Very High	Data Hilang	Kelalaian Administrator
	High	Data Hilang	Kerusakan Server
	High	Manipulasi data	Username password diketahui orang lain

Aset Informasi Kritis	Level Risiko	Potensi Mode Kegagalan	Poetensial Penyebab Kegagalan
Karyawan yang memiliki hak akses server maupun sistem	High	Sharing password	Kelalaian pegawai
	High	Data tidak sesuai (tidak valid)	Kesalahan input data
Seluruh sistem aplikasi yang dimiliki perusahaan	High	Aplikasi diakses oleh pihak yang tidak berwenang	Username dan password diketahui oleh pengguna lain
Kabel yang menghubungkan perangkat TI yang ada pada kantor	High	Kerusakan kabel LAN	Kurangnya kontrol pengamanan kabel

Berdasarkan hasil evaluasi penilaian risiko tersebut, maka dapat diketahui bahwa CV Cempaka memiliki beberapa kemungkinan risiko yang dapat timbul terkait keamanan asset informasi yaitu data hilang, manipulasi data, data tidak dapat diakses, kerusakan server dan lain lain yang mana risiko-risiko tersebut muncul dikarenakan oleh berbagai penyebab seperti yang telah dijelaskan diatas.

5.3 Pengendalian Risiko

Tahap pengendalian risiko merupakan tahap dalam menentukan tindakan pengendalian risiko yang tepat. Tahap ini dilakukan dengan melakukan pemetaan risiko terhadap kontrol yang dibutuhkan dalam kerangka kerja ISO27002:2013 serta melakukan penyesuaian dengan kondisi perusahaan sehingga dapat memberikan rekomendasi pengendalian risiko yang tepat.

Risiko dengan prioritas tertinggi dipetakan kedalam kontrol kerangka kerja ISO27002:2013. Tujuan dari pemetaan risiko kedalam kontrol kerangka kerja adalah untuk memastikan pengendalian risiko telah tepat dan sesuai dengan *control objective* dari setiap kontrol kerangka kerja. Selain pemetaan risiko dan kontrol pada kerangka kerja, dilakukan pula justifikasi kebutuhan kontrol. Justifikasi kebutuhan kontrol tersebut memiliki fungsi untuk memastikan bahwa kontrol yang ada sesuai dengan risiko yang akan dimitigasi.

Setelah melakukan pemetaan risiko terhadap kontrol ISO27002:2013, selanjutnya akan ditentukan rekomendasi pengendalian risiko berdasarkan kontrol yang telah ditentukan. Rekomendasi pengendalian risiko yang telah dipetakan sesuai dengan risiko dan kebutuhan kontrol, nantinya akan mendefinisikan usulan-usulan perbaikan dan juga sebagai input untuk membuat dokumen *Standard Operating Procedure* (SOP) Keamanan Aset Informasi pada CV Cempaka.

5.3.1. Pemetaan Risiko dengan Kontrol ISO27002:2013

Dalam pemetaan kontrol dengan kerangka kerja ISO27002:2013 terdapat 14 klausul yang digunakan yaitu ***:***

7.1.2. *Terms and conditions of employment,*
7.2.2. *Information security awareness, education & Training,*
9.1.1 *Access control policy,*
9.2.3 *Management of privileged access rights,*
9.3.1 *Use of secret authentication information,*
9.4.1 *Information access restriction,*
9.4.2 *Secure log-on procedures,*
9.4.3 *Password management system,*
11.2.3 *Cabling security,*
11.2.4 *Equipment maintenance,*
12.3.1 *Information Backup,*
12.4.1 *Event logging,*
12.4.2 *Protection of log information*

Pada tabel 5.11 berikut adalah pemetaan risiko dan kontrol ISO27002:2013, untuk justifikasi kebutuhan kontrol dapat dilihat pada Lampiran C.

Tabel 5.11 Pemetaan Risiko dan Kebutuhan Kontrol pada ISO27002:2013

Kategori Aset Informasi Kritis	Potensial Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013
Hardware	Kerusakan Server	Kesalahan konfigurasi server	*11.2.4 Equipment maintenance*
	Kerusakan PC	Kesalahan konfigurasi PC	*11.2.4 Equipment maintenance*

Kategori Aset Informasi Kritis	Potensial Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013
Data	Data Hilang	Kelalaian Administrator	*9.3.1 Use of secret authentication information*
			12.4.3 Administrator & Operator Logs
			7.2.2 Information security awareness, education and training
			9.1.1 Access control policy
	Data Hilang	Rusaknya media penyimpanan	*12.3.1 Information Backup*
			11.2.4 Equipment maintenance
	Manipulasi Data	Username password diketahui orang lain	*9.2.3 Management of privileged access rights*
			9.4.2 Secure log-on procedures
			9.4.3 Password management system

Kategori Aset Informasi Kritis	Potensial Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013
			9.1.1 Access control policy
Software	Aplikasi diakses oleh pihak yang tidak berwenang	Username dan password diketahui oleh pengguna lain	*9.4.1 Information access restriction*
			9.4.2 Secure log-on procedures
			9.4.3 Password management system
			9.1.1 Access control policy
			9.1.1 Access control policy
Jaringan	Kerusakan kabel LAN	Kurangnya kontrol pengamanan kabel	*11.2.3 Cabling security*
SDM	sharing password	Kelalaian karyawan yang memiliki hak akses	*7.1.2 Terms and conditions of employment*
			7.2.2 Information security awareness, education and training
			9.1.1 Access control policy
	Data tidak sesuai	Kesalahan input data	*12.4.1 Event logging*

Kategori Aset Informasi Kritis	Potensial Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013
	(tidak valid)		*12.4.2 Protection of log information*

5.3.2. Rekomendasi penyesuaian pengendalian risiko

Pada tahap penyesuaian dengan kondisi perusahaan ini akan dilakukan pemetaan petunjuk pelaksanaan yang di sarankan pada kerangka kerja ISO 27002:2013 dengan praktik keamanan yang sudah dilakukan oleh perusahaan Dengan adanya pemetaan ini, maka dapat diketahui ketidaksesuaian proses saat ini sehingga dapat dilakukan standarisasi untuk mengurangi kesenjangan dengan membuat hasil rekomendasi untuk menginisiasi pembuatan dokumen SOP. Pemetaan rekomendasi penyesuaian pengendalian risiko secara keseluruhan dapat dilihat pada Lampiran D

5.4 Prosedur dan Kebijakan Yang Dihasilkan Berdasarkan Hasil Rekomendasi Pengendalian Risiko

Dari hasil rekomendasi pengendalian risiko yang telah dijelaskan di sub bab sebelumnya, dapat disimpulkan bahwa untuk mengelola risiko keamanan aset informasi yang memiliki tingkat *High* dan *Very High* pada CV Cempaka diperlukan beberapa prosedur dan kebijakan. Prosedur dan kebijakan tersebut berfungsi untuk meningkatkan akuntabilitas pelaksanaan tugas dan menciptakan ukuran standar kinerja yang akan memberikan pegawai cara kerja yang konkrit untuk memperbaiki kinerja serta membantu mengevaluasi usaha yang telah dilakukan. Tabel 5.12 berikut merupakan prosedur yang dihasilkan berdasarkan pada hasil rekomendasi mitigasi risiko pada Lampiran D.

Tabel 5.12 Pemetaan Risiko dengan Kontrol ISO 27002 dan prosedur kebijakan yang dihasilkan

Potensi Mode Kegagalan	Potensial Penyebab Kegagalan	Kontrol ISO 27002 : 2013	Prosedur dan kebijakan yang Dihasilkan
Kerusakan Hardware	Kesalahan konfigurasi	***11.2.4 Equipment maintenance***	Prosedur Pemeliharaan Hardware
			Kebijakan Kemanan Hardware dan Jaringan
Data Hilang	Kelalaian Administrator	***9.2.3 Management of privileged access rights***	Prosedur Pengelolaan Hak akses
		9.3.1 Use of secret authentication information	Kebijakan *human resources security*
		12.4.3 Administrator & Operator Logs	Kebjakan Keamanan Informasi

Potensi Mode Kegagalan	Potensial Penyebab Kegagalan	Kontrol ISO 27002 : 2013	Prosedur dan kebijakan yang Dihasilkan
		9.1.1 Access control policy	Kebijakan Pengendalian Hak akses
	Rusaknya media penyimpanan	***12.3.1 Information Backup***	Prosedur Backup dan Restore
			Prosedur Pemeliharaan Hardware
			Kebijakan Keamanan Informasi
Manipulasi data	Username password diketahui orang lain	***9.2.3 Management of privileged access rights***	Prosedur Pengelolaan Hak akses
		9.4.2 Secure log-on procedures	Kebijakan Keamanan Informasi

Potensi Mode Kegagalan	Potensial Penyebab Kegagalan	Kontrol ISO 27002 : 2013	Prosedur dan kebijakan yang Dihasilkan
		9.4.3 Password management system	Prosedur pengelolaan Password
			Kebijakan Keamanan Informasi
		9.1.1 Access control policy	Kebijakan Pengendalian Hak akses
Aplikasi diakses oleh pihak yang tidak berwenang	Username dan password diketahui oleh pengguna lain	***9.4.1 Information access restriction***	Kebijakan Keamanan informasi
		9.4.2 Secure log-on procedures	Kebijakan Keamanan Informasi
		9.4.3 Password management system	Prosedur pengelolaan Password

Potensi Mode Kegagalan	Potensial Penyebab Kegagalan	Kontrol ISO 27002 : 2013	Prosedur dan kebijakan yang Dihasilkan
			Kebijakan Keamanan Informasi
		9.1.1 Access control policy	Kebijakan Pengendalian Hak akses
Kerusakan kabel LAN	Kurangnya kontrol pengamanan kabel	***11.2.3 Cabling security***	Prosedur Keamanan kabel
			Kebijakan Kemanan Hardware dan Jaringan
Sharing password aplikasi	Kelalaian karyawan yang memiliki hak akses	***7.1.2 Terms and conditions of employment***	Kebijakan Human resources security
		7.2.2 Information security awareness, education and training	Prosedur Pelatihan dan pengembangan SDM
			Kebijakan Human resources security

Potensi Mode Kegagalan	Potensial Penyebab Kegagalan	Kontrol ISO 27002 : 2013	Prosedur dan kebijakan yang Dihasilkan
		9.1.1 Access control policy	Kebijakan Pengendalian Hak akses
Data tidak sesuai (tidak valid)	Kesalahan input data	***12.4.1 Event logging***	Kebijakan keamanan Informasi
			Kebijakan pengendalian hak akses
		12.4.2 Protection of log information	Kebijakan keamanan Informasi

5.5 Penjelasan pembentukan prosedur dan kebijakan

Pada tahap ini akan di jelaskan bagaimana prosedur dan kebijakan dapat terbentuk berdasarkan penilaian risiko keamanan aset informasi yang memiliki tingkat *High dan Very High* dan hasil rekomendasi pengendalian risiko.

Dilihat dari hasil pemetaan pada tabel 5.11 diatas didapatkan 4 kebijakan dan 6 prosedur dimana kebijakan dan prosedur dibuat berdasarkan hasil rekomendasi pengendalian risiko dan risiko yang terjadi berikut penjelasan pembentukan prosedur dan kebijakan yang di hasilkan :

5.5.1 Kebijakan pengendalian hak akses

Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut :

- Aplikasi diakses oleh pihak tidak berwenang
- Sharing password karena kelalaian karyawan
- Adanya manipulasi data karena username password diketahuai orang lain

Dari risiko yang dijelaskan peneliti menentukan dengan membuat **kebijakan pengendalian hak akses** yang menggunakan acuan ISO27002:2013 pada klausa *9.1.1 Access control policy* yang berisikan mengenai pedoman peraturan hak akses yang diberikan, selain itu perusahaan juga belum memiliki dokumen kebijakan tertulis mengenai hak akses. Kebijakan ini akan terkait juga dengan **prosedur pengelolaan hak akses.**

5.5.1.1 Prosedur pengelolaan hak akses

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada perusahaan, prosedur ini akan menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam

prosedur pengelolaan hak akses dengan acuan ISO27002:2013 pada klausa *9.2.3 Management of privileged access* rights yang berisikan mengemai cara melakukan pengelolaan hak akses yang benar, selain itu juga aktivitas yang dilakukan akan disesuaikan dengan sumber daya pada unit bisnis yang ada pada CV cempaka tulungagung.

5.5.2 Kebijakan keamanan informasi

Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut :

- Data Hilang karena kelalaian administrator
- Manipulasi data karena username password diketahui pengguna lain.
- Aplikasi diakses oleh tidak berwenang karena username password diketahui pengguna lain
- Data tidak sesuai karena kesalahan input

Dari risiko yang dijelaskan peneliti menentukan dengan membuat **kebijakan keamanan informasi** yang menggunakan acuan ISO27002:2013 pada klausa *9.4.1 Information access restriction, 9.4.2 Secure log-on procedures, 9.4.3 Password management system, 12.4.1 Event logging, 12.4.2 Protection of log information, 12.4.3 Administrator & Operator Logs* yang berisikan tentang pedoman pengelolaan sistem, pedoman log-on pada sistem, pedoman password pengguna, pedoman pengelolaan backup informasi, dan juga peraturan adanya log kegiatan pada setiap aplikasi, dan pencatatan pada setiap kegiatan, selain itu perusahaan juga belum memiliki dokumen kebijakan tertulis mengenai keamanan informasi. Kebijakan ini akan terkait dengan 2 prosedur yaitu **prosedur pengelolaan password dan prosedur backup dan restore**

5.5.2.1 Prosedur pengelolaan password

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada perusahaan, prosedur ini akan

menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan password dengan acuan ISO27002:2013 pada *9.4.3 Password management system* yang berisikan mengenai tata cara dalam manajemen password, selain itu juga aktivitas yang dilakukan akan disesuaikan dengan sumber daya pada unit bisnis yang ada pada CV cempaka tulungagung.

5.5.2.2 Prosedur backup dan restore

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada perusahaan, prosedur ini akan menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan password dengan acuan ISO27002:2013 pada *12.3.1 Information Backup* yang berisikan tata cara melakukan backup data, selain itu aktivitas yang dilakukan akan disesuaikan dengan sumber daya pada unit bisnis yang ada pada CV cempaka tulungagung.

5.5.3 Kebijakan pengelolaan hardware dan jaringan

Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut :

- Kerusakan PC karena kesalahan konfigurasi
- Kerusakan Server karena kesalahan konfigurasi
- Data hilang karena rusaknya media penyimpanan
- Kerusakan kabel lan karena kurangnya kontrol pengamanan kabel

Dari risiko yang dijelaskan peneliti menentukan dengan membuat **kebijakan pengelolaan hardware dan jaringan** yang menggunakan acuan ISO27002:2013 pada klausa *11.2.4 Equipment maintenance, 11.2.3 Cabling security* yang berisikan tentang pedoman pengelolaan hardware dan jaringan, selain itu perusahaan juga belum memiliki dokumen kebijakan yang tertulis mengenai hardware dan jaringan.

Kebijakan ini akan terkait dengan 2 prosedur yaitu **prosedur perawatan hardware dan prosedur pengamanan kabel.**

5.5.3.1 Prosedur perawatan hardware

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada perusahaan, prosedur ini akan menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam prosedur pengelolaan password dengan acuan ISO27002:2013 pada *12.3.1 Information Backup* yang berisikan tata cara melakukan backup data, selain itu aktivitas yang dilakukan akan disesuaikan dengan sumber daya pada unit bisnis yang ada pada CV cempaka tulungagung.

5.5.4 Kebijakan human resource security

Kebijakan ini dibuat berdasarkan risiko dan hasil rekomendasi pengendalian risiko yang sudah dilakukan dimana risiko yang teridentifikasi sebagai berikut :

- Aplikasi diakses oleh pihak tidak berwenang karena password diketahui pengguna lain.
- Data hilang karena kelalaian administrator
- Sharing password karena kelalaian karyawan yang memiliki hak akses

Dari risiko yang dijelaskan peneliti menentukan dengan membuat ***kebijakan human resource security*** yang menggunakan acuan ISO27002:2013 pada klausa *7.1.2 Terms and conditions of employment***,** *7.2.2 Information security awareness, education and training* yang berisikan mengenai pembuatan kontrak perjanjian, dan pelatihan serta edukasi mengenai kesadaran mengenai keamanan informasi selain itu perusahaan juga belum memiliki dokumen kebijakan tertulis mengenai peraturan keamanan sumber daya manusia. Kebijakan ini akan terkait juga dengan **prosedur pelatihan dan pengembangan SDM.**

5.5.4.1 Prosedur pelatihan dan pengembangan SDM

Prosedur ini dibuat karena tidak adanya prosedur operasional secara tertulis pada perusahaan, prosedur ini akan menjelaskan langkah-langkah/aktivitas yang harus dilakukan dan dokumen pendukung apa yang dibutuhkan dalam melakukan pelatihan dan pengembangan SDM dengan acuan ISO27002:2013 pada klausa *7.2.2 Information security awareness, education and training* yang berisikan mengenai tata cara memberikan kesadaran dan edukasi mengenai keamanan informasi, selain itu juga aktivitas yang dilakukan akan disesuaikan dengan sumber daya pada unit bisnis yang ada pada CV cempaka tulungagung.

BAB VI
HASIL DAN PEMBAHASAN

Bab ini akan menjelaskan kesimpulan dari penelitian ini, beserta saran yang dapat bermanfaat untuk perbaikan di penelitian selanjutnya.

6.1 Prosedur dan Kebijakan yang Dihasilkan dalam Penelitian

Berdasarkan hasil Pemetaan rekomendasi penyesuaian pengendalian risiko, didefinisikan beberapa prosedur yang dapat diusulkan dalam penelitian. Selain itu, prosedur yang dihasilkan berikut ini juga telah disesuaikan dengan pelaksanaan praktik keamanan yang ada pada Bagian Personalia CV Cempaka sehingga telah dapat dipastikan bahwa tidak ada prosedur yang memiliki fungsi dan proses yang sama.

Namun dikarenakan CV Cempaka belum memiliki kebijakan yang terdokumentasi dengan baik, maka penulis melakukan pembuatan dokumen keijakan yang telah dilakukan oleh perusahaan terlebih dahulu. Dengan begitu, diharapkan dokumen prosedur, kebijakan, dan instruksi kerja yang telah dibuat dapat dijalankan dengan selaras. Berikut ini adalah kebijakan dan prosedur yang diusulkan dalam penelitian.

Tabel 6.1 Pemetaan Kontrol ISO 27002 dengan Prosedur dan kebijakan

Kontrol Objektif	Pemenuhan Mitigasi dari Risiko	Ruang Lingkup	Prosedur	Kebijakan
9.1.1 Access control policy	Kelalaian karyawan yang memiliki hak akses	Keamanan Data		Kebijakan Pengendalian Hak akses
	Username password diketahui pengguna lain	Pengelolaan SDM		
		Keamanan Data		
9.2.3 Management of privileged access rights	Username password diketahui orang lain	Keamanan Data	Prosedur Pengelolaan Hak akses	
9.3.1 Use of secret authentication information	Kelalaian Administrator	Keamanan Data		Kebijakan Human resources security
		Pengelolaan SDM		

Kontrol Objektif	Pemenuhan Mitigasi dari Risiko	Ruang Lingkup	Prosedur	Kebijakan
9.4.1 Information access restriction	Username password diketahui orang lain	Keamanan Data		Kebijakan Keamanan Informasi
9.4.2 Secure log-on procedures	password diketahui oleh pengguna lain	Keamanan Software Keamanan Data		Kebijakan Keamanan Informasi
9.4.3 Password management system	Username dan password diketahui oleh pengguna lain	Keamanan Software Keamanan Data	Prosedur Pengelolaan Password	Kebijakan Keamanan Informasi
12.4.1 Event logging	Kesalahan input data	Keamanan Software Keamanan Data		Kebijakan Keamanan Informasi Kebijakan pengendalian hak akses

Kontrol Objektif	Pemenuhan Mitigasi dari Risiko	Ruang Lingkup	Prosedur	Kebijakan
12.4.2 Protection of log information	Kesalahan input data	Keamanan Software Keamanan Data		Kebijakan Keamanan Informasi
12.4.3 Administrator & Operator Logs	Kelalaian Administrator	Keamanan Data Pengelolaan SDM		Kebjakan Keamanan Informasi
12.3.1 Information Backup	Rusaknya media penyimpanan	Keamanan Data	Prosedur Backup dan Restore	Kebijakan Keamanan Informasi
7.1.2 Terms and conditions of employment	Kelalaian karyawan yang memiliki hak akses	Pengelolaan SDM		Kebijakan *Human resources security*

Kontrol Objektif	Pemenuhan Mitigasi dari Risiko	Ruang Lingkup	Prosedur	Kebijakan
7.2.2 Information security awareness, education and training	Kelalaian karyawan yang memiliki hak akses	Pengelolaan SDM	Prosedur Pelatihan dan pengembangan SDM	Kebijakan *Human* resources security
11.2.4 Equipment maintenance	Kesalahan konfigurasi server	Keamanan Hardware	Prosedur Pemeliharaan Hardware	Kebijakan Pengelolaan Hardware dan Jaringan
	Rusaknya media penyimpanan			
	Kesalahan konfigurasi PC			
11.2.3 Cabling security	Kurangnya kontrol pengamanan kabel	Keamanan Jaringan	Prosedur Keamanan Kabel	

Berikut ini merupakan penjelasan dari masing masing prosedur yang akan dibuat untuk mendukung keamanan aset informasi pada CV Cempaka. Jumlah prosedur yang akan dihasilkan adalah sebanyak lima prosedur. Penjelasan untuk masing-masing prosedur keterkaitannya dengan proses kekinian akan dijelaskan pada Tabel 6.2 dibawah ini

Tabel 6.2 Deskripsi prosedur dan kebijakan

Prosedur	Penjelasan
Kebijakan Pengendalian Hak akses	Kebijakan ini dibuat untuk menjamin persyaratan mengenai pemberian hak akses terhadap aset informasi dapat di definisikan dengan tepat dan benar. Dalam kebijakan ini akan di jelaskan mengenai peraturan penggunaan hak akses yang diberikan, tanggung jawab karyawan yang di berikan hak akses, Peraturan penggunaan aplikasi sistem informasi yang dimiliki perusahaan, kebijakan penggunaan data data penting dan lain sebagainya. Kebijakan ini juga di keluarkan bertujuan untuk meminimalisir terjadinya risiko – risiko yang tida di inginkan seperti sharing password, terjadinya kesalahan input, manipulasi data, kehilangan data, password diketahui pengguna lain, aplikasi digunakan oleh orang yang tidak berwenang dan sebagainya

Prosedur	Penjelasan
Kebijakan Pengelolaan Hardware dan Jaringan	Kebijakan ini dibuat untuk memberikan pedoman pada pengelola hardware dan jaringan pada suatu instansi. Pengelola diharapkan mampu menjamin hardware sistem komputer yang dipergunakan akan dapat dioperasikan tanpa henti.
Kebijakan Keamanan Informasi	Kebijakan ini dibuat untuk memberikan pedoman dan peratiran keamanan informasi yang ada pada perusahaan baik pengamanan informasi pada sistem aplikasi dan informasi digital berupa data.
Kebijakan *Human resources security*	Kebijakan ini dibuat untuk memberikan pedoman dan peraturan mengenai pengelolaan SDM dalam mengatasi masalah keamanan aset informasi.
Prosedur Pengelolaan Hak akses	Prosedur ini di buat untuk menjadi pedoman dalam memberikan alokasi dan penggunaan hak akses terhadap sistem informasi yang seharusnya dikontrol dalam rangka melindungi keamanan data baik dari dalam maupun luar lingkungan perusahaan. Pengamanan
Prosedur *Back Up* dan *Restore*	Prosedur Backup dan Restore Data merupakan prosedur yang bertujuan untuk memastikan backup data yang dilakukans secara berkala telah sesuai dan data yang di backup telah lengkap

Prosedur	Penjelasan
Prosedur Perawatan Hardware	Prosedur ini dibuat dimaksudkan sebagai pedoman dan acuan untuk melakukan pengelolaan aset hardware pada perusahaan baik dalam melakukan pengadaan barang , maintenance , penggunaan serta keamanan dari hardware itu sendiri
Prosedur Pengamanan Kabel	Prosedur ini dibuat untuk memastikan bahwa seluruh kabel telekomunikasi yang membawa data dan mendukung layanan informasi pada perusahaan diatur atau dikelola secara terstruktur sehingga terlindungi dari kerusakan
Prosedur Pengelolaan Password	Prosedur ini dibuat dengan tujuan untuk memastikan pengelolaan penggunaan password telah memenuhi kualitas standard *strong* password dan memastikan password setiap pengguna telah sesuai dengan syarat kualitas password
Prosedur pelatihan dan pengembangan SDM	Prosedur ini mengatur segala pelatihan atau edukasi terkait keamanan informasi untuk karyawan yang mampu meningkatkan kualitas baik secara intelektual maupun kepribadian, sehingga mampu menjaga aset informasi yang dimiliki oleh perusahaan
Prosedur Keamanan *Information Log*	Prosedur ini dibuat untuk memastikan Pengamanan dari log event baik pada sistem aplikasi maupun berupa catatan ter dokumentasi

6.2 Perancangan Struktur dan Isi SOP

Pada sub-bab ini akan dijelaskan mengenai perancangan SOP yang akan dibuat. Perancangan SOP ini mengacu pada peraturan pemerintah (Menteri Pedahayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia nomor 35 tahun 2012) terkait dengan pedoman penyusunan standar operasional prosedur administrasi pemerintah. Namun, dalam perancangan struksur dan isi SOP tidak keseluruhan struktur konten akan mengacu pada standard tersebut karena akan disesuaikan dengan kebutuhan. Struktur dokumen SOP yang akan disusun ini akan dihasilkan ke dalam sebuah buku produk yang akan diberikan kepada pihak CV Cempaka sebagai rekomendasi tata kelola keamanan aset Informasi.

Adapun struktur atau konten yang akan dimasukkan ke dalam kerangka dokumen *Standard Operating Procedure* (SOP) Keamanan Aset Informasi pada CV Cempaka Tulungagung dapat dilihat pada tabel 6.3.

Tabel 6.3 Deskripsi prosedur dan kebijakan

Sturktur Bab	Sub-Bab	Konten
Pendahuluan	Tujuan	Deskripsi umum dokumen SOP Keamanan Aset Informasi
	Ruang Lingkup	
	Overview Keamanan Data	Aspek Kemanan Aset Informasi
	Evaluasi Penilaian Risiko Keamanan Aset Informasi pada CV Cempaka	Tabel Daftar Prioritas Risiko Keamanan Aset Informasi

Sturktur Bab	Sub-Bab	Konten
Kebijakan Pengendalian Hak Akses	Tujuan	Deskripsi umum Pengendalian Hak akses dan Keamanan Data
	Ruang Lingkup	
	Referensi	Acuan yang digunakan dalam pembuatan kebijakan
	Rincian Kebijakan	• Pengelolaan hak akses • hak akses pihak ketiga
	Dokumen Terkait	• Prosedur pengelolaan hak akses
Kebijakan Keamanan Informasi	Tujuan	Deskripsi umum kebijakan keamanan Informasi
	Ruang Lingkup	
	Referensi	Acuan yang digunakan dalam pembuatan kebijakan
	Rincian Kebijakan	• Pengelolaan sistem informasi • Pengelolaan sistem *log-on* • Password pengguna • Pengelolaan backup dan restore informasi

Sturktur Bab	Sub-Bab	Konten
	Dokumen Terkait	• Prosedur Pengelolaan Password • Prosedur Backup dan Restore
Kebijakan Pengelolaan Hardware dan Jaringan	Tujuan	• Deskripsi umum kebijakan pengelolaan hardware dan jaringan
	Ruang Lingkup	
	Referensi	• Acuan yang digunakan dalam pembuatan kebijakan
	Rincian Kebijakan	• Pengelolaan hardware • Pengelolaan jaringan
	Dokumen Terkait	• Prosedur Perawatan Hardware • Prosedur Pengamanan Kabel
Kebijakan *Human Resource Security*	Tujuan	• Deskripsi umum kebijakan human resource security
	Ruang Lingkup	
	Referensi	• Acuan yang digunakan dalam pembuatan kebijakan
	Rincian Kebijakan	• Keamanan SDM • Tanggung jawab penggunaan hak akses

Sturktur Bab	Sub-Bab	Konten
	Dokumen Terkait	• Prosedur pelatihan dan pengembangan SDM
Prosedur Pengelolaan Hak Akses	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	• Proses pemberian akses • Pergantian dan prnghapusan hak akses sistem aplikasi
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Pengelolaan Password	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	• Proses pengelolaan password • Proses permintaan pergantian password
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur *Backup* dan *Restore*	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	

Sturktur Bab	Sub-Bab	Konten
	Referensi	Acuan yang digunakan dalam pembuatan prosedur
	Rincian Prosedur	• Proses umum sebelum melakukan backup • Proses backup secara berkala • Proses pengujian backup secara berkala • Proses restore data
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Perawatan Hardware	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	• Proses pemeliharaan secara parsial • Proses pemeliharaan secara keseluruhan
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur Kemanan Kabel	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	

Sturktur Bab	Sub-Bab	Konten
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	Prosedur pengaman kabel
	Bagan Alur SOP	Tabel Bagan Alur SOP
Prosedur pelatihan dan pengembangan SDM	Tujuan	Deskripsi umum SOP
	Ruang Lingkup	
	Definisi	Penjelasan istilah dalam prosedur
	Rincian Prosedur	• Proses pelatihan pegawai perusahaan • Proses pelatihan pegawai magang
	Bagan Alur SOP	Tabel Bagan Alur SOP
Instruksi	Instruksi Pergantian hak akses	
	Instruksi backup data	
	Instruksi restore data	
	Instruksi reset password	
Formulir	Form pengelolaan hak akses	
	Form kontrak hak akses	
	Form log pengelolaan hak akses	
	Form perbaikan sistem informasi	
	Form permintaan pergantian password	

Sturktur Bab	Sub-Bab	Konten
	Form klasifikasi data	
	Form log backup data	
	Form restore data	
	Form pemeliharaan perangkat TI	
	Form berita acara kerusakan	
	Form laporan evaluasi pengelolaan perangkat TI	
	Form data pegawai	
	Form evaluasi kegiatan pengembangan kompetensi	

6.3 Hasil Perancangan SOP

Pada sub-bab ini akan dijelaskan mengenai hasil akhir dari perencanaan dan perancangan SOP yang telah diinisasi berdasarkan dari sub-bab sebelumnya. Pada tabel 6.4 berikut menampilkan pemetaan dari perancangan SOP dengan formulir dan instruksi yang digunakan pada setiap prosedur.

Tabel 6.4 Pemetaan Dokumen SOP dan Formulir serta Instruksi

No Dokumen	Nama Dokumen SOP	No Dokumen	Dokumen Terkait
PO – 01	Prosedur pengelolaan hak akses	KB – 01	Kebijakan pengendalian hak akses
		IN – 01	Instruksi Pergantian hak akses
		FM – 01	Formulir pengelolaan hak akses
		FM – 02	Formulir kontrak hak akses
		FM – 03	Formulir log pengelolaan hak akses
PO – 02	Prosedur pengelolaan password	KB – 02	Kebijakan Kemanan Informasi
		IN – 04	Instruksi reset password
		FM – 04	Formulir perbaikan sistem informasi
		FM – 05	Formulir

No Dokumen	Nama Dokumen SOP	No Dokumen	Dokumen Terkait
			permintaan pergantian password
PO – 03	Prosedur *backup and restore*	KB – 02	Kebijakan Kemanan Informasi
		IN – 03	Instruksi backup data
		IN – 04	Instruksi restore data
		FM – 06	Formulir klasifikasi data
		FM – 07	Formulir Log backup data
		FM – 08	Kebijakan pengelolaan hardware dan jaringan
PO – 04	Prosedur perawatan hardware	KB – 03	Kebijakan pengelolaan hardware dan jaringan
		FM – 09	Formulir pemeliharaan perangkat TI
		FM – 10	Formulir berita acara kerusakan
		FM – 11	Formulir laporan evaluasi penggunaan fasilitas TI

No Dokumen	Nama Dokumen SOP	No Dokumen	Dokumen Terkait
PO – 05	Prosedur keamanan kabel	KB – 03	Kebijakan pengelolaan hardware dan jaringan
		FM – 09	Formulir pemeliharaan perangkat TI
		FM – 10	Formulir berita acara kerusakan
PO – 06	Prosedur pengelolaan dan pengembangan SDM	KB – 04	Kebijakan human resource security
		FM – 12	Formulir data pegawai
		FM – 13	Formulir evaluasi kegiatan pengembangan kompetensi

Berikut adalah penjelasan dari setiap prosedur dan kebijakan beserta dokumen pendukung yaitu formulir yang dibutuhkan pada setiap proses didalamnya.

6.3.1. Kebijakan pengendalian hak akses

Sesuai dengan kontrol dalam ISO27002:2013 sub klausul 9.1.1 *access control policy*, 12.4.1 *Event* logging, dalam kebijakan ini terdapat beberapa hal yang terkandung di dalamnya yang mengatur mengenai pengelolaan hak akses. terlampir pada Lampiran F.

6.3.2. Kebijakan keamanan informasi

Sesuai dalam kontrol ISO 27002:2013 pada klausul 9.4.1 *Informastion access restriction, 9.4.2 Secure log-on procedures, 9.4.3 Password management system, 12.3.1 Information Backup, 12.4.1 Event logging, 12.4.2 Protection of log information,* dalam kebijakan memuat peraturan untuk menjamin keamanan dari informasi penting baik informasi digital dan fisik yang dimiliki perusahaan, terlampir pada Lampiran F.

6.3.3. Kebijakan pengelolaan hardware dan jaringan

Sesuai dalam kontrol ISO 27002:2013 pada klausul *11.2.3 Cabling Security* dan *11.2.4. Equipment Maintenance,* dalam kebijakan memuat peraturan untuk menjamin fasilitas perangkat hardware dan jaringan agar dapat selalu beroperasi selama proses bisnis berlangsung, terlampir pada Lampiran F.

6.3.4. Kebijakan human resource security

Sesuai dalam kontrol ISO 27002:2013 pada klausul *7.1.2. Term and conditions of employement, 7.2.2. Information Security awareness, education, training, 9.3.1. Use secret authentication,* dalam kebijakan memuat peraturan kepada seluruh civitas perusahaan dalam memberi perlindungan keamanan pada aset informasi yang dimiliki perusahaan, terlampir pada Lampiran F.

6.3.5. Prosedur Pengelolaan Hak Akses

Prosedur pengelolaan hak akses merupakan prosedur untuk menjadi pedoman dalam memberikan alokasi dan penggunaan hak akses terhadap sistem informasi yang seharusnya dikontrol dalam rangka melindungi keamanan data baik dari dalam maupun luar lingkungan perusahaan. terlampir pada Lampiran G.

6.3.6. Prosedur Pengelolaan Password

Prosedur Manajemen password merupakan prosedur untuk memastikan pengelolaan penggunaan password telah memenuhi kualitas standard *strong* password dan memastikan password

setiap pengguna telah sesuai dengan syarat kualitas password, terlampir pada Lampiran G.

6.3.7. Prosedur Back Up dan Restore

Prosedur ini menjelaskan langkah langkah dalam aktivitas backup yang sesuai dengan kontrol ISO27002:2013, sub klausul 12.3.1 *information backup*. Prosedur Back up dan restore dibagi kedalam empat proses utama yang terdiri dari beberapa aktivitas yang berurutan. Namun, sebelum mendeskripsikan prosedur penangan secara terstruktur, terlebih dahulu didefinisikan informasi pendukung yang dibutuhkan untuk menunjang aktivitas didalam prosedur tersebut. Pendefinisan tesebut berguna untuk menentukan strategi back up yang sesuai dengan kebutuhan bisnis. Pendefinisan dalam prosedur Back up dibagi kedalam tiga yaitu pendefinisian klasifikasi data, pendefinisian kritikalitas data dan pendefinisian tipe back up, terlampir pada Lampiran G

1 Pendefinisian Klasifikasi Data

Dalam penelitian ini, diusulkan pendefinisian klasifikasi data berdasarkan tingkat sensitivtas data. pendefinisian klasifikasi data berguna bagi manajemen untuk menentukan tipe back up yang sesuai. Pada tabel 6.5 berikut ini adalah klasifikasi data yang terdiri dari 3 tingkatan klasifikasi.

Tabel 6.5 Klasifikasi Data

Klasifikasi Data	Keterangan
Sangat Rahasia (*Strictly Confidential*)	Data yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian bagi perusahaan CV Cempaka
Rahasia (*Confidential*)	Data yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan atau menurunkan citra dan reputasi perusahaan CV Cempaka

Klasifikasi Data	Keterangan
Terbatas (*Internal Use Only*)	Data yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak sah atau tidak berhak akan mengganggu kelancaran kegiatan tetapi tidak akan mengganggu citra dan reputasi perusahaan CV Cempaka

2 Pendefinisian Kritikalitas Data

Dalam penelitian ini, diusulkan pendefinisian klasifikasi data yang didasarkan pada tingkat kritikalitas data. pengklasifikasian kritikalitas data ini berguna untuk menentukan prosedur backup yang sesuai. Pada tabel 6.6 berikut ini adalah pendefinisian dari kritikalitas data yang dibagi kedalam tiga tingkatan kritikalitas data.

Tabel 6.6 Kritikalitas Data

Tingkat Kritikal Data	RPO	MTD	Penanganan	
			Full Backup	Differential/ Incremental Backup
Tinggi	Maks 24 jam	Maks 24 jam	1 x Seminggu	Maks 24 jam
Sedang	Maks 1 minggu	Maks 1 minggu	1 x Sebulan	Maks 1 Minggu
Rendah	> 1 Minggu	> 1 Minggu	Min 1 x 3 Bulan	> 1 Minggu

Kritikaslitas data didasarkan pada RPO (*Recovery Point Object*) dan MTD (*Maximum Tolerable Downtime*). Berikut adalah masing masing penjelasannya.

- RPO (*Recovery Point Object*)
  RPO adalah jumlah waktu maksimal yang dapat ditoleransi perusahaan terhadap kehilangan data akibat risiko yang terjadi.
- MTD (*Maximum Tolerable Downtime*)
  MTD adalah jumlah waktu maksimal yang dapat ditoleransi oleh perusahaan terhadap kegagalan proses bisnis.

3 Pendefinisian Tipe Back Up

Dalam penelitian ini juga didefinisikan tipe backup pada server yang dapat dilakukan secara bekala dengan kurun waktu setiap hari setelah jam kerja aktif. Tipe backup yang umum diimplementasikan yaitu *full backup* dan *differential/incremental backup*. Pada tabel 6.7 berikut adalah penjelasan dari masing masing tipe back up.

Tabel 6.7 Tipe Back Up

Tipe Backup	Deskripsi
Full Backup	Backup dilakukan untuk seluruh sumber data/file termasuk folder ke media lain dan membutuhkan waktu serta ruang yang besar.
Differential/Incremental Backup	Backup dilakukan untuk file-file yang berubah dari saat backup terakhir dibuat.

Berikut merupakan SOP Back up secara detail beserta pemetaannya terhadap kontrol ISO27002:2013, sub klausul 12.3.1 *information backup*.

6.3.8. Prosedur Perawatan Hardware

Prosedur perawatan hardware ini merupakan pedoman dan acuan untuk melakukan pengelolaan aset hardware pada perusahaan baik dalam melakukan pengadaan barang, maintenance, penggunaan serta keamanan dari hardware itu sendiri, terlampir pada Lampiran G.

6.3.9. Prosedur Keamanan kabel

Prosedur keamanan kabel merupakan prosedur yang berguna untuk memastikan bahwa seluruh kabel telekomunikasi yang membawa data dan mendukung layanan informasi pada perusahaan diatur atau dikelola secara terstruktur sehingga terlindungi dari kerusakan, terlampir pada Lampiran G.

6.3.10. Prosedur Pelatihan dan Pengembangan SDM

Prosedur Pelatihan dan Pengembangan SDM merupakan prosedur yang mengatur segala pelatihan atau edukasi terkait keamanan informasi untuk karyawan yang mampu meningkatkan kualitas baik secara intelektual maupun kepribadian, sehingga mampu menjaga aset informasi yang dimiliki oleh perusahaan, terlampir pada Lampiran G.

6.4 Instruksi Kerja

Dalam mendukung pelaksanaan SOP, dibutuhkan beberapa instruksi kerja yaitu instruksi kerja pergantian hak akses sistem informasi, instruksi kerja back up data, instruksi kerja restore data dan instruksi kerja reset password.

6.4.1 Instruksi kerja pergantian hak akses sistem informasi

Dalam dokumen prosedur pengelolaan hak akses dibutuhkan sebuah instruksi kerja yaitu instruksi dalam melakukan pergantian

hak akses yang bertujuan untuk membantu pegawai baru untuk melakukan pergantian hak akses. terlampir pada Lampiran H

6.4.2 Instruksi kerja backup data

Dalam dokumen Prosedur Backup dan Restore, dibutuhkan sebuah instruksi kerja yaitu instruksi kerja back up yang bertujuan untuk membantu kerja DB Administrator baru dalam mempelajari proses back up data maupun back up file, terlampir pada Lampiran H.

6.4.3 Instruksi kerja restore data

Dalam dokumen Prosedur Backup dan Restore, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja restore yang bertujuan untuk membantu kerja DB Administrator baru dalam mempelajari proses restore, terlampir pada Lampiran H.

6.4.4 Instruksi kerja reset password

Dalam dokumen Prosedur pengelolaan password, juga dibutuhkan sebuah instruksi kerja yaitu instruksi kerja reset password yang bertujuan untuk membantu kerja pegawai baru dalam mempelajari proses reset password, terlampir pada Lampiran H.

6.5 Hasil Perancangan Formulir

Dalam mendukung pelaksanaan SOP, dibutuhkan beberapa formulir dengan tujuan mendokumentasikan dengan baik setiap aktivitas. Berikut adalah 13 formulir yang dibutuhkan untuk mendukung pelaksanaan SOP,

6.5.1 Formulir Pengelolaan hak akses

Formulir pengelolaan hak akses adalah formulir yang digunakan dalam prosedur pengelolaan hak akses dimana formulir ini berguna untuk mendokumentasikan pemberian hak akses pada pengguna sistem untuk dilakukan persetujuan pada pihak manajemen. terlampir pada Lampiran I.

6.5.2 Formulir kontrak perjanjian hak akses

Formulir kontrak perjanjian hak akses adalah formulir yang digunakan dalam prosedur pengelolaan hak akses yang berfungsi sebagai sebuah peraturan dan tanggung jawab yang harus disetujui oleh pengguna sistem jika hak akses diberikan ,terlampir pada Lampiran H.

6.5.3 Formulir log pengelolaan hak akses

Formulir log pengelolaan hak akses adalah formulir yang berfungsi sebagai media pencatatan pemberian, penghapusan ataupun pergantian hak akses yang dilakukan ,terlampir pada Lampiran H.

6.5.4 Formulir perbaikan sistem informasi

Formulir perbaikan sistem informasi adalah formulir yang digunakan untuk melakukan perbaikan pada sistem informasi atau aplikasi yang dimiliki perusahaan, terlampir pada Lampiran H.

6.5.5 Formulir permintaan reset password

Formulir permintaan pergantian password adalah formulir yang digunakan untuk prosedur pergantian password sebelum meminta pergantian password pengguna harus mengisi formulir ini,terlampir pada Lampiran H.

6.5.6 Formulir klasifikasi data

Formulir klasifikasi data digunakan untuk menentukan strategi back up yang akan digunakan. Berdasarkan kontrol dalam ISO27002:2013, penentuan strategi back up data ditentukan sesuai dengan kebutuhan bisnis organisasi dilihat dari kebutuhan keamanan dan tingkat kritikalitas data. Klasifikasi data akan didasarkan pada tingkat sensitivitas data dan tingkat kritikalitas data, terlampir pada Lampiran H.

6.5.7 Formulir log backup data

Formulir log back up digunakan oleh DB administrator untuk melakukan pemantauan (*monitoring*) secara berkala pada hasil eksekusi back up data. Tujuan dari formulir log back up data ini adalah untuk memastikan bahwa hasil eksekusi back up data telah akurat dan lengkap dan juga untuk memastikan keberhasilan data yang ter-back up dan data yang tidak berhasil di-back up, terlampir pada Lampiran I.

6.5.8 Formulir restore data

Formulir restore digunakan untuk permintaan kebutuhan restore data oleh pihak tertentu/unit kerja tertentu. Formulir restore data dibutuhkan untuk menjaga integritas data dan memastikan bahwa setiap proses restore data terdokumentasi dengan baik dan telah di validasi oleh pegawai bagian personalia yang bertanggung jawab, terlampir pada Lampiran I.

6.5.9 Formulir pemeliharaan perangkat TI

Formulir pemeliharaan perangkat TI adalah formulir yang digunakan untuk melakukan pencatatan kegitan (log) dalam melakukan perbaikan perangkat TI yang dimiliki perusahaan, terlampir pada Lampiran I.

6.5.10 Formulir berita acara kerusakan

Formulir berita acara kerusakan adalah formulir yang digunakan untuk pelaporan kerusakan pada perangkat TI yang dimiliki perusahaan, terlampir pada Lampiran I.

6.5.11 Formulir laporan evaluasi pengelolaan perangkat TI

Formulir laporan evaluasi adalah formulir yang digunakan dalam pencatatan setiap kegiatan pengelolaan perangkat TI baik itu perbaikan secara parsial maupun keseluruhan yang dilakukan, terlampir pada Lampiran I.

6.5.12 Formulir data pegawai

Formulir data pegawai adalah formulir yang digunakan perusahaan dalam prosedur pelatihan dan pengembangan SDM untuk mencatat peagwai yang mengikuti program pelatihan yang diadakan perusahaan terkait dengan keamanan aset informasi, terlampir pada Lampiran I.

6.5.13 Formulir evaluasi kegiatan pengembangan kompetensi.

Formulir evaluasi kegiatan pengembangan kompetensi adalah formulir digunakan untuk melakukan evaluasi pelatihan maupun pengembangan pegawai yang dilakukan perusahaan, terlampir pada Lampiran I.

6.6 Hasil Pengujian SOP

Pengujian SOP dilakukan dengan verifikasi dan validasi. Verifikasi dilakukan dengan wawancara untuk memastikan kesesuian antara prosedur yang dihasilkan dengan kebutuhan CV Cempaka Tulungagung. Sementara validasi dilakukan dengan cara mensimulasikan SOP untuk mengetahui ketepatan prosedur ketika diimplementasikan dalam kasus yang nyata.

6.6.1 Hasil Verifikasi

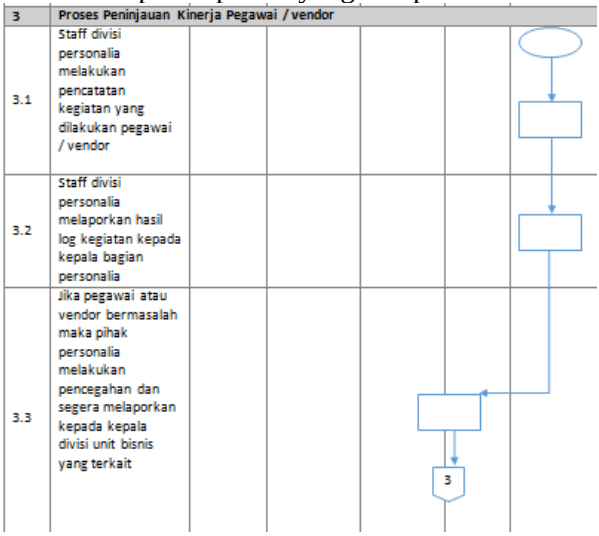
Verifikasi SOP dilakukan dengan cara wawancara pada Kasie personalia dan administrator yang hasilnya secara detail akan dilampirkan pada Lampiran E. Dari hasil verifikasi, dibutuhkan beberapa revisi dokumen SOP, yaitu :

1. **Pemisahan kebijakan pengendalian hak akses dan keamanan informasi**
   Dalam kebijakan ini dilakukan pemisahan antara kebijakan pengendalian hak akses dan kemanan informasi menjadi 2 bagian yang berbeda kebijakan pengendalian akses disendirikan dan kebijakan keamanan informasi disendirikan

karena keduanya memiliki peraturan dan pedoman yang berbeda.

2. **Penambahan kebijakan Human resource security**
   Sebelum adanya kebijakan ini tidak ada kebijakan mengenai pengelolaan sdm terkait keamanan informasi sehingga perusahaan meminta adanya kebijakan yang mengatur mengenai tanggung jawab penggunaan hak akses dan pengelolaan keamanan untuk pegawai.

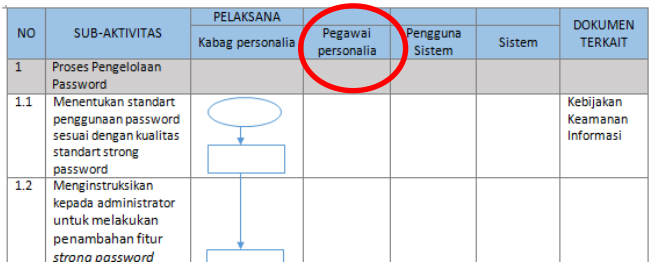
3. **Penghapusan proses pada prosedur pengelolaan hak akses**
   Setelah melakukan verifikasi kasie dan administrator
   Melakukan koreksi pada proses prosedur pengelolaan hak akses pada klausa 4.3 seblumnya ada proses peninjauan kinerja pegawai yang minta untuk di hapus saja karena untuk peninjauan kinerja perusahaan memiliki proses sendiri, pada gambar 6.1 merupakan proses yang dihapuskan.



Gambar 6.1 Prosedur pengelolaan hak akses yang dihapus

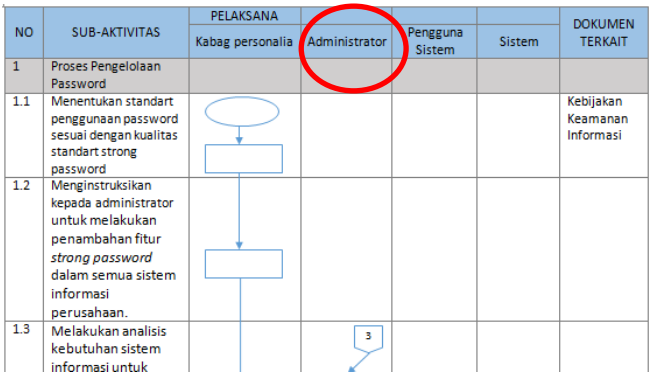
4. **Perubahan pelaksana dalam prosedur pergantian password**

Setelah melakukan verifikasi pada kasie bagian personalia melakukan koreksi pada pelaksana pada prosedur pergantian password bahwa pelaksana yang menjalankan perubahan password maupun perubahan sistem bukanlah pegawai personalia melainkan lebih dikerucutkan menjadi administrator. Perubahan yang dilakukan dapat dilihat pada gambar 6.2 merupakan pelaksanaan sebelum perubahan dan gambar 6.3.



NO	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Kabag personalia	Pegawai personalia	Pengguna Sistem	Sistem	
1	Proses Pengelolaan Password					
1.1	Menentukan standart penggunaan password sesuai dengan kualitas standart strong password					Kebijakan Keamanan Informasi
1.2	Menginstruksikan kepada administrator untuk melakukan penambahan fitur *strong password*					

Gambar 6.2 Pelaksana prosedur pergantian password

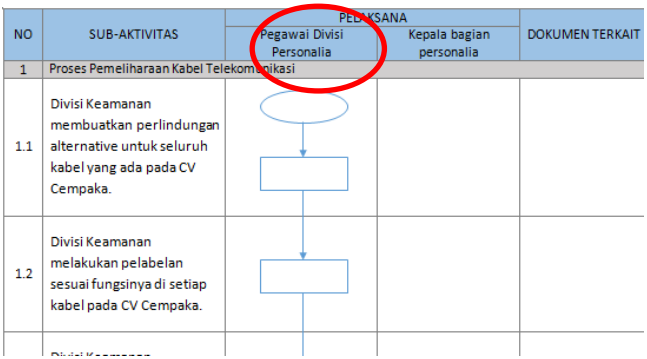


NO	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Kabag personalia	Administrator	Pengguna Sistem	Sistem	
1	Proses Pengelolaan Password					
1.1	Menentukan standart penggunaan password sesuai dengan kualitas standart strong password					Kebijakan Keamanan Informasi
1.2	Menginstruksikan kepada administrator untuk melakukan penambahan fitur *strong password* dalam semua sistem informasi perusahaan.					
1.3	Melakukan analisis kebutuhan sistem informasi untuk		3			

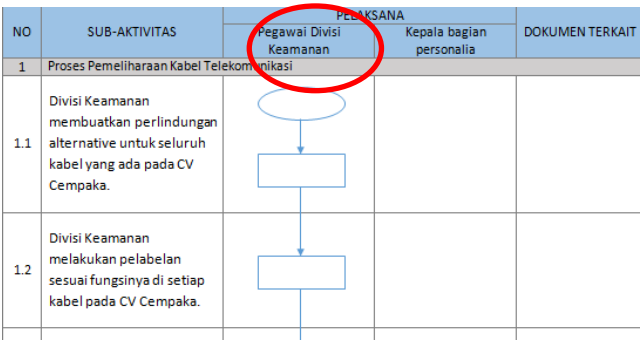
Gambar 6.3 Pelaksana prosedur pergantian password sesudah perubahan

5. Perubahan pelaksana dalam prosedur keamanan kabel

Setelah melakukan verifikasi kasie personalia melakukan koereksi pada pelaksana pada prosedur keamanan kabel bahwa untuk prosedur keamanan kabel pelaksana bukan dari pegawai divisi personalia melainkan pegawai divisi kemanan yang disetujui oleh kepala bagian personalia. Perubahan yang dilakukan dapat dilihat dari gambar 6.4 sebelum dan gambar 6.5 sesudah perubahan.



Gambar 6.4 Pelaksana prosedur keamanan kabel sebelum perubahan



Gambar 6.5 Pelaksanan prosedur keamanan kabel sesudah perubahan

6.6.2 Hasil Validasi

Validasi SOP dilakukan dengan mensimulasikan beberapa aktivitas operasional yang benar-benar terjadi. Validasi yang dilakukan tidak mencakup semua perosedur karena keterbatasan sumber daya pendukung dan kondisi dalam bagian personalia dan umum. Berikut adalah pemetaan antara masing-masing prosedur dan skenario simulasinya yang dijelaskan dalam Tabel 6.8.

Tabel 6.8 Deskripsi prosedur dan kebijakan

No	SOP	Skenario	Tanggal	Keterangan
1	Prosedur pengelolaan hak akses	Administrator melakukan proses pemberian hak akses pada pengguna baru	5 Januari 2017	Dilakukan dengan baik
2	Prosedur pengelolaan password	Pengguna sistem meminta perubahan password pada administrator dan administrator menyetujuinya	5 Januari 2017	Dilakukan dengan baik

No	SOP	Skenario	Tanggal	Keterangan
3	Prosedur backup and restore	Kasie personalia melakukan klasifikasi data untuk dilakukan backup setelah itu administrator melakukan backup dan merestore kembali data yang di backup	5 Januari 2017	Dilakukan dengan baik
4	Prosedur perawatan hardware	Seorang pegawai pabrik pegawai melaporkan kerusakan hardware printer, pegawai bagian personalia merespon dengan melakukan perbaikan dan mencatat proses pemeliharaan yang dilakukan	5 Januari 2017	Dilakukan dengan baik
5	Prosedur keamanan kabel	Pegawai melaporkan kerusakan pada divisi keamanan mengenai wifi	5 Januari 2017	Dilakukan dengan terbatas yatu hanya melakukan mengisi formulir berita acara

No	SOP	Skenario	Tanggal	Keterangan
		yang tiba tiba terputus, divisi keamanan menanggapi dan memproses melakukan proses perbaikan kabel lalu mencatat pada log kegiatan		kerusahakan karena dalam pemeliharaan atau perbaikan wifi bekerjasama dengan vendor tau pihak ketiga
6	Prosedur pelatihan dan pengembangan SDM	Membuat permintaan keikutsertaan dalam program pelatihan, pegawai divisi pegawaian menyebarkan pemberitahuan, setelah itu pegawai divisi kepegawaian mencatat pegawai yang hadir, membuat laporan dan melakukan evaluasi	5 Januari 2017	Skenario ini tidak dilakukan karena terbatasnya sumber daya dan terbatasnya waktu sehingga prosedur ini hanya di baca dan di validasi oleh pihak perusahaan cv cempaka

Halaman Sengaja Dikosongkan

BAB VII
KESIMPULAN DAN SARAN

Bab ini akan menjelaskan kesimpulan dari penelitian ini, beserta saran yang dapat bermanfaat untuk perbaikan di penelitian selanjutnya.

7.1. Kesimpulan

Kesimpulan yang dibuat adalah jawaban dari perumusan masalah yang telah didefinisikan sebelumnya dan berdasarkan hasil penelitian yang telah dilakukan. Kesimpulan yang didapat dari tahap analisis hingga perancangan dan validasi dokumen produk adalah :

1. **Analisis risiko kemanan aset informasi CV Cempaka Tulungagung berdasarkan tahap penilaian risiko pada kerangka kerja ISO 27002:2013**
   Analisis risiko dilakukan dengan menggunakan metode FMEA dan menganalisis ancaman serta kerentanan dari aset informasi yaitu perangkat lunak (*software*), perangkat keras (*hardware*), data, jaringan dan sumber daya manusia (*people*). Berdasarkan hasil evaluasi penilaian risiko, dapat diketahui bahwa CV Cempaka memiliki beberapa kemungkinan risiko yang tinggi yang dapat timbul terkait keamanan data yaitu risiko data hilang dengan nilai RPN 240, risiko kesalahan konfigurasi server dengan nilai RPN 140, risiko manipulasi data dengan nilai RPN 140, risiko kerusakan kabel LAN dengan nilai RPN 192, dan risiko password shared dengan RPN 140. Risiko tersebut muncul dikarenakan oleh berbagai penyebab seperti *human error*, kelalaian administrator dan kurangnya kontrol keamanan fisik.

Dari hasil evaluasi risiko tersebut, selanjutnya dilakukan analisis kebutuhan pengendalian risiko yang berupa sebuah pengimplementasian kontrol, praktek dan prosedur.

2. **Kontrol keamanan aset informasi yang mengacu pada kerangka kerja ISO 27002:2013.**

   Berdasarkan hasil penelitian keamanan informasi yang menyesuaikan dari hasil identifikasi dan analisa risiko pada aset informasi. Dilakukan pengendalian resiko dengan kerangka kerja ISO 27002 : 2013 yang dilakukan dengan menggunakan beberapa klausul yang telah ditentukan yaitu antara lain mengenai keamanan sumber daya manusia (Klausul 7) khususnya pada klausul 7.1.2. *Terms and conditions of employment*, 7.2.2. *Information security awareness, education & Training*, berikutnya perihal kontrol akses (Klausul 9) khususnya pada klausul 9.1.1 *Access control policy*, 9.2.3 *Management of privileged access rights*, 9.3.1 *Use of secret authentication information*, 9.4.1 *Information access restriction*, 9.4.2 *Secure log-on procedures*, 9.4.3 *Password management system*, berikutnya perihal keamanan fisik dan lingkungan (Klausul 11) khususnya pada klausul 11.2.3 *Cabling security*, 11.2.4 *Equipment maintenance*, dan yang terakhir mengeneai keamanan Operasional (Klausul 12) khususnya pada klausul 12.3.1 *Information Backup*, 12.4.1 *Event logging*, 12.4.2 *Protection of log information*.

3. **Hasil pembuatan dokumen *Standard Operating Procedure* (SOP) Keamanan Aset Informasi**

   Berdasarkan hasil analisis risiko dan rekomendasi pengendalian risiko, didapatkan usulan pembuatan 4 kebijakan yaitu 1) Kebijakan pengendalian hak akses, 2) Kebijakan keamanan informasi, 3) kebijakan pengelolaan hardware dan jaringan dan 4) kebijakan *human resource security*, kebijakan ini dibuat dengan acuan dari ISO 27002:2013 yang sudah di

tenrukan sebelumnya namun pelaksana dan peraturan yang ada pada perusahaan sehingga kebijakan hanya dapat digunakan untuk perusahan CV Cempaka.

Selain kebijakan juga didapatkan 6 prosedur yaitu 1) Prosedur Pengelolaan Hak Akses 2) Prosedur Pengelolaan *Password* 3) Prosedur *Back Up dan Restore* 4) Prosedur Perawatan *Hardware* 5) Prosedur Pengamanan Kabel 6) Prosedur Pelatihan dan Pengembangan SDM, prosedur ini dibuat dengan acuan dari ISO 27002:2013 yang sudah di tentukan sebelumnya namun mengikuti aktifitas dan pelaksana yang ada pada perusahaan sehingga kebijakan hanya dapat digunakan untuk perusahan CV Cempaka.

Dihasilkan juga beberapa instrument pendukung prosedur yatiu berupa formulir dan instruksi kerja untuk melengkapi dokumen SOP tersebut. Instruksi yang dihasilkan ada 4 terdiri dari 1) instruksi pergantian hak akses sistem informasi, 2) instruksi backup data, 3) instruksi *restore data*, 4) instrusksi *reset password*.

Sedangkan formulir yang dihasilkan ada 13. Formulir yang terdiri dari 1) Formulir Pengelolaan Hak Akses 2) Formulir Kontrak Hak Akses 3) Formulir Log Pengelolaan Hak Akses 4) Formulir Perbaikan Sistem Informasi 5) Formulir Permintaan Pergantian Password 6) Formulir Klasifikasi Data 7) Formulir Log Backup Data 8) Formulir Restore Data 9) Formulir Berita Acara Kerusakan 10) Formulir Pemeliharaan IT 11) Formulir Evaluasi Pengelolaan Perangkat IT 12) Formulir Data Pegawai 13) Formulir Evaluasi Kegiatan Pengembangan Kompetensi. Keseluruhan isi dokumen SOP dibukukan secara terpisah dari buku tugas akhir ini dan menjadi sebuah dokumen produk berjudul **Standard Operating Procedure (SOP) Keamanan Aset Informasi CV Cempaka Tulungagung**.

4. Hasil Pengujian dokumen SOP

Pengujian dokumen SOP dilakukan dengan verifikasi dan simulasi untuk memvalidasi ketepatan dokumen yang sudah sudah dibuat. Hasil dari verifikasi dari dokumen menunjukan ada beberapa bagian dari dokumen yang harus diperbaiki.

Verifikasi yang dilakukan menghasilkan beberapa perubahan dokumen antara lain :

1. **Pemisahan kebijakan pengendalian hak akses dan keamanan informasi**
   Dalam kebijakan ini dilakukan pemisahan antara kebijakan pengendalian hak akses dan kemanan informasi menjadi 2 bagian yang berbeda kebijakan pengendalian akses disendirikan dan kebijakan keamanan informasi disendirikan karena keduanya memiliki peraturan dan pedoman yang berbeda.

2. **Penambahan kebijakan Human resource security**
   Sebelum adanya kebijakan ini tidak ada kebijakan mengenai pengelolaan sdm terkait keamanan informasi sehingga perusahaan meminta adanya kebijakan yang mengatur mengenai tanggung jawab penggunaan hak akses dan pengelolaan keamanan untuk pegawai.

3. **Penghapusan proses pada prosedur pengelolaan hak akses**
   Setelah melakukan verifikasi kasie dan administrator melakukan koreksi pada proses prosedur pengelolaan hak akses pada klausa 4.3 sebelumnya ada proses peninjauan kinerja pegawai yang minta untuk di hapus saja karena untuk peninjauan kinerja perusahaan memiliki proses sendiri.

4. **Perubahan pelaksana dalam prosedur pergantian password**
   Setelah melakukan verifikasi kasie bagian personalia melakukan koreksi pada pelaksana pada prosedur pergantian password bahwa pelaksana yang menjalankan perubahan password maupun perubahan sistem bukanlah pegawai personalia melainkan lebih dikerucutkan menjadi administrator. Perubahan yang dilakukan dapat dilihat pada gambar berikut.

5. **Perubahan pelaksana dalam prosedur keamanan kabel**
   Setelah melakukan verifikasi kasie personalia melakukan koereksi pada pelaksana pada prosedur keamanan kabel bahwa untuk prosedur keamanan kabel pelaksana bukan dari pegawai divisi personalia melainkan pegawai divisi kemanan yang disetujui oleh kepala bagian personalia. Perubahan yang dilakukan dapat dilihat dari gabar berikut.

Pada umumnya perusahaan CV Cempaka sudah melakukan praktik keamanan terkait keamanan aset informasi, namun tidak ada pedoman ataupun peraturan tertulis untuk melaksanakan praktik keamanan aset informasi tersebut, sehingga kurangnya pendokumentasian mengakibatkan setiap proses perbaikan maupun pemeliharaan tidak dapat ditinjau dan tidak efektif, selain itu tidak adanya dokumen dan aturan tertulis dalam melaksanakan suatu kegiatan mengakibatkan beberapa kegiatan menjadi tidak teratur dan kerugian yang di dapatkan oleh perusahaan. Dengan dibuatkanya dokumen SOP Keamanan Aset Informasi ini diharapkan beberapa risiko yang terjadi yang mengakibatkan proses bisnis terhambat maupun kerugian bagi perusahaan dapat diminimalisir kemungkin untuk terjadinya.

7.3. Saran

Saran yang dapat peneliti sampaikan terkait dengan pengerjaan tugas akhir ini meliputi dua hal, yaitu saran untuk pihak manajemen CV Cempaka Tulungagung dan saran untuk penelitian selanjutnya.

Saran yang dapat diberikan untuk pihak manajemen CV Cempaka adalah :

1. Penulis menyarankan untuk tidak mengabaikan aset informasi yang dimiliki walaupun hanya sebagai pendukung dari bisnis utama, sehingga dapat membantu dan meningkatkan kinerja operasional perusahaan.
2. Penulis menyarankan agar dokumen SOP yang telah diuji bisa benar-benar diterapkan dengan baik. Hal pertama yang dapat dilakukan oleh pihak CV Cempaka adalah melakukan rencana penerapan dan melakukan sosialisasi pada seluruh pihak yang terkait pada seluruh pelaksanan SOP.
3. Usulan kebijakan dan prosedur dapat diimplementasikan oleh seluruh pelaksana pada CV Cempaka dan terus dikembangkan dengan menyesuaikan kondisi terkini pada perusahaan.
4. Usulan formulir yang telah dibuat dapat diimplementasikan dengan baik untuk melakukan pengelolaan keamanan aset informasi yang dimiliki perusahaan.

Saran yang dapat penulis berikan untuk penelitian selanjutnya adalah :

1. Penelitian ini sebatas pembuatan dokumen SOP hingga proses pengujian tanpa memantau pengimplementasian SOP tersebut dan pengaruhnya bagi proses bisnis organisasi. Untuk penelitian selanjutnya, dapat dilakukan pengujian dan evaluasi keefektifan dokumen SOP ini terhadap peningkatan keamanan aset informasi pada CV Cempaka Tulungagung.

2. Penelitian ini hanya mengacu pada beberapa kontrol dalam kerangka kerja ISO27002:2013 dan tidak secara keseluruhan memenuhi salah satu domain atau klausul pada kerangka kerja tesebut, karena pada dasarnya penelitian ini didasarkan pada hasil penilaian risiko untuk melakukan pengendalian risiko dengan tingkat prioritas tertinggi. Sehingga dalam penelitian selanjutnya dianjurkan untuk melengkapi objektif yang ada pada kerangka kerja sehingga kontrol dalam penyusunan SOP lebih menyeluruh dan patuh.
3. Dokumen SOP ini masih dapat terus dikembangkan dilihat dari perkembangan teknologi yang begitu pesat sehingga perusahaan dapat terus bersaing dan dapat terus menjalankan proses bisnisnya dengan baik

Halaman Sengaja Dikosongkan

DAFTAR PUSTAKA

[1] IBM, IBM survey of 224 Business Leaders, s.l: IBM, 2009.

[2] Doughty, Business Continuity Planning: Protecting Your Organization's Life, Auerbach, 2000.

[3] R. Stup, Standart Operating Procedures : Managing The Human Variables, Pennsylvania: Pennsylvania State University, 2002.

[4] ISO/IEC:27002, Information Technology - Security Techniques, Geneva, 2013.

[5] S. M. IKIT, Akutansi Penghimpun Dana Bank Syariah, Yogyakarta: CV Budi Utama, 2015.

[6] D. Ariyus, Pengantar Ilmu Kriptografi ; Teori analisis dan implementasi, Yogyakarta: CV ANDI OFFSET, 2008.

[7] H. Siahaan, Manajemen Risiko, Jakarta: PT Elex Media Comoutindo, 2007.

[8] Hughes, "Ancaman dalam IT," 2006. [Online]. Available: http://xondis.blogspot.com/2015/03/pengukuran-risiko-teknologi-informasi.html.

[9] A. Standards, "Pengertian Manajemen Risiko," 1999. [Online]. Available: http://kangnas.blogspot.com/2013/05/pengertian-manajemen-risiko-menurut-para-ahli.html.

[10] D. Stiawan, Sistem Keamanan Komputer, Jakarta: PT Elex Media Komputindo, 2005.

[11] E. Humphreys, Implementing the ISO/IEC 27002 ISMS Standart, Norwood: Artech House, 2015.

[12] B. Supradono, "MANAJEMEN RISIKO KEAMANAN INFORMASI," p. 5, 2009.

[13] P. Haapanen and A. Helminen, "Failure Mode and Effect Analysis Of Software Base Automation System," *stuk-yto-tr 190*, p. 37, 2002.

[14] M. Budihardjo, Panduan Praktis Menyusun SOP, Yogyakarta: Gadjah Mada University Press, 2014.

[15] M. H. Indonesia.Indonesia Patent 35 Tahun 2012 Tentang pedoman penyusunan SOP Administrasi Pemerintahan, 2012.

Halaman Sengaja Dikosongkan

BIODATA PENULIS

Penulis bernama lengkap Dheni Indra Rachmawan yang biasa dipanggil dengan Dheni. Penulis dilahirkan di Tulungagung pada tanggal 14 Juli 1993 dan merupakan anak kedua dari dua bersaudara. Penulis telah menempuh pendidikan formal di SDN Kampung dalem I Tulungagung, tamat SMP di SMPN 2 Tulungagung, tamat SMA di SMAN I Boyolangu Tulungagung, dan kemudian masuk perguruan tinggi negeri ITS Surabaya pada jurusan Sistem Informasi (SI), Fakultas Teknologi Informasi pada tahun 2012. Adapun pengalaman yang didapatkan penulis selama di ITS, yakni berkecimpung di organsiasi kemahasiswaan di jurusan SI selama dua tahun kepengurusan pada divisi komunitas. Penulis pernah menjalani kerja praktik di Perusahaan Kontraktor yaitu PT Ridlatama pada Divisi IT Support selama kurang lebih 3 bulan pada tahun 2015. Pengalaman yang didapatkan penulis selama bekerja praktik yaitu membangun sebuah aplikasi Pendataan Perusahaan.

Pada pengerjaan Tugas Akhir di Jurusan Sistem Informasi ITS, penulis mengambil bidang minat Manajemen Sistem Informasi dengan topik Manajemen Risiko TI, Tata Kelola TI dan Keamanan Aset Informasi , yakni mengenai pembuatan dokumen Standard Operating Procedure (SOP) Kemanan Aset Informasi yang mengacu pada kontrol kerangka kerja ISO27002:2013 pada Perusahaan Rokok CV Cempaka di Tulungagung. Untuk menghubungi penulis, dapat melalui email dheni178@gmail.com.

LAMPIRAN A
INTERVIEW DENGAN BAGIAN OPERASIONAL
CV CEMPAKA

I. Informasi Interview

Nama : Ibu Wahyu Juniarti

Jabatan : Kepala Divisi Operasional

Jenis Kelamin : Perempuan

Tanggal dan Waktu : 25 Oktober 2016, Pukul 09.00 WIB

1. Informasi Narasumber

1. Apakah peran dan tanggung jawab anda sebagai kepala divisi operasional pada CV Cempaka?

Melakukan pengelolaan aset yang dimiliki perusahaan baik mesin, peralatan kantor, peralatan IT sehingga proses bisnis pada CV Cempaka berjalan lancar

2. Apa sajakah aktivitas dan fungsi TI dalam proses bisnis CV Cempaka ?

Untuk proses bisnis sebaiknya di tanyakan kepada bagian produksi, tetapi untuk aktivitas bisnis yang terkait dengan teknologi informasi ada beberapa Aktivitas pencatatan penjualan, Laporan keuangan, penjadwalan produksi, pengaturan jam kerja karyawan, pengelolaan inventori yang mempengaruhi aktivitas produksi rokok dan banyaknya stok bahan baku yang dibutuhkan sehingga mampu memenuhi

permintaan pasar,selain itu ada juga pencatatan administrasi seperti pencatatan pegawai, pencatatan fasilitas antor, pengelolaan kas, pencatanan piutang, promosi produk dan sebagainya

2. Pertanyaan Mengenai Keamanan Aset Informasi

1. Menurut anda, apa sajakah data dan aset yang kritikal atau paling penting dalam operasional di CV Cempaka?

Diperusahaan cempaka ini semua data sebenarnya penting namun yang paling dirasa kritikal itu seperti data-data keuangan, data-data produksi Karena apabila data tersebut salah maka perusahaan bisa mengalami kerugian financial yang cukup besar. Disisi lain aset yang dirasa kritikal yaitu Server, PC, karena harus dapat digunakan selama proses binsis berjalan terus data yang dimiliki perusahaan sangat penting, selain itu wifi dan kabel jugapenting karena segala proses pada PC dan srver terhubung melalui kabel lan

2. Siapa sajakah yang memiliki hak akses terhadap aset informasi kritikal tersebut?

Yang memiliki hak akses secara khusus terhadap asset informasi tersebut adalah jajaran manajemen atau kepala bagian yang ada, selain itu beberapa karyawan yang kami berikan hak sebagai pengguna aplikasi juga.

3. Apa saja ancaman yang pernah terjadi terhadap asset informasi kritikal tersebut?

Ancaman yang pernah terjadi bisa dari beberapa faktor seperti dari lingkungan, dari manusia, atau dari infrastruktur. Kalau dari lingkungan ya bencana alam, lalu yang berasal dari SDM seperti kelalaian pegawai sehingga data yang diinputkan tidak valid. Bisa juga ancaman yang berasal dari kerusakan computer atau kesalahan konfigurasi

4. Apa saja praktek pengamanan yang telah dilakukan oleh CV Cempaka terhadap asset informasi kritikal tersebut?

Menurut saya CV Cempaka sudah melakukan beberapa usaha yang lumayan banyak untuk mengamankan asset informasi yang ada, seperti contohnya memiliki antivirus dan diupdate secara berkala, melakukan dokumentasi data dalam bentuk laporan cetak, melakukan backup server 2 minggu sekali, dan cempaka juga memiliki fire extinguisher untuk memadamkan api saat terjadi kebakaran

3. Pertanyaan mengenai pengelolaan asset informasi

1. Apakah CV Cempaka telah memiliki prosedur pengelolaan hak akses?

Sejauh ini sih cempaka memiliki beberapa prosedur tapi belum ada dokumentasinya. Prosedur seperti backup data Camera CCTV selama 1 bulan 2 kali, backup server 2 hari sekali, maintenance rutin setiap 6 bulan sekali setiap perangkat TI itu sudah ada

2. Adakah perbedaan hak akses bagi setiap pemilik hak akses?

Sudah ada, jadi tiap role masing-masing pegawai dibedakan sesuai dengan unit kerjanya

3. Apakah CV Cempaka telah memiliki prosedur dalam pencegahan (preventing) terhadap kerusakan pada asset informasi yang dimiliki saat ini?

Sudah ada, namun masih belum terdokumentasi sama seperti yang sudah saya sebutkan tadi. Mengenai bagaimana sebaiknya pengelolaan pada software maupun hardware seperti server seperti itu, namun pada ruangan server sendiri kondisinya sudah ada penataan kabel, sudah ada detektor asap dan hal hal lain yang pada umumnya ada untuk pengamanan

4. Siapa saja yang bertanggung jawab mengenai aset informasi pada perusahaan?

Ya saya, khususnya bagian personalia karena hampir semua proses baik perawatan maupun pengadaan kami yang bertanggung jawab dan menjalankan, Cuma jobdesknya di bagi ada beberapa divisi di bagian personalia ada juga administrator yang mengurus server dan aplikasi di perusahaan

4. Identifikasi Ancaman serta kebutuhan keamanan

1. Apakah dampak dari masing masing ancaman (yang disebutkan sebelumnya) tersebut terhadap berjalannya proses bisnis?

Dampaknya bagi perusahaan sendiri bisa mengganggu proses bisnis yang sedang berjalan. Contoh nya seperti data-

data yang penting itu ada kesalahan input maka jumlah produksinya juga akan salah lalu berpengaruh ke proses-proses setelahnya dan itu bisa merugikan perusahaan secara financial walaupun mungkin tidak banyak. Kalau ancaman yang bersifat fisik seperti kerusakan server atau wifi dampaknya mungkin akan sedikit mengganggu proses bisnis karena memakan waktu yang tidak sedikit untuk maintenance

2. Kebutuhan keamanan seperti apa yang dibutuhkan berdasarkan masing masing ancaman (yang disebutkan sebelumnya)?

Mungkin kebutuhan keamanan yang dibutuhkan CV Cempaka ya seperti, adanya kebijakan dan prosedur yang tertulis, keamanan ruangan server diperketat, log kegiatan harus dicatat dan hak akses setiap aplikasi harus dibatasi soalnya data sering tidak sesuai jadi itu dibutuhkan sehingga informasi yang penting sebisa mungkin tidak jatuh ke orang yang tidak bertanggung jawab.

LAMPIRAN B
PENILAIAN RISIKO PADA CV CEMPAKA

Kategori Aset	Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Potensi Penyebab Kegagalan	Occ	Proses Kontrol Saat Ini	Det	RPN	Level	Pemilik Risiko
Hardware	Server	Kerusakan Server	kerugian secara finansial dan menghambat proses bisnis	7	Gempa bumi	3	Server berada pada ruangan khusus	5	**105**	Medium	Bagian Operasional
					Banjir	3	Server berada pada ruangan khusus	5	**105**	Medium	Bagian Operasional
					Kebakaran	3	Adanya fire extinguisher untuk memadamkan api	4	**84**	Medium	Bagian Operasional
					Overheat	5	Telah dipasang pendingin pada ruang server untuk menngurangi terjadinya overheat	3	**105**	Medium	Bagian Operasional
					Kerusakan pada bangunan (bocor)	5	Dilakukan pengecekan kerusakan ruangan setiap 2 minggu sekali	3	**105**	Medium	Bagian Operasional

Kategori Aset	Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Potensi Penyebab Kegagalan	Occ	Proses Kontrol Saat Ini	Det	RPN	Level	Pemilik Risiko
					Kesalahan konfigurasi server	4	Dilakukan maintenance rutin setiap 6 bulan sekali	5	**140**	High	Bagian Operasional
		Server mati	Terhambatnya proses bisnis	7	Tidak ada aliran listrik	8	Adanya Genset dan UPS	2	**112**	Medium	Bagian Operasional
					Kerusakan pada Genset dan UPS	3	Dilakukan maintenance rutin setiap 6 bulan sekali	5	**105**	Medium	Bagian Operasional
		Server down	Terhambatnya proses bisnis	6	RAM mengalami kelebihan memori	3	Dilakukan maintenance rutin setiap 6 bulan sekali	5	**90**	Medium	Bagian Operasional
					(*Harddisk)* penuh	3	Dilakukan maintenance rutin setiap 6 bulan sekali	5	**90**	Medium	Bagian Operasional

Kategori Aset	Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Potensi Penyebab Kegagalan	Occ	Proses Kontrol Saat Ini	Det	RPN	Level	Pemilik Risiko
		Hilangnnya komponen TI	kerugian secara finansial dan menghambat proses bisnis	7	Kelalaian pegawai dalam mengunci ruang server	4	Adanya Camera CCTV yang bekerja 24 jam	3	**84**	Medium	Satuan Keamanan
	PC	PC rusak	kerugian secara finansial dan menghambat proses bisnis	7	Gempa bumi	3	Ada alat pelindung PC	3	**63**	Low	Bagian Operasional
					Banjir	3	Berada pada ruangan tinggi	4	**84**	Medium	Bagian Operasional
					Kebakaran	3	Adanya fire extinguisher untuk memadamkan api saat terjadi kebakaran	4	**84**	Medium	Bagian Operasional
					Overheat	5	Telah dipasang pendingin pada ruangan	3	**105**	Medium	Bagian Operasional

Kategori Aset	Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Potensi Penyebab Kegagalan	Occ	Proses Kontrol Saat Ini	Det	RPN	Level	Pemilik Risiko
					Kerusakan pada bangunan (bocor)	5	Dilakukan pengecekan kerusakan ruangan setiap 2 minggu sekali	3	**105**	Medium	Bagian Operasional
					Kesalahan konfigurasi PC	4	Dilakukan maintenance rutin setiap 6 bulan sekali	5	**140**	High	Bagian Operasional
		PC Tidak dapat beroperasi	Menghambat proses bisnis dan penurunan kinerja	6	Tidak ada aliran listirk	8	Adanya Genset dan UPS	2	**96**	Medium	Bagian Operasional
					Genset tidak bekerja	3	Dilakukan maintenance rutin setiap 6 bulan sekali	5	**90**	Medium	Bagian Operasional
		Hilangnnya komponen TI	kerugian secara finansial dan menghambat proses bisnis	7	Kelalaian pegawai dalam mengunci ruang server	4	Adanya Camera CCTV yang bekerja 24 jam	3	**84**	Medium	Satuan Keamanan

Kategori Aset	Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Potensi Penyebab Kegagalan	Occ	Proses Kontrol Saat Ini	Det	RPN	Level	Pemilik Risiko
Software	• Sistem Informasi Keuangan (SISKA) • Sistem Informasi Administrasi (SIADMIN) • Sistem Informasi Pendataan dan penjadwalan (SIMDATA) • Sistem Informasi Pemasaran (SIMPEM)	Sistem tidak dapat diakses	kerugian secara finansial Terhambatnya proses bisnis	7	Server Down	4	perawatan maintenance pada server 6 bulan sekali	4	**112**	Medium	Bagian Operasional
		Aplikasi diakses oleh pihak yang tidak berwenang	kerugian secara finansial Terhambatnya proses bisnis	7	Pembobolan sistem	4	Membedakan role atau hak akses untuk masing masing pegawai sesuai dengan unit kerja dan fungsinya	3	**84**	Medium	Bagian Operasional
							Data hanya bisa dimasukkan, diganti atau dihapus oleh database administrator saja	3	**84**	Medium	Bagian Operasional
					Username dan password diketahui oleh pengguna lain	5	Adanya pergantian password secara berkala	4	**140**	High	Bagian Operasional
		Sistem tidak berjalan normal (error)	kerugian secara finansial dan menghambat proses bisnis	7	Serangan virus	7	Adanya antivirus dan diupdate secara berkala	2	**98**	Medium	Bagian Operasional

Kategori Aset	Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Potensi Penyebab Kegagalan	Occ	Proses Kontrol Saat Ini	Det	RPN	Level	Pemilik Risiko
					Kesalahan Konfigurasi pada Sistem	5	Dilakukan maintenance rutin setiap 6 bulan sekali setiap perangkat TI	2	**70**	Low	Bagian Operasional
					Bug pada Software	6	Dilakukan maintenance rutin setiap 6 bulan sekali setiap perangkat TI	2	**84**	Medium	Bagian Operasional
Data	Seluruh data yang dimiliki pada setiap bagian dan divisi pada perusahaan CV Cempaka yang mempengaruhi proses bisnis	Manipulasi data	menyebabkan kerugian dan menghambat proses bisnis	7	Adanya hacker	4	Adanya update patch dan firewall secara berkala	3	**84**	Medium	Bagian Operasional
					Username password diketahui orang lain	5	Adanya pergantian password secara berkala	4	**140**	High	Bagian Operasional
		Data Hilang	menyebabkan kerugian dan sangat menghambat	8	Kelalaian administrator	6	Telah dilakukan backup server 2 hari sekali	5	**240**	Very High	Bagian Operasional

Kategori Aset	Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Potensi Penyebab Kegagalan	Occ	Proses Kontrol Saat Ini	Det	RPN	Level	Pemilik Risiko
			proses bisnis		Rusaknya media penyimpanan	3	Telah dilakukan backup server 2 hari sekali	5	**120**	High	Bagian Operasional
					Virus Bug	5	Adanya antivirus dan diupdate secara berkala	2	**80**	Medium	Bagian Operasional
		Pencurian data	menyebabkan kerugian dan sangat menghambat proses bisnis	8	Adanya hacker	3	Adanya update patch dan firewall secara berkala	3	**72**	Low	Bagian Operasional
		Data tidak dapat diakses	penurunan kinerja sehingga proses bisnis terhambat	6	Server mati	5	Adanya genset dan ups	3	**90**	Medium	Bagian Operasional
					Server Down	5	Dilakukan maintenance rutin setiap 6 bulan sekali setiap perangkat TI	3	**90**	Medium	Bagian Operasional

Kategori Aset	Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Potensi Penyebab Kegagalan	Occ	Proses Kontrol Saat Ini	Det	RPN	Level	Pemilik Risiko
Jaringan	Wifi	Gangguan koneksi	penurunan kinerja sehingga proses bisnis terhambat	6	Kesalahan Konfigurasi wifi	4	Dilakukan maintenance Wifi setiap 2 minggu sekali	4	**96**	Medium	Bagian Operasional
		Internet mati	penurunan kinerja sehingga proses bisnis terhambat	6	Listrik mati	6	Adanya genset dan ups	3	**108**	Medium	Bagian Operasional
	Kabel	Kerusakan kabel LAN	penurunan kinerja sehingga proses bisnis terhambat	6	Adanya hewan pengerat	8	Dilakukan maintenance rutin setiap 6 bulan sekali setiap perangkat TI	4	**192**	High	Bagian Operasional
					Kurangnya kontrol pengamanan kabel	6	Dilakukan maintenance rutin setiap 6 bulan sekali setiap perangkat TI	4	**144**	High	Bagian Operasional
	Router	Router mengalami gangguan	penurunan kinerja sehingga proses bisnis terhambat	6	Kesalahan Konfigurasi router	4	Dilakukan maintenance rutin setiap 6 bulan sekali setiap perangkat TI	4	**96**	Medium	Bagian Operasional

Kategori Aset	Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Potensi Penyebab Kegagalan	Occ	Proses Kontrol Saat Ini	Det	RPN	Level	Pemilik Risiko
		Hilangnnya komponen TI	penurunan kinerja sehingga proses bisnis terhambat	6	Kelalaian pegawai	4	Adanya Camera CCTV yang bekerja 24 jam	3	**72**	Low	Satuan Keamanan
	Switch	Router mengalami gangguan	penurunan kinerja sehingga proses bisnis terhambat	6	Kesalahan Konfigurasi router	4	Dilakukan maintenance rutin setiap 6 bulan sekali setiap perangkat TI	4	**96**	Medium	Bagian Operasional
		Hilangnnya komponen TI	penurunan kinerja sehingga proses bisnis terhambat	6	Kelalaian pegawai	4	Adanya Camera CCTV yang bekerja 24 jam	3	**72**	Low	Satuan Keamanan
SDM	Karyawan	Penyalahguaan data organisasi	penurunan kinerja dan sedikit kerugian	6	Penurunan Loyalitas Pegawai	3	Membedakan role atau hak akses untuk masing masing pegawai sesuai dengan unit kerja dan fungsinya	3	**54**	Low	Semua bagian pada perusahaan
		Pelanggaran hak akses	penurunan kinerja dan sedikit kerugian	6	Penurunan Loyalitas Pegawai	3	Membedakan role atau hak akses untuk masing masing pegawai sesuai dengan unit kerja dan	3	**54**	Low	Semua bagian pada perusahaan

Kategori Aset	Aset	Potensi Mode Kegagalan	Potensi Dampak Kegagalan	Sev	Potensi Penyebab Kegagalan	Occ	Proses Kontrol Saat Ini	Det	RPN	Level	Pemilik Risiko
							fungsinya				
		Data tidak sesuai	penurunan kinerja dan sedikit kerugian	6	Kesalahan input data	5	Adanya log setiap aktivitas dalam sistem informasi yang dimiliki	4	**120**	High	Semua bagian pada perusahaan
		Password shared	menyebabkan kerugian dan menghambat proses bisnis	7	Kelalaian pegawai	5	Membedakan role atau hak akses untuk masing masing pegawai sesuai dengan unit kerja dan fungsinya	4	**140**	High	Semua bagian pada perusahaan
	Satuan Keamanan	Tidak melakukan monitoring keamanan	Kerugian secara finansial	5	Penurunan Loyalitas Pegawai	4	Adanya Camera CCTV yang bekerja 24 jam	4	**80**	Medium	Bagian Operasional

LAMPIRAN C
PEMETAAN DAN JUSTIFIKASI KONTROL

Kategori Aset Informasi Kritis	Aset Informasi Kritis	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi
Hardware	Server	Kerusakan Hardware	Kesalahan konfigurasi	***11.2.4 Equipment maintenance***	Kontrol yang memastikan pemeliharaan alat atau aset yang dimiliki kegunaanya untuk memastikan alat dapat digunakan selama proses bisnis berjalan
	PC				
Data	Data keuangan, Data Produksi, Data penjualan, Data Kepegawaian	Data Hilang	Kelalaian Administrator	***9.3.1 Use of secret authentication information***	Kontrol yang memastikan administrator atau pengguna memiliki hak akses harus mengikuti praktek-praktek dalam menggunakan informasi penting
				12.4.3 Administrator & Operator Logs	Kontrol untuk memastikan aktivitas sistem administrator dan sistem operasi selalu tercatat dalam sebuah *log* dan selalu terkendali. Sehingga apabila adanya kesalahan yang diakibatkan *human error* maka dapat dilakukan audit trail untuk melacak kesalahan yang terjadi.
				7.2.2 Information security awareness, education and training	

Kategori Aset Informasi Kritis	Aset Informasi Kritis	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi
				9.1.1 Access control policy	Kontrol yang memastikan suatu penetapan sebuah kebijakan akses harus ditinjau dan sesuai dengan persyaratan keamanan informasi
		Data Hilang	Rusaknya media penyimpanan	***12.3.1 Information Backup***	Kontrol yang memastikan adanya salinan cadangan informasi yang diambil dan diuji secara teratur
				11.2.4 Equipment maintenance	Kontrol yang memastikan pemeliharaan alat atau aset yang dimiliki kegunaanya untuk memastikan alat dapat digunakan selama proses bisnis berjalan
		Manipulasi data	Username password diketahui orang lain	***9.2.3 Management of privileged access rights***	Kontrol yang memastikan pembatasan alokasi dan penggunaan hak akses
				9.4.2 Secure log-on procedures	Kontrol yang memastikan prosedur akses pada sistem aplikasi kegunaanya adalah menghindari akses oleh orang luar (tidak memiliki hak akses)
				9.4.3 Password management system	Kontrol yang memastikan sistem manajemen password interaktif dan berkualitas
				9.1.1 Access control policy	Kontrol yang memastikan suatu penetapan sebuah kebijakan akses harus ditinjau dan sesuai dengan persyaratan keamanan informasi
Software	Seluruh sistem aplikasi yang	Aplikasi diakses oleh pihak yang	Username dan password	***9.4.1 Information access restriction***	Kontrol yang memastikan pembatasan akses ke fungsi dalam sistem aplikasi yang harus sesuai dengan kebijakan dari kontrol akses

Kategori Aset Informasi Kritis	Aset Informasi Kritis	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi
	dimiliki perusahaan	tidak berwenang	diketahui oleh pengguna lain	***9.4.2 Secure log-on procedures***	Kontrol yang memastikan prosedur akses pada sistem aplikasi kegunaanya adalah menghindari akses oleh orang luar (tidak memiliki hak akses)
				9.4.3 Password management system	Kontrol yang memastikan sistem manajemen password interaktif dan berkualitas
				9.1.1 Access control policy	Kontrol yang memastikan suatu penetapan sebuah kebijakan akses harus ditinjau dan sesuai dengan persyaratan keamanan informasi
Jaringan	Kabel	Kerusakan kabel LAN	Kurangnya kontrol pengamanan kabel	***11.2.3 Cabling security***	Kontrol yang memastikan adanya proses cabling yang mampu melindungi dari kerusakan atau gangguan
SDM	Karyawan yang memiliki hak akses	sharing password	Kelalaian karyawan yang memiliki hak akses	***7.1.2 Terms and conditions of employment***	Kontrol yang memastikan perjanjian kontrak karyawan menyatakan bertanggung jawab atas keamanan dari informasi yang telah diberikan padanya gunanya untuk menghindari kelalaian dan ketidaksengajaan karyawan (human error) menyebarkan informasi penting
				7.2.2 Information security awareness, education and training	Kontrol yang memastikan seluruh karyawan sudah diberikan pendidikan dan pelatihan dalam melaksanakan kebijakan dan prosedur sesuai dengan fungsi dan tanggungjawab yang mereka terima

Kategori Aset Informasi Kritis	Aset Informasi Kritis	Potensi Mode Kegagalan	Potensi Penyebab Kegagalan	Kontrol ISO27002:2013	Justifikasi
				9.1.1 Access control policy	Kontrol yang memastikan suatu penetapan sebuah kebijakan akses harus ditinjau dan sesuai dengan persyaratan keamanan informasi
		Data tidak sesuai (tidak valid)	Kesalahan input data	***12.4.1 Event logging***	Kontrol yang memastikan pencatatan aktivitas pengguna pada sistem aplikasi, untuk menghindari terjadinya kesalahan maupun kejadian pengubahan data yang tidak seharusnya dilakukan oleh pengguna
				12.4.2 Protection of log information	Kontrol yang memastikan log informasi terlindungi dari gangguan maupun akses yang tidak sah

LAMPIRAN D
PEMETAAN HASIL REKOMENDASI PENGENDALIAN RISIKO

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
7.1.2 **Terms and conditions of employment**	Perjanjian kontrak dengan karyawan yang menyatakan bahwa mereka bertanggung jawab atas keamanan informasi perusahaan	• Semua karyawan yang akan diberi akses informasi rahasia harus menandatangani perjanjian *non-disclosure* sebelum diberi akses pada pengolahan informasi • Adanya Tanggung jawab hukum untuk hak hak dari karyawan, misalnya hukum hak cipta atau undang undang perlindungan data • Adanya Tanggung jawab untuk klasifikasi informasi dan manajemen aset perusahaan terkait dengan informasi, fasilitas pengolahan informasi dan layanan informasi yang ditangani oleh karyawan • Adanya tanggung jawab karyawan untuk penanganan informasi yang diterima dari perusahaan lain atau pihak eksternal • Adanya Tindakan yang harus	• Perusahaan memberikan tanggung jawab hak akses yang akan di kelola untuk masing masing pegawai sesuai dengan unit kerja dan fungsinya • Perusahaan memberlakukan punishment terhadap karyawan yang melanggar peraturan hak akses seperti pengurangan gaji dan pergantian hak akses	• Membuat kontrak perjanjian untuk semua karyawan yang akan diberikan tanggung jawab dan hak akses pada pengolahan informasi • Adanya tanggung jawab secara hukum untuk karyawan yang menandatangani perjanjian perihal perlindungan data • Adanya Tanggung jawab untuk klasifikasi informasi dan manajemen aset perusahaan terkait dengan informasi, fasilitas pengolahan informasi dan layanan informasi yang ditangani oleh karyawan • Adanya tanggung jawab karyawan untuk penanganan informasi yang diterima dari perusahaan lain atau pihak eksternal • Adanya Tindakan yang harus diambil jika karyawan atau mengabaikan persyaratan keamanan organisasi

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
		diambil jika karyawan atau mengabaikan persyaratan keamanan organisasi		

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
7.2.2 Information security awareness, education and training	Semua karyawan harus memiliki kesadaran, edukasi, dan pelatihan terkait kebijakan dan prosedur perusahaan sesuai dengan fungsi kerja mereka	• Program *awareness* (peringatan kesadaran) terkait keamanan informasi membuat para karyawan menyadari akan tanggung jawab mereka untuk keamanan informasi perusahaan dan supaya mereka tidak mengabaikannya • Program *awareness* (peringatan kesadaran) terkait keamanan informasi harus ditetapkan sesuai dengan kebijakan dan prosedur perusahaan. • Program *awareness* (peringatan kesadaran) harus direncanakan dengan mempertimbangkan peran karyawan dalam organisasi. Kegiatan ini harus dijadwalkan dari waktu ke waktu secara teratur sehingga kegiatan ini mampu diikuti oleh karyawan yang baru. Program ini juga harus diperbarui secara berkala sehingga tetap sejalan dengan kebijakan dan prosedur organisasi, dan juga dapat diperbarui dari insiden keamanan informasi yang pernah terjadi.	• Adanya pemberitahuan dan peringatan setiap karyawan saat diberikan tanggung jawab hak akses maupun tugas agar mengerjakan dengan teliti dan benar. • Adanya pemberitahuan dan peringatan setiap karyawan mengenai betapa pentingnya data yang dikerjakan maupun yang berada di bawah tanggung jawabnya. • Adanya training setiap adanya software baru maupun update software. • Adanya training untuk karyawan magang ataupun karyawan baru.	• Membuat Program kesadaran seperti training dan seminar secara terjadwal untuk setiap karyawan yang menggunakan aset informasi baik karyawan baru, karyawan lama, dan karyawan sementara atau magang • Membuat poster mengenai kesadaran keamanan informasi pada setiap bagian perusahaan yang menggunakan aset informasi • Membuat perencanaan dan konten program kesadaran yang sesuai dengan kebutuhan dengan mempertimbangkan peran dari karyawan • Membuat reward dan punishment untuk karyawan yang menjalankan program kesadaran dengan sesuai

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
		• Program awareness harus dilakukan sesuai kebutuhan keamanan informasi organisasi. Awarness training dapat menggunakan media pengiriman yang berbeda, pembelajaran jarak jauh, berbasis web, self-paced dan lain-lain.		
9.1.1 Access control policy	Kebijakan untuk mengontrol hak akses harus ditetapkan, didokumentasikan, dan ditinjau berdasarkan bisnis dan kebutuhan keamanan informasi perusahaan	Pengguna dan penyedia layanan harus diberikan pernyataan yang jelas dari kebijakan control akses dimana harus memperhatikan hal-hal berikut : • Kebutuhan keamanan dari aplikasi • Kebijakan untuk penyebaran informasi dan otorisasi • konsitensi antara hak akses dan kebijakan klasifikasi informasi dari sistem dan jaringan; • peraturan yang relevan dan kewajiban kontraktual mengenai pembatasan akses ke data atau layanan • pengelolaan hak akses dalam lingkungan terdistribusi dan jaringan yang mengakui semua jenis koneksi yang tersedia	• Perusahaan memiliki catatan log setiap aktivitas dalam sistem informasi yang dimiliki misalkan log login siapa saja yang akses aplikasi, apa saja data yang baru dimasukan, di ubah, maupun di hapus • Perusahaan membedakan role atau hak akses untuk masing masing pegawai sesuai dengan unit kerja dan fungsinya o Setiap system memiliki user level. Direktur, kepala bagian, dan staff memiliki user interface system yang berbeda • Perusahaan memberlakukan peraturan tidak dapat menginstal aplikasi lain dalam PC selain admin PC yang ada di perusahaan	• Membuat aturan yang jelas dan tertulis mengenai hak akses terhadap aset sistem informasi yang di dalamnya ada antara lain : o Kebutuhan keamanan dari aplikasi o Peraturan kebijakan untuk penyebaran informasi o Peraturan relevan dan kewajiban secara tertulis atau kontaktual mengenai pembatasan hak akses o Peraturan pengelolaan hak akses, pengahapusan serta roles yang di berikan o Pengarsipan catatan semua kegiatan mengenai pengguanaan dan pengelolaan

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
		• pemisahan peran kontrol akses • Requirement untuk otorisasi permintaan akses • Requirement untuk mereview hak akses • Penghapusan hak akses • Pengarsipan catatan semua peristiwa penting mengenai penggunaan dan pengelolaan identitas pengguna dan informasi otentikasi rahasia • Roles terkait privileged akses	hanya berisikan aplikasi-aplikasi yang menunjang kinerja perusahaan • Data perusahaan hanya bisa dimasukkan, diganti atau dihapus oleh database administrator saja. Sehingga para staff tidak dapat memodifikasi data yang sifatnya rahasia	• Membuat peraturan mengenai pembatasan akses data maupun sistem aplikasi yang dimiliki, o Pemisahan peran kontrol akses o Roles terkait privileged akses o Requirement otorisasi hak akses o Requirement mereview hak akses
9.2.3 Management of privileged access rights	Alokasi dan penggunakan hak akses privileges harus dibatasi dan di kontrol	• Hak akses privilaged yang terkait dengan setiap system atau proses (ex. sistem manajemen database dan masing-masing aplikasi dan pengguna operasi kepada siapa mereka harus dialokasikan harus diidentifikasi) • Hak akses privileged harus dialokasikan kepada pengguna berdasarkan kebutuhan yang digunakan dan sejalan dengan kebijakan kontrol akses • Proses otorisasi dan catatan hak privileged yang dialokasikan harus didokumentasikan • Kebutuhan untuk hak akses privileged harus didefinisikan	• Perusahaan telah membedakan role atau hak akses untuk masing masing pegawai sesuai dengan unit kerja dan fungsinya o Setiap system memiliki user level. Direktur, kepala bagian, dan staff memiliki user interface system yang berbeda • Data perusahaan hanya bisa dimasukkan, diganti atau dihapus oleh database administrator saja. Sehingga para staff tidak dapat memodifikasi data yang sifatnya rahasia • Adanya prosedur yang telah berjalan untuk melakukan	• Adanya Membedakan role atau hak akses untuk masing masing pegawai sesuai dengan unit kerja dan fungsinya • Membuat aturan dan prosedur tertulis mengenai penggunaan hak akses privileges o Proses otorisasi dan catatan hak privileged yang dialokasikan harus didokumentasikan o Kebutuhan untuk hak akses privileged harus didefinisikan o Hak akses privileged harus diserahkan kepada pengguna ID yang berbeda dari yang digunakan untuk kegiatan bisnis dengan yang biasa o Peninjauan pengguna atau

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
		• Hak akses privileged harus diserahkan kepada pengguna ID yang berbeda dari yang digunakan untuk kegiatan bisnis biasa • kompetensi pengguna dengan hak akses privilaged harus ditinjau secara teratur untuk memverifikasi apakah mereka sejalan dengan tugas mereka • prosedur tertentu harus ditetapkan dan dimaintenance untuk menghindari penggunaan yang tidak sah dari ID pengguna • untuk ID administrasi pengguna generik, kerahasiaan informasi otentikasi rahasia harus dijaga saat bersama (ex. Sering mengubah password dan menghapus sesegera mungkin ketika pengguna hak privileged meninggalkan atau mengubah pekerjaan)	pergantian *password* ○ Setiap 3 bulan sekali, system secara otomatis meminta administrator untuk melakukan perubahan password	karyawan yang diberikan hak akses secara teratur unruk memverifikasi apakah sudah sesuai dengan tugas yang di berikan ○ Adanya otentikasi rahasia dari ID administrasi maupun pemilik hak akses seperti Sering mengubah password dan log out sesegera mungkin ketika pengguna hak privileged meninggalkan atau mengubah pekerjaan
9.3.1 Use of secret authentication information	Pengguna harus diminta untuk mengikuti praktek-praktek organisasi dalam penggunaan informasi otentikasi rahasia	• Menyimpan otentikasi informasi rahasia, memastikan bahwa tidak dibocorkan kepada pihak lain • Menjaga kerahasiaan catatan otentikasi informasi • Mengubah otentikasi informasi rahasia setiap kali	• Perusahaan telah membedakan role atau hak akses untuk masing masing pegawai sesuai dengan unit kerja dan fungsinya ○ Setiap system memiliki user level. Direktur, kepala bagian, dan staff memiliki	• Adanya penyimpanan otentikasi rahasia khusus untuk memastikan bahwa dokumen tidak di bocorkan kepada pihak lain • Mengubah otentikasi informasi rahasia setiap terjadinya indikasi masalah • Diharuskan menggunakan password

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
		ada indikasi masalah yang mungkin terjadi • Ketika password digunakan sebagai otentikasi informasi rahasia, pilih password yang berkualitas dengan panjang minimum 8 dan bebas karakter yang identik (semua abjad atau semua angka) • Tidak berbagi otentikasi informasi rahasia dengan individu lain • memastikan perlindungan yang tepat dari password ketika password yang digunakan sebagai informasi otentikasi rahasia otomatis log-on disimpan • tidak menggunakan informasi otentikasi yang sama untuk tujuan bisnis dan non-bisnis	user interface system yang berbeda • Adanya prosedur yang telah berjalan untuk melakukan pergantian *password* ○ Setiap 3 bulan sekali, system secara otomatis meminta administrator untuk melakukan perubahan password • Adanya pemberitahuan dan peringatan setiap karyawan mengenai betapa pentingnya data yang dikerjakan maupun yang berada di bawah tanggung jawabnya	yang berkualitas dengan panjang minimum 8 dan alfanumeric • Tidak membagikan otentikasi rahasia dengan individu lain • Adanya pemastian password yang di gunakan adalah strong dan keamanan penyimpanan dari password aman • Tidak menggunakan informasi otentikasi yang sama untuk tujuan bisnis atau non-bisnis
9.4.1 Information access restriction	Akses untuk fungsi informasi dan system aplikasi harus dibatasi sesuai dengan kebijakan kontrol akses	• menyediakan menu untuk control akses ke fungsi system aplikasi • pengendalian data yang dapat diakses oleh pengguna tertentu • mengontrol hak akses pengguna, (Ex. read, create, delete and excute) • mengontrol hak akses dari aplikasi lain; • membatasi informasi yang	• Perusahaan telah membedakan role atau hak akses untuk masing masing pegawai sesuai dengan unit kerja dan fungsinya ○ Setiap system memiliki user level. Direktur, kepala bagian, dan staff memiliki user interface system yang berbeda • Data perusahaan hanya bisa	• Adanya menu khusus pada sistem aplikasi untuk mengubah kontrol akses yang ada • Adanya pengendalian data yang dapat diakses oleh pengguna tertentu • Mengontrol penyesuaian penggunaan hak akses oleh pengguna (Ex. read, create, delete and excute) Pada sistem aplikasi • Membedakan hak akses dari aplikasi lain • Adanya kontrol akses fisik atau

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
		terkandung dalam output • menyediakan kontrol akses fisik atau logika untuk isolasi aplikasi sensitif, aplikasi data, atau sistem	dimasukkan, diganti atau dihapus oleh database administrator saja ○ Sehingga para staff tidak dapat memodifikasi data yang sifatnya confidential • Perusahaan memberlakukan peraturan tidak dapat menginstal aplikasi lain dalam PC selain admin ○ PC yang ada di perusahaan hanya berisikan aplikasi-aplikasi yang menunjang kinerja perusahaan	logika untuk isolasi aplikasi sensitif, aplikasi data, atau sistem (Ex. Camera CCTV, pengggembokan ruangan, dll)
9.4.2 Secure log-on procedures	Akses ke system dan aplikasi harus dikontrol dengan prosedur keamanan log-on	• Tidak menampilkan system atau aplikasi pengenal hingga proses log-on terselesaikan • Menampilkan pemberitahuan umum yang memperingatkan bahwa computer hanya bisa diakses oleh pengguna yang berwenang • Tidak memberikan bantuan pesan selama proses log-on • Memvalidasi log-on hanya pada proses input data terselesaikan. Jika ada kesalahan, system tidak harus menunjukkan bagaimana data yang benar • Melindungi terhadap upaya	• Adanya autentikasi untuk login pengguna ○ Setiap akan menggunakan system yang ada pada perusahaan, pengguna harus memasukkan username dan password yang sesuai terlebih dahulu • Data perusahaan hanya bisa dimasukkan, diganti atau dihapus oleh database administrator saja. Sehingga para staff tidak dapat memodifikasi data yang sifatnya rahasia • Perusahaan memiliki catatan log setiap aktivitas dalam sistem informasi yang dimiliki	• Adanya proses log-on pada setiap sistem aplikasi • Adanya notifikasi yang memperingatkan bahwa komputer ataupun sistem aplikasi hanya dapat diakses oleh pengguna yang berwenang • Tidak adanya hint atau bantuan dalam proses log on sehingga hanya dapat diakses oleh pihak yang berwenang saja • Tidak adanya pemberitahuan penulisan input data yang benar selama proses log-on • Adanya perlindungan terhadap brute force • Meningkatkan keamanan jika terjadi potensi pelanggaran yang mulai

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
		brute force log-on • Percobaan log unsuccess dan log success • Meningkatkan keamanan jika terdapat potensi pelanggaran yang terdeteksi • Menampilkan informasi berikut pada proses log-on selesai : o tanggal dan waktu dari sukses log-on sebelumnya; o rincian dari setiap berhasil log-on upaya sejak sukses log-on terakhir; • tidak menampilkan password yang dimasukkan • tidak mengirimkan password dalam bentuk teks melalui jaringan • mengakhiri sesi aktif setelah periode tertentu tidak aktif, terutama di lokasi berisiko tinggi seperti area public • membatasi koneksi untuk memberikan keamanan tambahan untuk aplikasi berisiko tinggi	misalkan log login siapa saja yang akses aplikasi, apa saja data yang baru dimasukan, di ubah, maupun di hapus	terdeteksi • Menampilkan informasi proses log-on antara lain : o Tanggal dan waktu sukse log on o Log-on berhasil hingga log-on terakhir • Tidak menampilkan password yang di inputkan • Tidak bisa mencopas password dalam bentuk teks • Membatasi sesi log-on dalam periode tertentu jika sistem aplikasi sudah tidak digunakan • Membatasi koneksi internet untuk memberikan keamanan tambahan pada aplikasi maupun komputer yang di gunakan
9.4.3 Password management system	sistem manajemen password harus interaktif dan harus memastikan kualitas password	• Menerapkan penggunaan user ID dan password untuk menjaga akuntabilitas • memungkinkan pengguna untuk memilih dan mengubah password mereka sendiri dan	• Data perusahaan hanya bisa dimasukkan, diganti atau dihapus oleh database administrator saja. Sehingga para staff tidak dapat memodifikasi data yang	• Adanya prosedur untuk melakukan pergantian *password.* o Setiap 2 bulan sekali, system secara otomatis meminta administrator untuk melakukan perubahan password

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
		menerapkan prosedur konfirmasi untuk kesalahan input; • menegakkan pilihan password berkualitas • memaksa pengguna untuk mengubah password mereka pada pertama log-on • menegakkan perubahan password secara teratur dan sesuai kebutuhan • mempertahankan catatan password yang digunakan sebelumnya dan mencegah penggunaan kembali • tidak menampilkan password di layar ketika sedang masuk • menyimpan dan mengirimkan password dalam bentuk enkripsi	sifatnya rahasia • Adanya prosedur yang telah berjalan untuk melakukan pergantian *password.* o Setiap 3 bulan sekali, system secara otomatis meminta administrator untuk melakukan perubahan password	• memungkinkan pengguna untuk memilih dan mengubah password mereka sendiri dan menerapkan prosedur konfirmasi untuk kesalahan input; • Mewajibkan staff menggunakan password yang berkualitas o Panjang minimal 8 karakter o Wajib menggunakan huruf Kapital, Angka dan symbol • tidak menampilkan password di layar ketika sedang masuk • menyimpan dan mengirimkan password dalam bentuk enkripsi • Mencegah penggunaan password yang sama dengan sebelumnya saat pergantian password
11.2.3 Cabling security	Listrik dan kabel telekomunikasi yang membawa data atau mendukung layanan informasi harus dilindungi dari intersepsi, gangguan atau kerusakan	• Listrik dan telekomunikasi sebaiknya ditanam dibawah tanah dan diberi perlindungan alternative yang memadai • kabel listrik harus dipisahkan dari kabel komunikasi untuk mencegah gangguan • untuk sistem sensitif atau kritis, kontrol yang dipertimbangkan seperti : o instalasi saluran lapis baja dan mengunci kotak pada inspeksi	• Adanya pengaturan kabel dengan melakukan pelabelan untuk masing masing fungsi kabel o Adanya label di setiap ujung kabel o Adanya Pembedaan warna kabel • Perusahaan memastikan peletakan kabel yang teratur dan tidak berantakan	• Membuat perlindungan alternative yang memadai seperti penanaman kabel bawah tanah • Pemisahan kabel telekomunikasi dengan kabel listrik untuk menghindari terjadinya konsleting • Pembuatan pelindung kabel agar tidak ada hewan pengerat maupun akses dari orang yang tidak berwenang • Melakukan pemeriksaan fisik secara berkala untuk menghindari perangkat tidak sah yang terhubung

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
		○ menggunakan perisai elektromagnetik untuk melindungi kabel ○ pemeriksaan fisik untuk perangkat yang tidak sah yang melekat pada kabel ○ Mengontrol akses ke patch panel dan kabel room.		• Mengontrol akses pada panel patch dan kabel pada ruangan secara rutin
11.2.4 Equipment maintenance	Perlengkapan harus dipelihara dengan benar untuk memastikan integritas dan ketersediaan secara terus menerus	• Equipment harus dipelihara sesuai dengan spesifikasi dan interval servis yang direkomendasikan pemasok; • Hanya personil yang berwenang yang boleh melakukan pemeliharaan dan perbaikan • catatan harus disimpan dari semua aktual kesalahan, dan semua pemeliharaan preventif dan korektif • Kontrol yang tepat harus dilaksanakan bila maintenance equipment telah dijadwalkan. Dengan mempertimbangkan apakah maintenance ini dilakukan oleh pihak eksternal, bila perlu maka informasi rahasia harus dibersihkan terlebih dahulu dari equipment • Semua kebutuhan maintenance yang dikenakan asuransi harus dipenuhi • Sebelum meletakkan	• Perusahaan melakukan maintenance rutin setiap 6 bulan sekali pada perangkat TI ○ Setiap Staff dapat melaporkan setiap terjadinya kerusakan pada perangkat TI yang di gunakan pada Bagian Operasional ○ Bagian Operasional Mencatat setiap kejadian kerusakan dan melaporkan pada teknisi perusahaan maupun pihak eksternal ○ Teknisi perusahaan maupun eksternal diwajibkan mencatat setiap komponen yang di ganti maupun setiap merubah konfigurasi pada perangkat TI ○ Bagian Operasional memastikan perangkat TI sudah dapat digunakan dengan baik dan memastikan tidak adanya	• Pemeliharaan equipment harus sesuai dengan spefikasi dan interval servis yang telah di rekomendasikan • Adanya hak akses khusus untuk melakukan pemeliharaan dan perbaikan pada equipment perusahaan • Membuat form catatan pada semua kendala dan pemeliharaan prefentive maupun korektif • Adanya penyimpanan catatan pelaporan kerusakan dan pemeliharaan secara preventif maupun korektif • Adanya penjadwalan yang tepat atau sesuai dengan rekomendasi dari pihak pemasok equipment • Membuat kontrol yg sesuai dengan kebutuhan untuk merekomendasi sebelum melakukan maintenance dengan pihak eksternal • Memastikan equipment dengan benar equipment dapat digunakan kembali dalam operasional setelah dilakukan maintenance baik

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
		equipment kembali kedalam operasi setelah dimaintenance, harus dipastikan bahwa peralatan tersebut berfungsi dan tidak rusak	data yang dicuri • Adanya penguncian pada ruang server sehingga tidak dapat sembarang orang bisa masuk • Perusahaan melakukan maintenance Wifi setiap 2 minggu sekali • Adanya anggota satuan keamanan yang berkeliling selama 24 jam penuh • Adanya Camera CCTV yang bekerja 24 jam yang memantau perlengkapan • Perusahaan melakukan pengecekan kerusakan ruangan setiap 1 bulan sekali	maintenance pihak internal dan eksternal
12.3.1 Information Backup	Backup cadangan dari informasi penting, software dan system image harus diambil dan diuji secara berkala sesuai dengan kebijkana yang disepakati.	• Dokumentasi yang akurat dan lengkap dari Salinan backup dan prosedur dokumentasi harus dibuat • Frekuensi backup harus mencerminkan kebutuhan bisnis organisasi • Backup harus disimpan di lokasi terpencil, pada jarak yang cukup untuk menghindari bencana pada lokasi utama • Informasi backup harus diberi tingkat perlindungan fisik dan lingkungan yang konsisten • Media backup harus diuji secara teratur untuk memastikan bahwa mereka	• Perusahaan melakukan backup data Camera CCTV selama 1 bulan 2 kali • Adanya dokumentasi data dalam bentuk laporan cetak pada setiap sistem yang dimiliki o Penyimpanan laporan cetak dilakukan dengan terstruktur • Perusahaan melakukan backup server 2 hari sekali	• Membuat prosedur atau aturan backup yang lengkap dan sesuai kebutuhan o Dilakukan dokumentasi setiap melakukan backup o Frekuensi melakukan backup harus sesuai dengan kepntingan dan kebutuhan sebuah data bagi perusahaan o Backup data harus disimpan pada tempat yang aman dari terjadinya bencana o Lokasi backup harus di beri pengamanan fisik dan lingkungan yang aman o Melakukan pengujian lokasi backup secara berkala

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
		dapat diandalkan • Backup harus dilindungi dengan cara enkripsi		○ Backup data harus dilindungi dengan enkripsi
12.4.1 Event logging	Event log merekam aktivitas pengguna, exceptions, kesalahan dan kejadian keamanan informasi harus diproduksi, disimpan secara berkala	Merekam aktivitas berikut : • User ID • System Activities • tanggal, waktu dan rincian peristiwa penting, misalnya log-on dan log-off • identitas perangkat atau lokasi jika mungkin dan sistem pengenal • Dokumentasi upaya success dan reject akses system • perubahan konfigurasi system • Penggunaan hak akses privileged • penggunaan sistem utilitas dan aplikasi • file diakses dan jenis akses • alamat jaringan dan protocol • Meningkatkan alarm pada control akses • aktivasi dan de-aktivasi sistem perlindungan, seperti sistem anti-virus • Dokumentasi transaksi yang dilakukan oleh pengguna pada aplikasi	• Perusahaan memiliki catatan log setiap aktivitas dalam sistem informasi yang dimiliki misalkan log login siapa saja yang akses aplikasi, apa saja data yang baru dimasukan, di ubah, maupun di hapus • Adanya dokumentasi data dalam bentuk laporan cetak pada setiap sistem yang dimiliki ○ Penyimpanan laporan cetak dilakukan dengan terstruktur	• Adanya log kegiatan pada setiap sistem aplikasi maupun kegiatan yang dilakukan • Pada dokumen log harus terekam beberapa aktivitas berikut : ○ Adanya User ID ○ Sistem apa yang sedang beraktivitas ○ tanggal, waktu dan rincian peristiwa penting, misalnya log-on dan log-off ○ Dokumentasi upaya success dan reject akses system ○ perubahan konfigurasi system ○ Penggunaan hak akses privileged ○ penggunaan sistem utilitas dan aplikasi ○ file diakses dan jenis akses ○ aktivasi dan de-aktivasi sistem

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
				perlindungan, seperti sistem anti-virus o Dokumentasi transaksi yang dilakukan oleh pengguna pada aplikasi
12.4.2 Protection of log information	Fasilitas logging dan log informasi harus dilindungi terhadap gangguan dan akses yang tidak sah	• Memiliki dokumentasi terhadap perubahan jenis pesan • Melingungi file log yang sedang diedit atau dihapus • Menghindari kapasitas penyimpanan media File log yang sudah berlebih, sehingga gagal untuk melakukan penyimpanan	• Perusahaan memiliki catatan log setiap aktivitas dalam sistem informasi yang dimiliki misalkan log login siapa saja yang akses aplikasi, apa saja data yang baru dimasukan, di ubah, maupun di hapus • Adanya dokumentasi data dalam bentuk laporan cetak pada setiap sistem yang dimiliki • Data perusahaan hanya bisa dimasukkan, diganti atau dihapus oleh database administrator saja. Sehingga para staff tidak dapat memodifikasi data yang sifatnya rahasia	• Adanya perlindungan khusus pada file log yang akan diedit maupun di hapus • Adanya pengecekan secara berkala pada kapasitas database untuk penyimpanan media file logging yang sudah berlebih, untuk mengurangi terjadinya kegagalan dalam pencatatan log atau kegiatan dalam setiap aktivitas yang dilakukan
12.4.3 Administrator & Operator Logs	Kegiatan login system administrator & system operator harus dilindungi secara berkala	• Melindungi dan meninjau log untuk menjaga akuntabilitas pengguna akses privilaged	• Adanya autentikasi untuk login pengguna • Perusahaan telah membedakan role atau hak akses untuk masing masing pegawai sesuai dengan unit kerja dan	• Adanya pembedaan hak akses untuk administrator khusus dalam melakukan perlindungan dan meninjau data log untuk menjaga akuntabilitas dan penggunaan akses privilaged

Kontrol ISO 27002:2013	*Control Objective*	Petunjuk pelaksanaan ISO 27002:2013	Pelaksanaan keamanan yang dilakukan perusahaan	Hasil Rekomendasi
			fungsinya o Setiap system memiliki user level. Direktur, kepala bagian, dan staff memiliki user interface system yang berbeda	

LAMPIRAN E
HASIL VERIFIKASI DAN VALIDASI

Hasil verifikasi SOP

Tabel dibawah ini berisikan penjelasan dari hasil verifikasi dokumen produk SOP Keamanan Aset Informasi CV Cempaka yang dilakukan dengan Kasie personalia dan administrator. Verifikasi dokumen produk SOP dilakukan dengan teknik wawancara secara langsung.

Tanggal Wawancara : 5 Januari 2017
Nama Narasuber I : Ida Wahyu Yuniarti, S.H.
Peran Narasumber I : Kasie Personalia CV Cempaka
Nama Narasuber II : Budi Hartanto, S.Kom.
Peran Narasumber II : Kasie Personalia CV Cempaka

Pertanyaan	Jawaban
Menurut Ibu dan bapak apakah kebijakan yang di rekomendasikan telah sesuai dengan kondisi pada CV Cempaka? Atau adakah kebijakan yang kurang sesuai dan perlu diubah?	Narasumber I : Karena secara spesifik belum ada kebijakan khusus mengenai Teknologi Informasi dan Komunikasi di CV Cempaka, saya rasa kebijakan sudah cukup tapi saya rasa untuk kebijakan pengendalian hak akses dan keamanan informasi dipisah saja karena biar lebih spesifik mengenai hak akses dan kemanan informasi, Narasumber II : Selaim yang di sampaikan ibu ida tolong di tambahkan lagi mengenai

	kebijakan human resource security soalnya disini kurang ada peraturan maupun pedoman untuk SDM itu sendiri terkait dalam keamanan informasi
Menurut Bapak dan Ibu apakah ada istilah yang kurang tepat yang digunakan dalam dokumen SOP ini?	Secara keseluruhan sudah tepat.
Apakah menurut Bapak dan Ibu ada aktivitas dalam SOP yang perlu diperbaiki atau ditambahkan?	Narasumber I : Ada beberapa koreksi untuk prosedur di pengelolaan hak akses untuk peninjauan kinerja pegawai saya rasa di hapus saja karen untuk peninjauan kinerja kita sudah ada prosedur sendiri untuk melakukan penilaian kinerja. Narasumber II : untuk prosedur perawatan hardware pada poin 1.5 sepertinya untuk melakukan perbaikan tidak perlu melakukan pengelolaan hak akses lagi karena untuk vendor kita sudah ada perjanjian tersendiri Narasumber II : pelaksana pada prosedur pergantian password di kerucutkan langsung saja pegawai divisi operasional digantikan dengan

	administrator saya baca dari flownya itu flow untuk bagian saya dan tim Narasumber I : Untuk prosedur keamanan kabel yang bertanggung jawab bagian personalia tapi untuk yang melakukan pelaksanaan dari divisi keamanan jadi di ganti saja pelaksana untuk itu
Terakait dengan formulir dalam mendukung setiap prosedur yang dihasilkan apakah ada koreksi?	Secara keseluruhan sudah lengkap dan cukup, mungkin lebih lanjut kesesuiannya bisa dilihat pada saat simulasi prosedurnya saja.

Hasil Validasi Pengujian SOP

Berikut ini adalah lampiran yang berisi hasil skenario pengujian SOP beserta formulir-formulir yang diisi saat pengujian prosedur berlangsung.

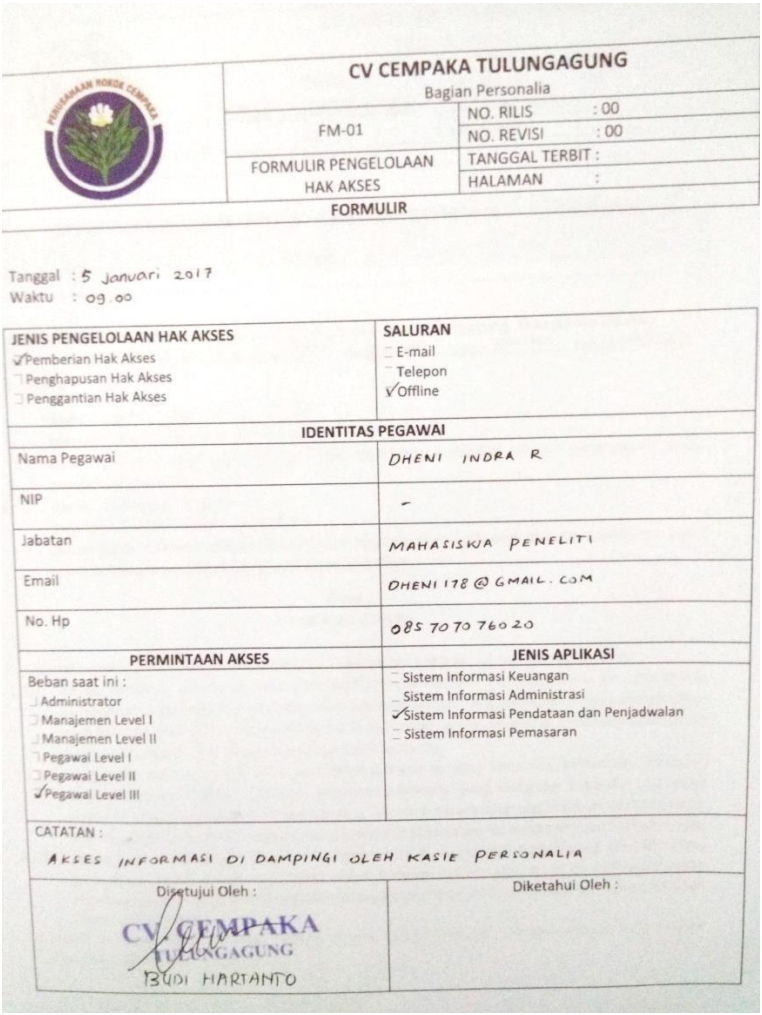
1. **Pengujian prosedur pengelolaan hak akses**
   Tanggal Pengujian : 5 Januari 2017
   Pelaksana : Budi Hartanto, Administrator
   Dheni Indra, Mahasiswa Peneliti
   Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

Tabel E.1 Tabel validasi pemberian hak akses

No	Aktivitas	Keterangan
Proses pemberian hak akses		
1	Mempersiapkan formulir pengelolaan hak akses, formulir log hak akses, dan formulir perjanjian hak akes	Proses persiapan untuk melakukan prosedur pengelolaan hak akses
2	Calon pengguna sistem mengisi formulir pengelolaan hak akses	Disini calon pengguna mengisikan form untuk penambahan hak akses baru pada sistem aplikasi perusahaan
3	Administrator melakukan persetujuan dan menyiapkan hak akses baru untuk pengguna	Dalam tahap ini administrator melakukan persetujuan kepada kepala bagian personalia dan menyiapkan hak akses baru
4	Setelah persetujuan dilakukan administrator memberikan form perjanjian penggunaan hak akses	Form perjanjian penggunaan hak akses ini bertujuan untuk memberikan peraturan2 terkait informasi yang boleh digunakan dan disimpan oleh calon pengguna dimana tertera beberapa pasal di dalamnya dan ada punisment jika pengguna sistem melanggar

5	Pengguna membaca dan mengisi formulir perjanjian dan menandatanganinya	Adminisrator menandatangani sehingga kontrak perjanjian sudah di verifikasi
6	Setelah itu administrtor mencatat pada log hak akses menambahkan hak akses baru	Pencatatan di perlukan untuk data pengelolaan hak akses
7	Administrator mengabarkan hak akses baru sudah dapat di gunakan oleh pengguna dan hak akses pn dapat di gunakan	Pada proses ini penguuna sudah dapat menggunakan hak akses yang dimilikinya pada sistem yang sudah disepakati.

Berikut merupakan gambar validasi pemberian hak akses yang di lakukan :



CV CEMPAKA TULUNGAGUNG
Bagian Personalia

FM-01	NO. RILIS : 00
	NO. REVISI : 00
FORMULIR PENGELOLAAN HAK AKSES	TANGGAL TERBIT :
	HALAMAN :

FORMULIR

Tanggal : 5 Januari 2017
Waktu : 09.00

JENIS PENGELOLAAN HAK AKSES	SALURAN
✓Pemberian Hak Akses Penghapusan Hak Akses Penggantian Hak Akses	E-mail Telepon ✓Offline

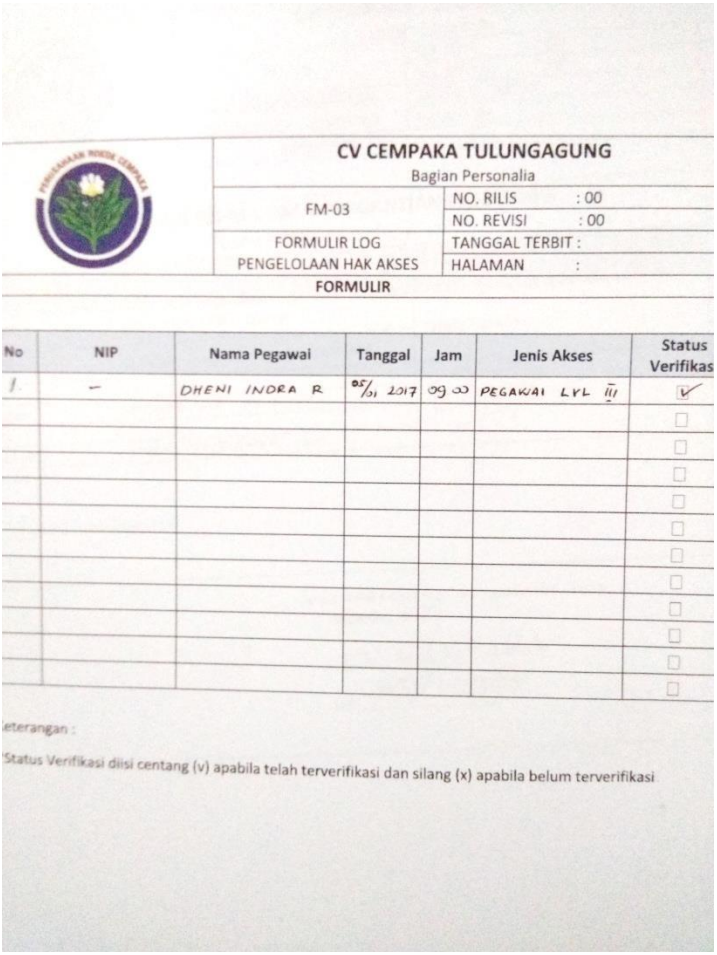
IDENTITAS PEGAWAI	
Nama Pegawai	DHENI INDRA R
NIP	-
Jabatan	MAHASISWA PENELITI
Email	DHENI178@GMAIL.COM
No. Hp	085 7070 760 20

PERMINTAAN AKSES	JENIS APLIKASI
Beban saat ini : Administrator Manajemen Level I Manajemen Level II Pegawai Level I Pegawai Level II ✓Pegawai Level III	Sistem Informasi Keuangan Sistem Informasi Administrasi ✓Sistem Informasi Pendataan dan Penjadwalan Sistem Informasi Pemasaran

CATATAN :
AKSES INFORMASI DI DAMPINGI OLEH KASIE PERSONALIA

Disetujui Oleh :	Diketahui Oleh :
CV CEMPAKA TULUNGAGUNG BUDI HARTANTO	

Gambar E.1 Formulir pengelolaan hak akses



CV CEMPAKA TULUNGAGUNG

Bagian Personalia

FM-03	NO. RILIS	: 00
	NO. REVISI	: 00
FORMULIR LOG PENGELOLAAN HAK AKSES	TANGGAL TERBIT	:
	HALAMAN	:

FORMULIR

No	NIP	Nama Pegawai	Tanggal	Jam	Jenis Akses	Status Verifikasi
1	-	DHENI INDRA R	05/01, 2017	09 00	PEGAWAI LVL III	☑
						☐
						☐
						☐
						☐
						☐
						☐
						☐
						☐
						☐
						☐
						☐

Keterangan :

Status Verifikasi diisi centang (v) apabila telah terverifikasi dan silang (x) apabila belum terverifikasi

Gambar E.2 Log pengelolaan hak akses

CV CEMPAKA TULUNGAGUNG		
Bagian Personalia		
FM-02	NO. RILIS	: 00
	NO. REVISI	: 00
FORMULIR KONTRAK HAK AKSES	TANGGAL TERBIT	:
	HALAMAN	:
FORMULIR		

PERJANJIAN KERAHASIAAN ATAS HAK AKSES CV CEMPAKA TULUNGAGUNG

Nomor :

Perjanjian Kerahasiaan atas Hak Akses yang ada di CV Cempaka Tulungagung, selanjutnya disebut Perjanjian Kerahasiaan, dibuat pada hari ini, *Kamis*, tanggal *05*, bulan *Januari*, tahun *2017* oleh dan antara:

I. Nama : *BUDI HARTANTO, S.KOM*
Jabatan : *PERSONALIA (ADMINISTRATOR)*
Dalam hal ini disebut sebagai PIHAK PERTAMA yang bertindak sebagai penanggung jawab pemberian hak akses.

II. Nama : *DYENI INDRA R.*
Jabatan : *MAHASISWA PENELITI*
Dalam hal ini disebut sebagai PIHAK KEDUA yang bertanggung jawab atas diberikannya hak akses dan menyetujui peraturan-peraturan sebagai berikut :

Pasal 1
Informasi Rahasia

1.1. Untuk kepentingan Perjanjian ini, definisi dari "**Informasi Rahasia**" adalah sebagai berikut:
1.1.1. Setiap informasi mengenai atau yang berhubungan dengan Pemberi, anak perusahaannya, pelanggannya, dan kegiatan usahanya serta operasionalnya, yang disampaikan atau diungkapkan oleh Pemberi kepada Penerima baik secara lisan, tertulis, grafik, magnetik, elektronik atau dalam bentuk lain, baik secara langsung maupun tidak langsung;
1.1.2. Setiap informasi mengenai atau yang berhubungan dengan Transaksi, ketentuan Transaksi, perjanjian yang mengatur Transaksi, ketentuan perjanjian yang mengatur Transaksi dan setiap dokumen yang terkait dengan Transaksi yang diberikan secara langsung ataupun tidak langsung, oleh Pemberi kepada Penerima sehubungan dengan atau dalam hal terkait dengan Transaksi; atau
1.1.3. Segala komunikasi antara Para Pihak, baik secara lisan maupun tulisan yang diketahui atau semestinya diketahui oleh Para Pihak untuk menjadi rahasia atau menjadi milik perusahaan secara alami, dan yang dibuat didalam serangkaian diskusi atau pekerjaan lain yang dilakukan diantara Para Pihak.
1.2. Informasi Rahasia tidak termasuk "Informasi yang Tidak Dilindungi" sebagaimana dijelaskan dalam Pasal 2 Perjanjian ini.

Pasal 2
Informasi yang Tidak Dilindungi

Untuk kepentingan Perjanjian ini, yang dimaksud dengan "**Informasi yang Tidak Dilindungi**" adalah sebagai berikut:

2.1. Informasi yang pada saat penyampaiannya atau penggunkapannya, sudah berada pada kepemilikan yang sah dari Penerima atau tersedia pada Penerima dari sumber lain yang tidak memiliki kewajiban untuk tidak menyampaikan atau mengungkapkannya; atau
2.2. Informasi yang merupakan, atau setiap saat setelah ini menjadi, tersedia untuk umum selain dari pelanggaran Perjanjian ini oleh Penerima.

Pasal 3
Lingkup Perjanjian

3.1. Penerima setuju untuk setiap saat:
3.1.1. Tidak akan mengungkapkan Informasi Rahasia kepada pihak manapun;
3.1.2. Mengambil seluruh tindakan yang diperlukan untuk melindungi kerahasiaan dari Informasi Rahasia; dan
3.1.3. Menghindari pengungkapan atau penyalahgunaan dari Informasi Rahasia,

Pasal 4
Ketentuan Penalti

4.1. Penalti berbentuk ganti rugi sebesar Rp 5.000.000,- akan dikenakan terhadap Karyawan dalam situasi dimana Karyawan melakukan pelanggaran terhadap isi dari perjanjian ini.
4.2. Apabila dalam hal pembebanan ganti rugi sebesar Rp 5.000.000,- tersebut dianggap tidak sepadan oleh lembaga pengadilan yang berwenang, maka keputusan dari lembaga pengadilan yang berwenang tersebut lah yang akan dipakai.
4.3. Akan dilakukan penghapusan hak akses secara sepihak oleh perusahaan CV Cempaka

Demikian Perjanjian Kerahasiaan atas hak akses ini dibuat dan ditandatangani oleh PIHAK PERTAMA dan PIHAK KEDUA di tempat dan pada tanggal tersebut di atas, dalam rangkap 2 (dua) asli bermaterai cukup, masing-masing pihak telah menandatangani Perjanjian ini melalui wakil yang ditunjuk.

Pihak Pertama
CV. CEMPAKA
TULUNGAGUNG
BUDI HARTANTO

Pihak Kedua
DYENI INDRA R

Gambar E.3 Perjanjian hak akses

2. Pengujian prosedur pengelolaan password

Tanggal Pengujian : 5 Januari 2017
Pelaksana : Budi Hartanto, Administrator
Dheni Indra, Mahasiswa Peneliti

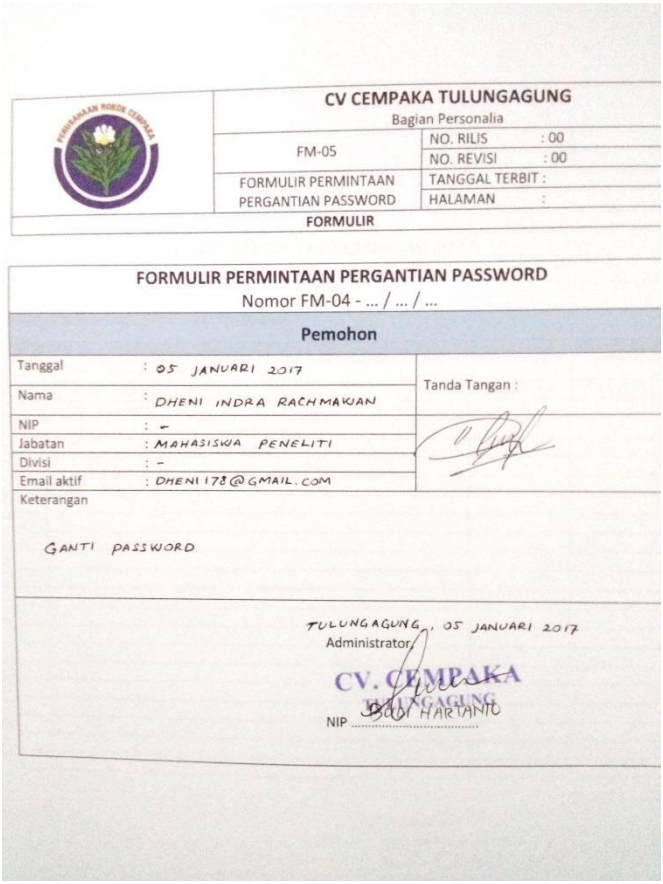
Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

Tabel E.2 tabel proses pergantian password

No	Aktivitas	Keterangan
Proses permintaan pergantian password		
1	Mempersiapkan formulir permintaan pergantian password, formulir log hak akses	Proses persiapan untuk melakukan prosedur pengelolaan password
2	Pengguna sistem mengisi formulir permintaan pergantian password	Dilakukan dengan baik
3	Administrator melakukan persetujuan dan menyiapkan pembukaan sistem untuk pergantian password pada akun milik pengguna	Dilakukan dengan baik
4	Administrator memberi kabar pada pengguna jika sudah dapat menggantikan passwordnya sistem ini akan menutup sendiri jika password tidak segera di ganti oleh pengguna	Dilakukan dengan baik
5	Pengguna mengganti password sesuai ketentuan jika tidak sesuai dengan ketentuan maka akan muncul alert pada sistem	Dilakukan dengan baik

6	Setelh pergantian password selesai administrator melakukan pencatatan pada log pengelolaan hak akses	Dilakukan dengan baik

Berikut merupakan gambar validasi formulir permintaan pergantian password yang di lakukan :



CV CEMPAKA TULUNGAGUNG
Bagian Personalia

FM-05	NO. RILIS	: 00
	NO. REVISI	: 00
FORMULIR PERMINTAAN PERGANTIAN PASSWORD	TANGGAL TERBIT	:
	HALAMAN	:

FORMULIR

FORMULIR PERMINTAAN PERGANTIAN PASSWORD
Nomor FM-04 - ... / ... / ...

Pemohon

Tanggal	: 05 JANUARI 2017	Tanda Tangan :
Nama	: DHENI INDRA RACHMAWAN	
NIP	: -	
Jabatan	: MAHASISWA PENELITI	
Divisi	: -	
Email aktif	: DHENI178@GMAIL.COM	

Keterangan

GANTI PASSWORD

TULUNGAGUNG, 05 JANUARI 2017
Administrator,

CV. CEMPAKA TULUNGAGUNG
BUDI HARTANTO

NIP .....

Gambar E.4 formulir permintaan pergantian password

3. Pengujian prosedur backup dan restore

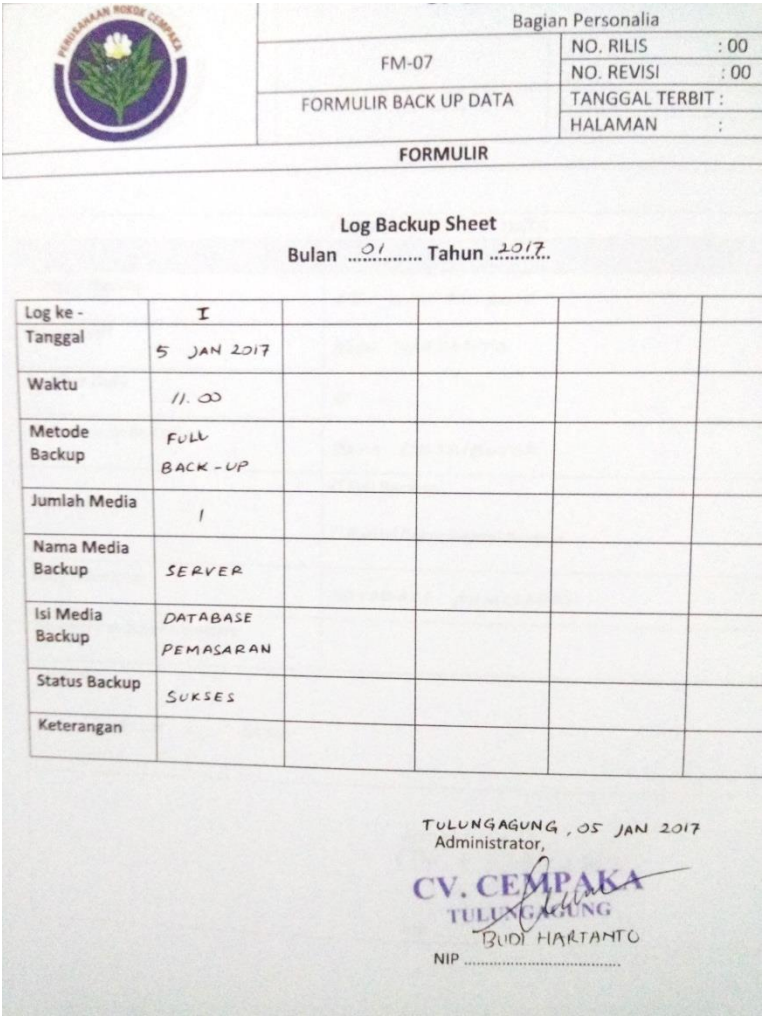
Tanggal Pengujian : 5 Januari 2017
Pelaksana : Budi Hartanto, Administrator
Ida Wahyu Yuniarti, Kasie personalia

Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

No	Aktivitas	Keterangan
Proses Uji Coba Back up Data secara berkala		
1	Melakukan uji back up data	Uji coba back up dilakukan dengan baik dengan menggunakan aplikasi Putty dan data yang di backup adalah database pemasaran pada media back up dbpemasaran
2	Melakukan set up persiapan uji coba back up data	Dilakukan dengan baik pada aplikasi Putty dan penjadwalan back up pada aplikasi crowntab sesuai dengan Intruksi kerja Back up dan Inturksi kerja Restore
3	Melakukan uji coba back up data pada media back up yang telah disiapkan	Dilakukan pada media back up dbpemasaranuji

Proses Restore data		
1	Menentukan database yang akan dilakukan restore	Dilakukan dengan baik yaitu pada database pemasaran pada media back up dbpemasaran
2	Menentukan jadwal pelaksanaan restore data	Dilakukan dengan baik pada aplikasi crowntab
3	Melakukan proses restore data	Proses dalam sistem berjalan dengan baik
4	Menganalisa hasil restore data **Successful** Adminitrator mendokumentasikan pelaksanaan retore data dengan mengisi Formulir Restore Data **Failed** Administrator melakukan kembali proses restore data (kembali ke poin 3)	Hasil restore data ***successful***, sehingga lanjut pada poin 5
4a	Mendokumentasikan pelaksanaan retore data dengan mengisi Formulir Restore Data	Dilakukan dengan baik pada formulir restore data

Berikut merupakan gambar validasi formulir restore dan backup yang di lakukan :



	Bagian Personalia	
FM-07	NO. RILIS	: 00
	NO. REVISI	: 00
FORMULIR BACK UP DATA	TANGGAL TERBIT	:
	HALAMAN	:

FORMULIR

Log Backup Sheet

Bulan 01 Tahun 2017

Log ke -	I				
Tanggal	5 JAN 2017				
Waktu	11.00				
Metode Backup	FULL BACK-UP				
Jumlah Media	1				
Nama Media Backup	SERVER				
Isi Media Backup	DATABASE PEMASARAN				
Status Backup	SUKSES				
Keterangan					

TULUNGAGUNG, 05 JAN 2017

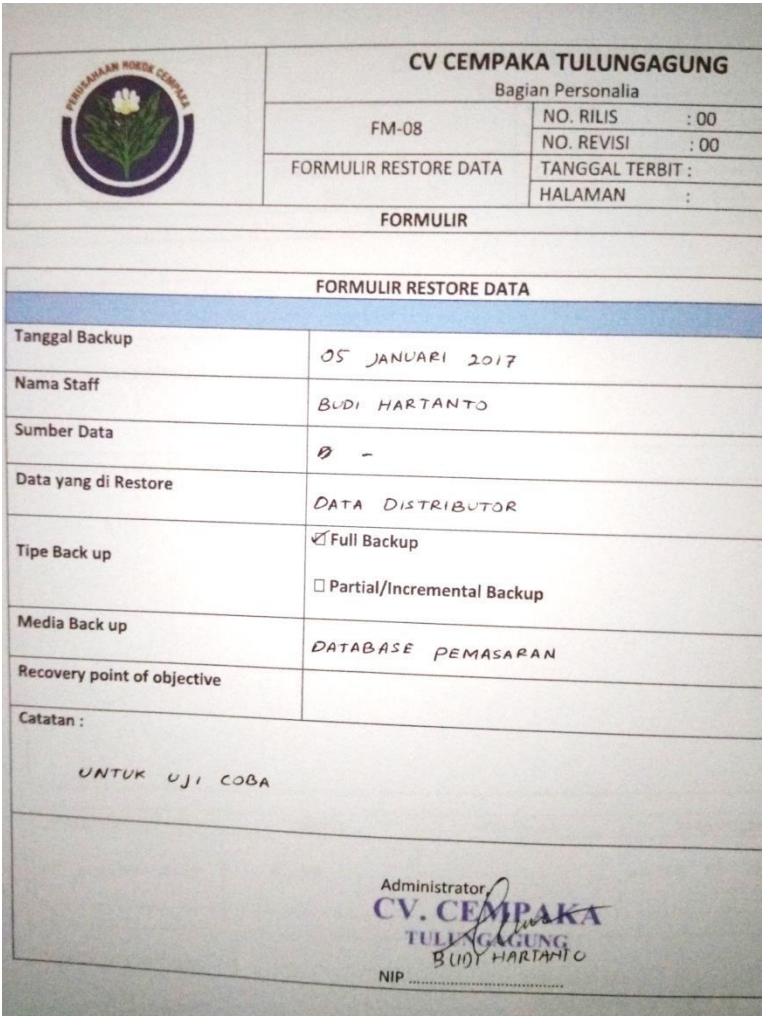
Administrator,

CV. CEMPAKA TULUNGAGUNG

BUDI HARTANTO

NIP .....

Gambar E.5 Formulir Log backup



CV CEMPAKA TULUNGAGUNG Bagian Personalia		
FM-08	NO. RILIS	: 00
	NO. REVISI	: 00
FORMULIR RESTORE DATA	TANGGAL TERBIT	:
	HALAMAN	:

FORMULIR

FORMULIR RESTORE DATA

Tanggal Backup	05 JANUARI 2017
Nama Staff	BUDI HARTANTO
Sumber Data	Ø -
Data yang di Restore	DATA DISTRIBUTOR
Tipe Back up	☑ Full Backup ☐ Partial/Incremental Backup
Media Back up	DATABASE PEMASARAN
Recovery point of objective	

Catatan :

UNTUK UJI COBA

Administrator,
CV. CEMPAKA
TULUNGAGUNG
BUDY HARTANTO
NIP .....

Gambar E.6 Formulir restore data

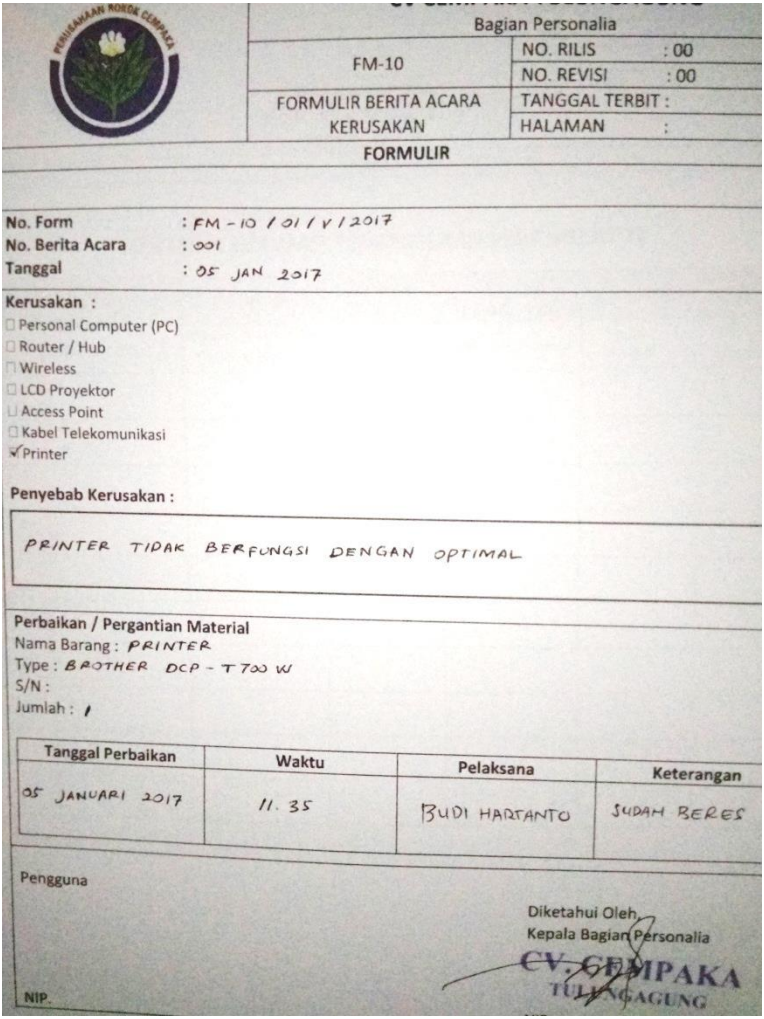
4. Pengujian prosedur perawatan hardware

Tanggal Pengujian : 5 Januari 2017
Pelaksana : Budi Hartanto, Administrator
Wahyu, pegawai bagian produksi

Hasil simulasi pengujian secara rinci dijelaskan dalam tabel berikut :

No	Aktivitas	Keterangan
Proses pemeliharaan parsial		
1	Mempersiapkan formulir berita acara kerusakan, formulir pemeliharaan, dan formulir log pengelolaan perangkat TI	Proses persiapan untuk melakukan prosedur pengelolaan password
2	Mas wahyu melaporkan kerusakan printer pada divisi personalia	Dilakukan dengan baik
3	Mas budi membuat berita acara kerusakan	Dilakukan dengan baik
4	Setelah itu pegawai melapor pada kabag personalia untuk persetujuan melakukan maintenance	Dilakukan dengan baik
5	Pegawai divisi personalia melakukan maintenance	Dilakukan dengan baik
6	Melakukan pencatatan pemeliharaan hardware	Dilakukan dengan baik
7	Pegawai divisi personalia memastikan hardware dapat digunakan dengan baik kembali	

Berikut merupakan gambar validasi formulir restore dan backup yang di lakukan :



Bagian Personalia

FM-10	NO. RILIS	: 00
	NO. REVISI	: 00
FORMULIR BERITA ACARA KERUSAKAN	TANGGAL TERBIT	:
	HALAMAN	:

FORMULIR

No. Form : FM-10 / 01 / V / 2017
No. Berita Acara : 001
Tanggal : 05 JAN 2017

Kerusakan :
- ☐ Personal Computer (PC)
- ☐ Router / Hub
- ☐ Wireless
- ☐ LCD Proyektor
- ☐ Access Point
- ☐ Kabel Telekomunikasi
- ☑ Printer

Penyebab Kerusakan :

PRINTER TIDAK BERFUNGSI DENGAN OPTIMAL

Perbaikan / Pergantian Material
Nama Barang : PRINTER
Type : BROTHER DCP - T700 W
S/N :
Jumlah : 1

Tanggal Perbaikan	Waktu	Pelaksana	Keterangan
05 JANUARI 2017	11.35	BUDI HARTANTO	SUDAH BERES

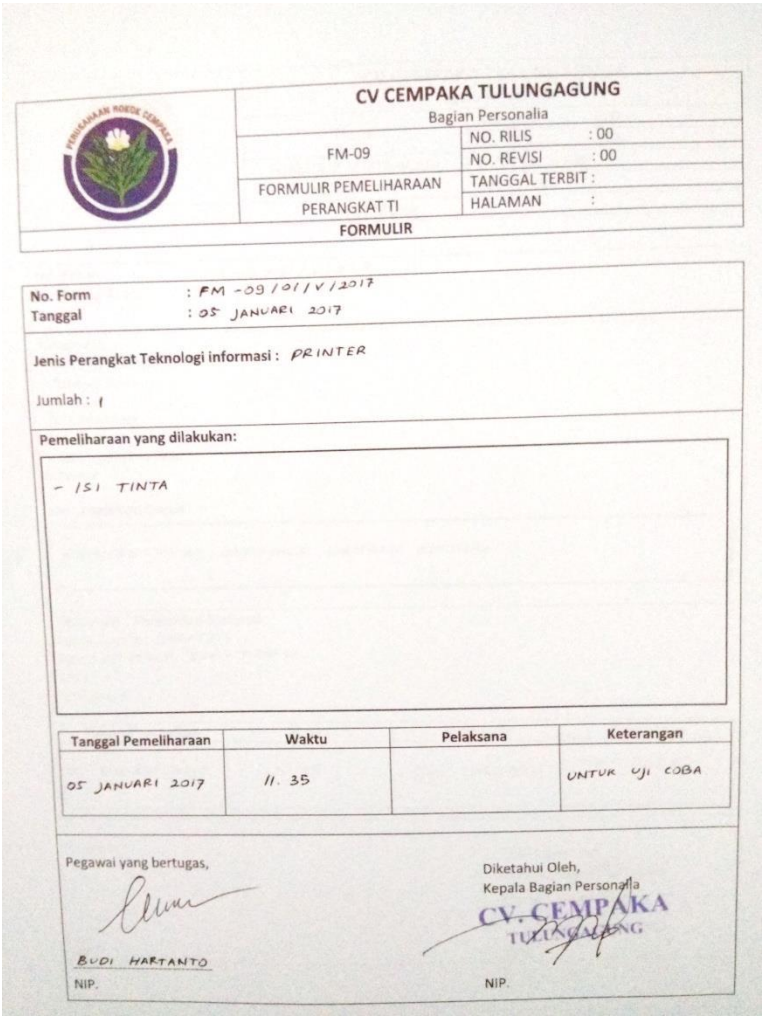
Pengguna

Diketahui Oleh,
Kepala Bagian Personalia

CV. GEMPAKA
TULUNGAGUNG

NIP.

Gambar E.7 formulir berita acara kerusakan



CV CEMPAKA TULUNGAGUNG Bagian Personalia		
FM-09	NO. RILIS	: 00
	NO. REVISI	: 00
FORMULIR PEMELIHARAAN PERANGKAT TI	TANGGAL TERBIT	:
	HALAMAN	:

FORMULIR

No. Form : FM -09 / 01 / V / 2017
Tanggal : 05 JANUARI 2017

Jenis Perangkat Teknologi informasi : PRINTER

Jumlah : 1

Pemeliharaan yang dilakukan:

- ISI TINTA

Tanggal Pemeliharaan	Waktu	Pelaksana	Keterangan
05 JANUARI 2017	11. 35		UNTUK UJI COBA

Pegawai yang bertugas,

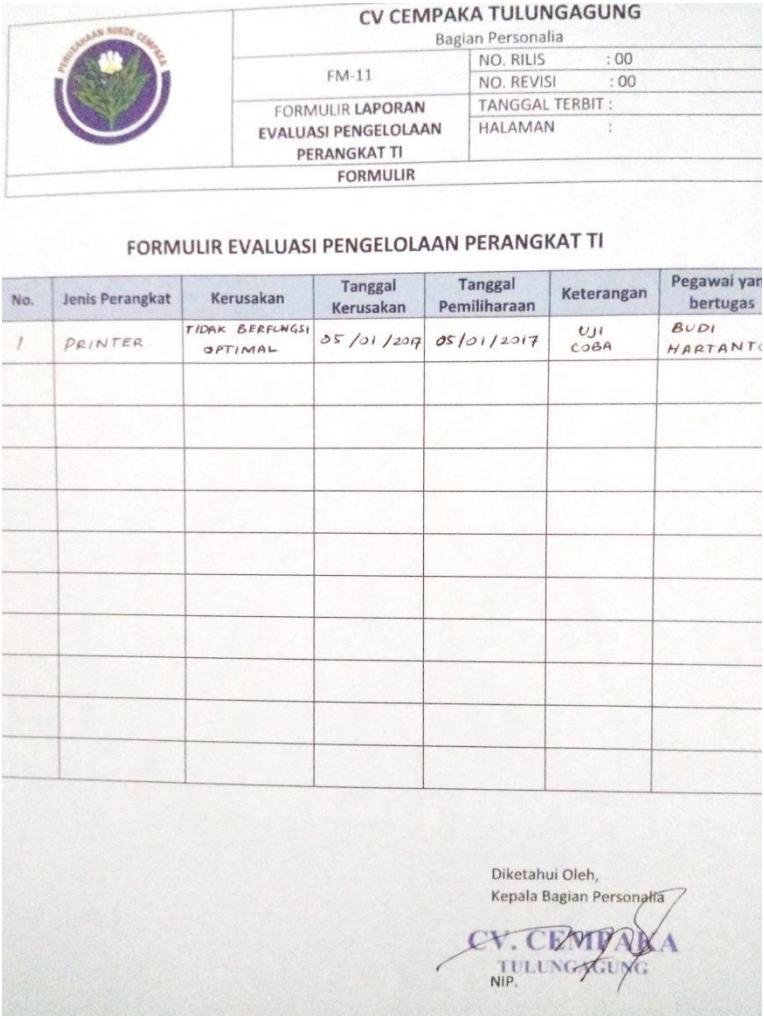
BUDI HARTANTO
NIP.

Diketahui Oleh,
Kepala Bagian Personalia

CV. CEMPAKA TULUNGAGUNG

NIP.

Gambar E.8 Formulir pemeliharaan perangkat TI



CV CEMPAKA TULUNGAGUNG
Bagian Personalia

FM-11	NO. RILIS	: 00
	NO. REVISI	: 00
FORMULIR **LAPORAN EVALUASI PENGELOLAAN PERANGKAT TI**	TANGGAL TERBIT	:
	HALAMAN	:

FORMULIR

FORMULIR EVALUASI PENGELOLAAN PERANGKAT TI

No.	Jenis Perangkat	Kerusakan	Tanggal Kerusakan	Tanggal Pemiliharaan	Keterangan	Pegawai yan bertugas
1	PRINTER	TIDAK BERFUNGSI OPTIMAL	05/01/2017	05/01/2017	UJI COBA	BUDI HARTANT

Diketahui Oleh,
Kepala Bagian Personalia

CV. CEMPAKA
TULUNGAGUNG

NIP.

Gambar E.9 Formulir laporan pengelolaan TI

LAMPIRAN F
KEBIJAKAN

Berikut ini adalah lampiran kebijakan yang dihasilkan dalam penelitian.

1. KEBIJAKAN PENGENDALIAN HAK AKSES APLIKASI

1. TUJUAN

Kebijakan berikut ini dibuat untuk menjamin persyaratan pengendalian hak akses terhadap informasi dan fasilitas informasi yang dimiliki agar dapat di definisikan dengan tepat.

2. RUANG LINGKUP

Kebijakan ini berlaku untuk pihak-pihak yang terkait dengan pengguna dalam menggunakan sistem informasi. sistem informasi yang dimaksud dalam kebijakan tersebut meliputi :

- Sistem Informasi Keuangan
- Sistem Informasi Administrasi
- Sistem Informasi Pendataan dan Penjadwalan
- Sistem informasi Pemasaran

3. REFERENSI

3.1. ISO/IEC 27002:2013 – 9.1.1 Access control policy
3.2. ISO/IEC 27002:2013 – 12.4.1 Event logging

4. KEBIJAKAN

4.1. Pengelolaan hak akses sistem informasi

4.1.1. Hak akses pada setiap sistem informasi yang terkait dengan informasi perusahaan harus dibedakan sesuai peran dan fungsi dari masing masing pengguna.

4.1.2. Pemberian hak akses pada sistem informasi penggunaanya harus dibatasi berdasarkan tugas pokok dan fungsi pengguna dan harus disetujui oleh kepala divisi pada unit bisnis terkait dan kepala bagian personalia selaku penanggung jawab.

4.1.3. Pemberian hak akses sistem informasi yang tingkatannya tinggi (root, super user atau administrator) hanya diberikan kepada karyawan yang benar-benar kompeten, memiliki pengalaman kerja kurang lebih 3 tahun dan mendapat rekomendasi dari kepala divisi unit bisnis terkait dengan sistem informasi.

4.1.4. Setiap pemberian hak akses sistem aplikasi pada pengguna harus disertai dengan kontrak tanggung jawab terkait tanggung jawab yang diberikan.

4.1.5. Setiap proses pengelolaan baik penghapusan maupun pemberian hak akses harus di dokumentasikan.

4.1.6. Hak akses yang sudah di berikan tidak boleh di gunakan maupun di pinjamkan kepada orang lain tanpa adanya ijin dan pemberitahuan perubahan hak akses baru.

4.1.7. Dilakukan peninjauan secara langsung pengguna yang di berikan hak akses minimal 2 kali dalam sebulan.

4.1.8. Dokumentasi wajib di sertai dengan User ID, Aktivitas yang dilakukan, tanggal dan waktu, waktu peristiwa, hak akses yang di berikan, tanda tangan pengguna sistem, tanda tagan kepala bagian personalia, tanda tangan kepala bagian personalia.

4.2. Pengelolaan hak akses - pihak ketiga

4.2.1. Vendor, konsultan, mitra, atau pihak ketiga lainnya yang melakukan akses pada sistem aplikasi CV Cempaka harus menandatangani Ketentuan/Persyaratan Menjaga Kerahasiaan Informasi

4.2.2. Pemberian Hak akses pihak ketiga dapat dilakukan setelah ada konfirmasi dari CV Cempaka dan pihak ketiga.

4.2.3. Setiap hak akses yang di berikan pada pihak ketiga harus di tinjau dan dibatasi waktunya.

4.2.4. Setiap kegiatan yang dilakukan pihak ketiga harus di dokumentasikan.

4.2.5. Dokumentasi wajib di sertai dengan User ID, Aktivitas yang dilakukan, tanggal dan waktu peristiwa, hak akses yang di berikan, tanda tangan pihak ketiga yang diberi akses, tanda tagan kepala bagian personalia

5. DOKUMEN TERKAIT

PO – 01 Prosedur Pengelolaan hak akses

2. KEBIJAKAN KEAMANAN INFORMASI

1. TUJUAN

Kebijakan berikut ini dibuat untuk menjamin keamanan dari informasi penting baik informasi digital dan fisik yang dimiliki perusahaan.

2. RUANG LINGKUP

Kebijakan ini berlaku untuk pihak-pihak yang terkait dengan pengguna dalam menggunakan sistem aplikasi dan menjaga keamanan informasi yang berupa data elektronik. Data elektronik yang dimaksud dalam kebijakan tersebut meliputi :

- Basis Data
- Aplikasi
- Sistem Operasi
- File

3. REFERENSI

3.1. ISO/IEC 27002:2013 – 9.4.1 Information access restriction
3.2. ISO/IEC 27002:2013 – 9.4.2 Secure log-on procedures
3.3. ISO/IEC 27002:2013 – 9.4.3 Password management system
3.4. ISO/IEC 27002:2013 – 12.3.1 Information Backup
3.5. ISO/IEC 27002:2013 – 12.4.1 Event logging
3.6. ISO/IEC 27002:2013 – 12.4.2 Protection of log information
3.7. ISO/IEC 27002:2013 – 12.4.3 Administrator & Operator logs

4. KEBIJAKAN

4.1. Pengelolaan sistem informasi (aplikasi)

4.1.1. Pada setiap sistem aplikasi yang dimiliki perusahaan wajib diberi perbedaan hak akses disesuaikan dengan fungsi dan unit bisnis yang dilakukan.

4.1.2. Pada setiap sistem aplikasi yang dimiliki perusahaan diharuskan ada menu admin untuk melakukan kontrol pada pengguna pada sistem aplikasi tertentu.

4.1.3. Pada setiap sistem operasi dan sistem aplikasi wajib diberikan log-on sistem untuk meverifikasi hak akses pengguna yang akan menggunakan sistem.

4.1.1. Pada setiap sistem aplikasi output yang di hasilkan dari sistem harus di batasi sesuai dengan hak akses yang dimiliki.

4.1.2. Pada setiap sistem aplikasi wajib adanya log-event atau pencatatan kegiatan.

4.1.3. Menghindari terjadinya kapasitas penyimpanan media file log yang sudah berlebih, dengan melakukan backup teratur.

4.1.4. Log-event yang ada pada setiap sistem wajib di dokumentasikan atau di cetak setiap 2 minggu sekali untuk melakukan peninjauan dari kegiatan pengguna pada sistem tersebut.

4.1.5. Dokumentasi Log pada sistem wajib di sertai dengan :

- 4.1.5.1. User ID,
- 4.1.5.2. Aktivitas pada sistem,
- 4.1.5.3. tanggal dan waktu,
- 4.1.5.4. waktu peristiwa,
- 4.1.5.5. jenis hak akses,
- 4.1.5.6. file yang diakses,
- 4.1.5.7. Nyala dan tidaknya kontrol pengamanan pada sistem (seperti antivirus, firewall)
- 4.1.5.8. transaksi yang dilakukan pada sistem.

4.2. Pengelolaan sistem *Log-on*

4.2.1. Tidak menampilkan pengidentifikasi sistem atau tampilan aplikasi sampai proses log-on sudah berhasil dan selesai.

4.2.2. Menampilkan peringatan pemberitahuan umum bahwa komputer hanya bisa diakses oleh pengguna yang berwenang.

4.2.3. Tidak menyediakan pesan bantuan selama prosedur secure log-on berlangsung yang bisa memberikan bantuan kepada pengguna yang tidak berwenang.

4.2.4. Validasi informasi log-on hanya jika seluruh data yang dibutuhkan diisi secara lengkap dan benar. Jika sebuah kondisi error muncul, sistem tidak boleh menunjukkan bagian data mana yang benar dan yang salah.

4.2.5. Batasi jumlah kesempatan log-on gagal yang diizinkan.

4.2.6. Wajib mencatat berapa kali gagal log-on untuk menghindari akses tidak berwenang.

4.2.7. Adanya pesan pengingat untuk maksimal percobaan login.

4.2.8. Karakter password disembunyikan.

4.3. Pengelolaan password pengguna

4.3.1. Menerapkan user id dan password pada setiap sistem untuk menjaga akuntabilitas

4.3.2. Pengguna dapat merubah password mereka sendiri tetapi dengan syarat dan ketentuan yang ada

4.3.3. Password yang digunakan wajib menggunakan password yang berkualitas.

4.3.4. Perubahan password dilakukan dengan teratur selama 3 minggu sekali.

4.3.5. Tidak menggunakan password yang sama saat pergantian password

4.3.6. Tidak menampilkan password ketika melakukan login pada sistem

4.3.7. Password yang dikirimkan ke database akan dikirim dalam bentuk enkripsi.

4.4. Pengelolaan backup dan restore informasi

4.4.1. Backup hanya dapat dilakukan oleh DB Administrator.

4.4.2. Adanya dokumentasi lengkap dari backup maupun restore data yang dilakukan.

4.4.3. Frekuensi backup dilakukan secara teratur dan sesuai kebutuhan bisnis dari organisasi

4.4.4. Data atau Informasi hasil backup dan dokumentasi disimpan dalam tempat yang aman untuk menghindari terjadinya bencana pada lokasi sebelumnya.

4.4.5. Informasi backup harus diberi tingkat perlindungan fisik dan lingkungan yang konsisten.

4.4.6. Media untuk melakukan ackup wajib di uji secara teratur

4.4.7. Data backup wajib dilindungi dengan enkripsi.

5. DOKUMEN TERKAIT

5.1. PO – 02 Prosedur pengelolaan password

5.2. PO – 03 Prosedur backup dan restore

3. KEBIJAKAN PENGELOLAAN HARDWARE DAN JARINGAN

1. TUJUAN

Kebijakan berikut ini dibuat dengan tujuan untuk menjamin fasilitas perangkat hardware dan jaringan agar dapat selalu beroperasi selama proses bisnis berlangsung.

2. RUANG LINGKUP

Kebijakan ini berlaku untuk pihak-pihak yang terkait dalam pengelolaan baik pemeliharaan maupun pengamanan hardware dan jaringan yang ada pada kantor CV Cempaka. Hardware dan jaringan yang dimaksud dalam kebijakan tersebut meliputi :

- Server
- Perangkat PC
- Printer
- Kamera CCTV
- Router
- Kabel listrik
- Kabel Lan

3. REFERENSI

3.1. ISO/IEC 27002:2013 – 11.2.3 Cabling security

3.2. ISO/IEC 27002:2013 – 11.2.4 Equipment maintence

4. KEBIJAKAN

4.1. Pengelolaan hardware

4.1.1. Setiap ruangan diberikan pendingin ruangan untuk menghindari *overheat* (panas berlebih) pada perangkat hardware.

4.1.2. Server berada pada ruangan khusus yang dapat diakses oleh administrator saja.

4.1.3. Setiap ruangan dilengkapi CCTV untuk menghindari adanya pencurian.

4.1.4. Setiap ruangan dilengkapi *fire extinguisher* (alat pemadam) untuk menghindari kemungkinan resiko kebakaran yang meluas.

4.1.5. Setiap kerusakan, kendala perangkat hardware IT pada setiap unit bisnis, wajib segera dilaporkan kepada kepala divisi dan melaporkan kepada pihak divisi personalia selaku penanggung jawab.

4.1.6. Dilarang melakukanmaintenance maupun mengotak atik perangkat hardware tanpa adanya izin dari pihak divisi personalia

4.1.7. Dilarang menambahkan perangkat lain ke perangkat hardware yang ada pada perusahaan.

4.1.8. Dilarang mengambil atau membawa pulang perangkat hardware yang dimiliki perusahaan tanpa izin dari kepala divisi personalia

4.1.9. Setiap 3 bulan sekali wajib dilakukan maintenance perangkat hardware oleh pihak ketiga yang sudah menjalin kerjasama dan persetujuan dari kepala bagian operasional.

4.1.10. Maintenance yang dilakukan harus mengikuti ketentuan dan peraturan perusahaan CV cempaka.

4.1.11. Divisi personalia wajib memastikan perangkat hardware yang dimaintenance dapat digunakan kembali dalam kegiatan operasinal perusahaan.

4.1.12. Setiap kerusakan, kendala, peminjaman, *maintenance* hardware wajib di dokumentasikan.

4.2. Pengelolaan Jaringan

4.2.1. Dibuatkan perlindungan alternative untuk seluruh kabel yang ada pada CV Cempaka.

4.2.2. Dilakukan pelabelan sesuai fungsinya di setiap kabel pada CV Cempaka.

4.2.3. Dilakukan Pembedaan warna kabel untuk mempermudah proses *maintenance* dan pemasangan kabel.

4.2.4. Kabel telekomunikasi dan kabel listrik di tempatkan pada tempat berbeda untuk menghindari terjadinya konsleting.

4.2.5. Setiap kerusakan, kendala perangkat jaringan pada setiap unit bisnis, wajib segera dilaporkan kepada kepala divisi dan melaporkan kepada pihak divisi personalia selaku penanggung jawab.

4.2.6. Setiap 3 bulan sekali wajib dilakukan maintenance perangkat jaringan seperti wifi oleh pihak ketiga yang sudah menjalin kerjasama dan persetujuan dari kepala bagian personalia.

4.2.7. Setiap kerusakan, kendala, *maintenance* hardware wajib di dokumentasikan.

4. KEBIJAKAN HUMAN RESOURCES SECURITY

1. TUJUAN

Kebijakan ini dibuat untuk memberikan peraturan kepada seluruh civitas perusahaan dalam memberi perlindungan keamanan pada aset informasi yang dimiliki perusahaan.

2. RUANG LINGKUP

Kebijakan ini berlaku untuk pengguna yang menggunakan seluruh fasilitias aset informasi yang ada di CV Cempaka. Pengguna yang dimaksudkan tersebut antara lain :

- Pegawai CV Cempaka
- Pegawai magang
- Asosiasi / Pihak Ketiga

3. REFERENSI

3.1. ISO/IEC 27002:2013 – 7.1.2 Terms and conditions of employment.

3.2. ISO/IEC 27002:2013 – 7.2.2 Information security awareness, education, training.

3.3. ISO/IEC 27002:2013 – 9.3.1 Usesecret authentication.

4. KEBIJAKAN

4.1. Keamanan Sumber daya manusia

4.1.1. Setiap pegawai pada perusahaan harus menandatangani dan menyetujui perjanjian (*non-disclosure)* hak akses sebelum diberikan akses pada aset pengolahan informasi

4.1.2. Setiap pihak ketiga yang akan melakukan akses harus menandatangani dan menyetujui perjanjian (*non-disclosure)* hak akses sebelum diberikan akses pada aset pengolahan

4.1.3. Setiap pegawai pada perusahaan harus diberikan pelatihan tentang kesadaran keamanan informasi yang dilakukan setiap 3 bulan sekali.

4.1.4. Pegawai magang pada perusahaan harus diberikan pelatihan dan pemahaman sebelum menggunakan hak akses dan memulai magang.

4.1.5. Kepala bagian personalia berhak untuk melakukan rotasi atau pergantian pegawai yang dinilai tidak relevan pada hak akses yang di berikan dengan persetujuan kepala bagian masing2 unit bisnis.

4.1.6. Setiap pegawai akan dilakukan evaluasi kinerja secara berkala pada tiap akhir bulan oleh kepala divisi pada masing2 unit bisnis

4.1.7. Setiap pegawai yang hak aksesnya di ganti ataupun dihentikan wajib mengisi form pengelolaan hak akses kembali yang di setujui kepala bagian masing-masing unit bisnis

4.2. Tanggung jawab penggunaan hak akses

4.2.1. Menghormati dan melindungi privasi orang lain. Pengguna maupun administrator harus menghormati privasi orang lain ketika mengetahui informasi yang bersifat pribadi dan harus mengambil tindakan pencegahan yang tepat untuk melindungi informasi tersebut dari penggunaan oleh orang yang tidak berwenang.

4.2.2. Menyimpan otentikasi informasi rahasia, memastikan bahwa tidak dibocorkan kepada pihak lain. Pengguna yang memiliki hak akses wajib menjaga informasi rahasia perusahaan baik informasi dalam aplikasi maupun informasi dalam bentuk fisik atau cetakan dan memastikan informasi disimpan pada tempat yang aman untuk menghindari akses dari pihak yang tidak berwenang.

4.2.3. PC dan perangkat pengolahan informasi terlindungi. Administrator maupun pengguna memastikan tidak adanya perangkat lain yang terhubung ke sistem pengolahan informasi perusahaan, memastikan antivirus dan firewall menyala saat digunakan dan pengguna tidak diperbolehkan mengintall aplikasi lain selain yang sudah disediakan perusahaan.

4.2.4. Memastikan penggunaan password berkualitas. Menggunakan password panjang minimal 8 dan menggunakan semua karakter huruf, angka dan symbol.

4.2.5. Melindungi password Password yang digunakan dalam mengakses sistem pengolahan informasi harus dilindungi. Setiap pengguna maupun administrator bertanggung jawab untuk melindungi password yang dimiliki dan tidak membagikannya dengan orang lain, pengguna tidak diperkenankan menggunakan password yang sama dengan akun hak akses lainya.

5. DOKUMEN TERKAIT

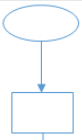
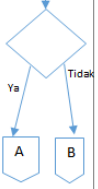
5.1. PO – 06 Prosedur Pelatihan dan Pengembangan SOP

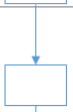
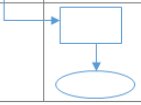
LAMPIRAN G
PROSEDUR

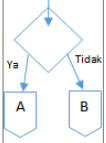
Berikut ini adalah lampiran prosedur yang dihasilkan dalam penelitian.

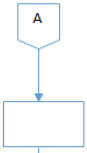
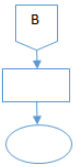
1. Prosedur pengelolaam hak akses

<table>
<tr><td rowspan="5">CV CEMPAKA
TULUNGAGUNG</td><td>Nomor SOP</td><td>PO - 01</td></tr>
<tr><td>Nomor Revisi</td><td>/ /</td></tr>
<tr><td>Tanggal Berlaku</td><td></td></tr>
<tr><td>Nama SOP</td><td>PENGELOLAAN HAK AKSES</td></tr>
<tr><td>Disahkan oleh</td><td>(.....)</td></tr>
<tr><td colspan="2">DESKRIPSI SOP</td><td>KUALIFIKASI DAN DAFTAR PELAKSANA</td></tr>
<tr><td colspan="2">Prosedur pengelolaan hak akses merupakan prosedur untuk menjadi pedoman dalam memberikan alokasi dan penggunaan hak akses terhadap sistem informasi yang seharusnya dikontrol dalam rangka melindungi keamanan data baik dari dalam maupun luar lingkungan perusahaan</td><td>DAFTAR PELAKSANA
- Pengguna sistem
- Administrator
- Kepala bagian personalia
- Kepala Divisi (unit bisnis terkait)
KUALIFIKASI PELAKSANA
1. Memiliki kemampuan pemahaman proses bisnis yang baik.
2. Memiliki pemahaman penggunaan sistem dengan baik.
3. Memiliki kemampuan komunikasi yang baik.
4. Memiliki tanggung jawab kerja.
5. Telah mengikuti pelatihan penggunaan sistem informasi.</td></tr>
<tr><td colspan="2">KETERKAITAN
- Kebijakan pengendalian hak akses</td><td></td></tr>
<tr><td colspan="2">REFERENSI</td><td>PERLENGKAPAN / PERSYARATAN</td></tr>
<tr><td colspan="2">ISO27002:2013 – 9.2.3
Management of privileged access rights</td><td>1. Media komunikasi : Telepon, Email
2. FM – 01 Formulir pengelolaan hak akses
3. FM – 03 Formulir log pengelolaan hak akses
4. FM – 02 Formulir kontrak hak akses</td></tr>
<tr><td colspan="2">PERINGATAN</td><td>PENCATATAN DAN PENDATAAN</td></tr>
<tr><td colspan="2">Jika SOP ini tidak dijalankan, maka pemberian akses pada sistem pelohan informasi tidak sesuai dengan standard keamanan sehingga dapat mengakibatkan kerugian yang ada pada perusahaan (ex : kehilangan data, manipulasi data, akses oleh pihak yang tidak berwenang)</td><td>Admin sistem mencatat setiap perubahan hak akses.</td></tr>
</table>

NO	SUB-AKTIVITAS	PELAKSANA				Dokumen Terkait
		Pengguna Sistem	Admin	Kasie Personalia	Kasie Terkait sistem	
1.	**proses pemberian akses sistem pengolahan informasi perusahaan**					
1.1	Mengajukan permintaan pemberian hak akses baru pada administrator (via : *email*, telepon, maupun langsung)					
1.2	Menanyakan beberapa informasi kepada Kasie terkait sistem, mengenai : Data pegawai yg diberikan akses, Jenis akses, Sistem informasi yang akan di akses, Alasan pemberian hak akses					
1.3	Memberikan balasan terkait informasi yang diminta pada administrator					
1.4	Melakukan pengisian formulir pada formulir pengelolaan hak akses					FM-01 Formulir pengelolaan hak akses
1.5	Melakukan persetujuan dengan kepala bagian personalia ataupun Kasie personalia sebagai perwakilan					FM01 Formulir pengelolaan hak akses

NO	SUB-AKTIVITAS	PELAKSANA				Dokumen Terkait
		Pengguna Sistem	Admin	Kasie Personalia	Kasie Terkait sistem	
A1	**Disetujui :** Jika pegawai telah mengikuti pleatihan, hak akses sesuai dengan jabatan, mampu mengoperasikan sistem dengan baik					
B1	**Tidak Disetujui:** Administrator memberikan informasi terkait persetujuan ditolak karena pengguna Tidak memenuhi kualifikasi dan proses selesai					
1.6	Memproses pemberian hak akses mengikuti instruksi perubahan hak akses					IN-01 Instruksi kerja perubahan hak akses
1.7	memberikan informasi terkait status hak akses yang diberikan pada calon pengguna (via : email, telepon, maupun langsung)					
1.8	Menerima Informasi dari administrator					
1.9	Melakukan tanda tangan persetujuan hak akses					FM-02 Formulir Kontrak Hak Akses
1.10	Memberikan ID, password dan mencatatnya pada formulir log hak akses					FM-03 Formulir Log

NO	SUB-AKTIVITAS	PELAKSANA				Dokumen Terkait
		Pengguna Sistem	Admin	Kasie Personalia	Kasie Terkait sistem	
2.	**Penghapusan hak akses sistem informasi**					
2.1	Mengajukan permintaan penghapusan hak akses pada administrator (via : *email*, telepon, maupun langsung)					
2.2	Menanyakan beberapa informasi, seperti : data pegawai dan alasan penghapusan hak akses					
2.3	Memberikan balasan terkait informasi yang diminta pada administrator					
2.4	Melakukan pengisian formulir pada formulir pengelolaan hak akses					FM-01 Formulir pengelolaan hak akses
2.5	Melakukan persetujuan dengan kepala bagian personalia ataupun Kasie personalia sebagai perwakilan					FM-01 Formulir pengelolaan hak akses

NO	SUB-AKTIVITAS	PELAKSANA				Dokumen Terkait
		Pengguna Sistem	Admin	Kasie Personalia	Kasie Terkait sistem	
A1	**Disetujui :** Jika pegawai telah mengikuti pleatihan, hak akses sesuai dengan jabatan, mampu mengoperasikan sistem dengan baik					
B1	**Tidak di setujui:** Administrator memberikan informasi terkait persetujuan ditolak karena pengguna Tidak memenuhi kualifikasi dan proses selesai.					
2.6	Memproses penghapusan hak akses mengikuti instruksi perubahan hak akses					IN-01 Instruksi kerja perubahan hak akses
2.7	Memberikan informasi terkait status hak akses yang ada pada pegawai yang dihapus (via : email, telepon, maupun langsung)					
3	**Penggantian hak akses sistem informasi**					
3.1	Mengajukan permintaan penggantian hak akses pada administrator (via : *email*, maupun langsung)					
3.2	Menanyakan beberapa informasi					

NO	SUB-AKTIVITAS	PELAKSANA				Dokumen Terkait
		Pengguna Sistem	Admin	Kasie Personalia	Kasie Terkait sistem	
3.3	Memberikan balasan terkait informasi yang diminta pada administrator		1			
3.4	Melakukan pengisian formulir pada formulir pengelolaan hak akses					FM-01 Formulir pengelolaan hak akses
3.5	Melakukan persetujuan dengan kepala bagian personalia ataupun Kasie personalia sebagai perwakilan	Tidak	Ya			FM-01 Formulir pengelolaan hak akses
A1	**Disetujui :** Jika pegawai telah mengikuti pleatihan, hak akses sesuai dengan jabatan, mampu mengoperasikan sistem dengan baik					
B1	**Tidak di setujui:** Administrator memberikan informasi terkait persetujuan ditolak karena pengguna Tidak memenuhi kualifikasi dan proses selesai.					
3.6	Memproses penghapusan hak akses		2			IN-01 Instruksi kerja perubahan hak akses

NO	SUB-AKTIVITAS	PELAKSANA				Dokumen Terkait
		Pengguna Sistem	Admin	Kasie Personalia	Kasie Terkait sistem	
3.7	Memberikan informasi terkait status hak akses yang ada pada pegawai yang digantikan		2			
3.8	Memberikan informasi terkait status hak akses yang diberikan pada calon pengguna hak akses baru					
3.9	Pengguna lama dan calon pengguna Menerima informasi					
3.10	melakukan tanda tangan persetujuan hak akses					FM-02 Formulir Kontrak Hak Akses
3.11	Memberikan id dan password sistem informasi dan mencatatnya pada formulir log pengelolan hak akses					FM-03 Formulir Log

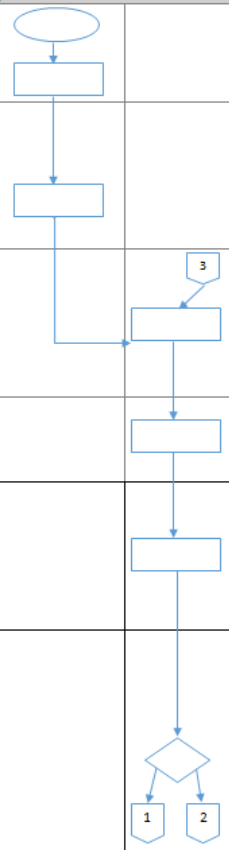
2. Prosedur pengelolaam password

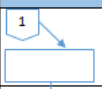
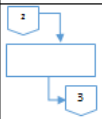
<table>
<tr><td rowspan="5">CV CEMPAKA
TULUNGAGUNG</td><td>Nomor SOP</td><td>PO - 02</td></tr>
<tr><td>Nomor Revisi</td><td>/ /</td></tr>
<tr><td>Tanggal Berlaku</td><td></td></tr>
<tr><td>Nama SOP</td><td>PENGELOLAAN PASSWORD</td></tr>
<tr><td>Disahkan oleh</td><td>(.....)</td></tr>
<tr><td>DESKRIPSI SOP</td><td colspan="2">KUALIFIKASI DAN DAFTAR PELAKSANA</td></tr>
<tr><td>Prosedur Manajemen password merupakan prosedur untuk memastikan pengelolaan penggunaan password telah memenuhi kualitas standard strong password dan memastikan password setiap pengguna telah sesuai dengan syarat kualitas password
KETERKAITAN
- Kebijakan Keamanan Informasi</td><td colspan="2">DAFTAR PELAKSANA
- Pengguna Sistem
- Kepala bagian personalia
- Admnistrator (sistem aplikasi)

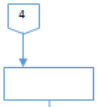
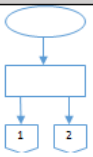
KUALIFIKASI PELAKSANA
- Memiliki pemahaman teknis dan kemampuan mengenai pemrograman
- Memiliki kemampuan pemahaman proses bisnis yang baik
- Memiliki kemampuan komunikasi yang baik</td></tr>
<tr><td>REFERENSI</td><td colspan="2">PERLENGKAPAN / PERSYARATAN</td></tr>
<tr><td>ISO27002:2013 – 9.4.3 Password Management System</td><td colspan="2">- Media komunikasi : Email
- FM – 04 Formulir perbaikan sistem informasi
- FM – 05 Formulir permintaan reset password</td></tr>
<tr><td>PERINGATAN</td><td colspan="2">PENCATATAN DAN PENDATAAN</td></tr>
<tr><td>Jika SOP ini tidak dijalankan, maka pengelolaan password pada sistem informasi tidak sesuai dengan standard keamanan sehingga dapat mengakibatkan risiko hilangnya kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability) data</td><td colspan="2">Pencatatan formulir Perbaikan sistem informasi
Pencatatan formulir permintaan pergantian password</td></tr>
</table>

BAGAN ALUR – PO.02 PENGELOLAAN PASSWORD

NO	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Bagian personalia	Administrator	Pengguna Sistem	Sistem	
1	Proses Perubahan *strong password*					
1.1	Menentukan standart penggunaan password sesuai dengan kualitas standart strong password					KB-03 Kebijakan Keamanan Informasi
1.2	Meminta administrator untuk melakukan penambahan fitur *strong password* dalam semua sistem informasi perusahaan.					
1.3	Melakukan analisis kebutuhan sistem informasi untuk penambahan fitur *strong password* dan menentukan waktu pengerjaan					
1.4	Menambahkan fitur *strong password* sesuai dengan waktu yang ditentukan					
1.5	Memastikan seluruh sistem informasi yang membutuhkan prosedur *log in* telah memiliki ketentuan inputan *strong password*					
1.6	Melakukan pengujian terhadap fitur baru *strong password*					



NO	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Bagian personalia	Administrator	Pengguna Sistem	Sistem	
A1	**Uji coba berhasil** Melakukan pelaporan kepada kepala divisi personalia					
A2	Melakukan validasi dan persetujuan hasil penambahan fitur					
A3	Mengisi laporan perbaikan fitur pada system informasi pada formulit perbaikan system informasi					FM-04 Formulir perbaikan sistem informasi
B1	**Uji coba gagal** Melakukan kembali sub-proses 1.3					
1.7	Mempersiapkan prosedur perubahan *password* lama dan melakukan *setup* pada seluruh sistem					
1.8	Menyediakan *password default* sementara yang telah sesuai dengan standar *strong password* untuk masing masing pengguna sistem					
1.9	Mensosialisasikan penambahan fitur baru kepada seluruh pegawai CV Cempaka					
1.10	Mengirimkan *email* yang berisikan *password default* sementara untuk seluruh pengguna sistem dan informasi mengenai ketentuan penggunaan kualitas standard *strong password*					

NO	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Bagian personalia	Administrator	Pengguna Sistem	Sistem	
1.11	Melakukan *login* dengan menggunakan *password default*					
1.12	Mengeluarkan notifikasi untuk meminta seluruh pegawai melakukan pergantian *password default* dengan *password* baru yang sesuai dengan ketentuan kualitas standard *strong password*					
1.13	Memastikan seluruh pegawai telah mengganti *password default* dalam kurun waktu kurang dari satu bulan					
1.14	Mengelola data penggunaan password lama dan memastikan tidak ada penggunaan kembali *password defaul*					
2	Proses permintaan pergantian password					
2.1	melakukan permintaan reset password : **a. Secara langsung kepada divisi personalia** **b. Via email kepada administrator**					

NO	SUB-AKTIVITAS	PELAKSANA				DOKUMEN TERKAIT
		Bagian personalia	Administrator	Pengguna Sistem	Sistem	
A1	Pengguna Mengajukan permintaan reset password pada divisi personalia			1		
A2	Mengisikan formulir permintaan reset password dan menyertakan alasan pengajuan permintaan password					FM-05 Formulir reset password
B1	Mengajukan permintaan reset password pada administrator via email			2		
B2	membalaskan dengan meminta data informasi terkait pengguna sistem informasi					
B3	Mengirim informasi yang diminta					
B4	Mengisi formulir reset password					FM-05 Formulir reset password
2.2	Melakukan validasi pada permintaan reset password					
2.3	Melakukan reset password dengan mengikuti instruksi reset password					IN-04 Instruksi kerja Reset Password
2.4	Mengirimkan email yang berisikan password sementara yang hanya dapat digunakan sementara					
2.5	Mengakses aplikasi dengan password baru lalu otomatis akan muncul notifikasi untuk segera mengganti password					

4. Prosedur backup dan restore

<table>
<tr><td rowspan="5">CV CEMPAKA
TULUNGAGUNG</td><td>Nomor SOP</td><td>PO - 03</td></tr>
<tr><td>Nomor Revisi</td><td>/ /</td></tr>
<tr><td>Tanggal Berlaku</td><td></td></tr>
<tr><td>Nama SOP</td><td>BACKUP DAN RESTORE</td></tr>
<tr><td>Disahkan oleh</td><td>(.....)</td></tr>
<tr><td colspan="2">DESKRIPSI SOP</td><td>KUALIFIKASI DAN DAFTAR PELAKSANA</td></tr>
<tr><td colspan="2">Prosedur Backup dan Restore Data merupakan prosedur yang bertujuan untuk memastikan backup data yang dilakukans secara berkala telah sesuai dan data yang di backup telah lengkap</td><td rowspan="2">DAFTAR PELAKSANA
- Kabag Personalia
- DB Administrator
KUALIFIKASI PELAKSANA
- Memiliki pemahaman teknis back up dan restore data
- Memiliki kemampuan pemahaman terhadap database, server dan perangkat lain pendukung back up data
- Memiliki kemampuan komunikasi yang baik</td></tr>
<tr><td colspan="2">KETERKAITAN

- Kebijakan Kemanan Informasi</td></tr>
<tr><td colspan="2">REFERENSI</td><td>PERLENGKAPAN / PERSYARATAN</td></tr>
<tr><td colspan="2">ISO27002:2013 – 12.3.1
Information Backup</td><td>- Perangkat media back up dan server
- FM – 06 Formulir klasifikasi data
- FM – 07 Formulir log backup data
- FM – 08 Formulir restore data</td></tr>
<tr><td colspan="2">PERINGATAN</td><td>PENCATATAN DAN PENDATAAN</td></tr>
<tr><td colspan="2">Jika SOP ini tidak dijalankan, maka back up data tidak berjalan dengan baik sehingga dapat mengakibatkan risiko yang berkaitan dengan ketersediaan (availability) data serta terganggunya proses bisnis</td><td>- Mencatat pengklasifikasian data padaformulir Klasifikasi Data
- Mencatat hasil back up data pada formulir Log Backup Data
- Mencatat proses dan hasil restore data pada formulir Restore Data</td></tr>
</table>

BAGAN ALUR – PO. 03 BACK UP DAN RESTORE

NO	SUB-AKTIVITAS	PELAKSANA			DOKUMEN TERKAIT
		Kabag Personalia	Administrator	Sistem	
1	Proses umum sebelum melakukan back-up data				
1.1	Melakukan klasifikasi data dan menentukan tingkat kritikalitas data				FM-06 Formulir klasifikasi data
A1	Membuat strategi backup Melakukan klasifikasi terhadap data dan menentukan tingkatan kritikalitas data untuk menentukan tipe backup				
A2	Melakukan pembaharuan pada formulir daftar klasifikasi data				
A3	Membuat sebuah strategi untuk melakukan backup data sesuai dengan tipe backup				
A4	Menentukan penjadwalan untuk backup data dan tipe backup				
B1	Penentuan Media Backup Administrator melakukan checklist pemeliharaan media backup data				
2	Proses back up data secara berkala				
2.1	Menginstruksikan administrator untuk melakukan back up secara berkala				
2.2	Melakukan setting penjadwalan backup data		1		

NO	SUB-AKTIVITAS	PELAKSANA			DOKUMEN TERKAIT
		Kabag Personalia	Administrator	Sistem	
2.3	Melakukan monitoring secara berkala untuk memastikan bahwa hasil eksekusi backup data telah lengkap		1		
2.4	Mengelola log pada system backup				
2.5	Membuat laporan pada formulir log backup data				FM-07 Formulir log backup data
2.6	Memastikan bahwa administrator telah mengimplementasikan dan melakukan monitoring secara berkala				FM-07 Formulir log backup data
3	Proses uji back up data secara berkala				
3.1	Melakukan uji back up data secara berkala 3 bulan sekali				
3.2	Melakukan set up persiapan uji coba back up data				
3.3	Melakukan uji coba back up data pada media back up				
3.4	Menganalisis log back up data **Apakah back up berhasil ?**	Berhasil			
A1	**Status gagal** Melakukan kembali proses uji coba back up data pada sub-proses 3.2			Gagal	
B1	**Status berhasil** Melakukan pengecekan kesesuaian data yang berhasil ter-backup		2		

NO	SUB-AKTIVITAS	PELAKSANA			DOKUMEN TERKAIT
		Kabag Personalia	Administrator	Sistem	
B2	Membuat laporan pada formulir uji coba log back up data		2		FM-07 Formulir log backup data
4	Proses restore data				
4.1	Menentukan database yang akan dilakukan restore				
4.2	Menentukan jadwal pelaksanaan restore data				
4.3	Melakukan proses restore data				
4.4	Menganalisis hasil restore data **Apakah restore data berhasil ?**		Berhasil		
A1	**Failed** Administrator melakukan kembali sub-proses 4.3		Gagal		
B1	**Successful** Administrator mendokumentasikan pelaksanaan restore data				FM-08 Formulir restore data
4.5	Memvalidasi formulir restore data				

6. Prosedur perawatan hardware

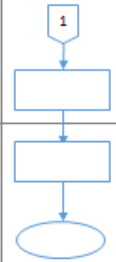
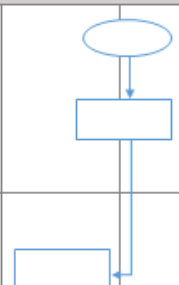
PO – 04. PERAWATAN HARDWARE

CV CEMPAKA TULUNGAGUNG	Nomor SOP	PO - 04
	Nomor Revisi	/ /
	Tanggal Berlaku	
	Nama SOP	PERAWATAN HARDWARE
	Disahkan oleh	(.....)

DESKRIPSI SOP	KUALIFIKASI DAN DAFTAR PELAKSANA
Prosedur perawatan hardware ini merupakan pedoman dan acuan untuk melakukan pengelolaan aset hardware pada perusahaan baik dalam melakukan pengadaan barang, maintenance, penggunaan serta keamanan dari hardware itu sendiri **KETERKAITAN** - Kebijakan Pengelolaan hardware dan jaringan	**DAFTAR PELAKSANA** - Pegawai (Divisi Personalia) - Pegawai (Pengguna fasilitas hardware) - Kepala Bagian Personalia **KUALIFIKASI PELAKSANA** - Memiliki pemahaman teknis dan kemampuan mengenai hardware - Memiliki kemampuan komunikasi yang baik
REFERENSI	**PERLENGKAPAN / PERSYARATAN**
ISO27002:2013 – 11.2.4. *Equipment Maintenance*	- Media komunikasi : Email, telepon - Formulir pemeliharaan perangkat TI - Formulir berita acara kerusakan - Formulir Laporan pengelolaanperangkat TI
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan, maka pengelolaan asset hardware akan tidak sesuai dengan standard keamanan sehingga dapat mengakibatkan terganggunya proses bisnis yang sedang berjalan di perusahaan	Pegawai mencatat aktivitas pada formulir pemeliharaan perangkat TI. Pegawai mencatat pada formulir berita acara setiap terjadinya kerusakan. Pegawai mencatat semua laporan pada formulir laporan evaluasi pengelolaan perangkat TI.

BAGAN ALUR – PO.04 PERAWATAN HARDWARE

NO	SUB-AKTIVITAS	PELAKSANA			DOKUMEN TERKAIT
		Pengguna	Pegawai Divisi Personalia	Vendor	
1	Proses Pelaporan Kerusakan				
1.1	Melapor kerusakan hardware pada divisi personalia (via : email, telepon ataupun langsung).				
1.2	Memproses laporan dengan membuat berita acara kerusakan terkait teknologi informasi yang dilaporkan				
1.3	Melakukan pengecekan pada hardware yang dilaporkan				
1.4	Mencatat pada formulir laporan pengelolaan perangkat TI				FM-11 Formulir laporan pengelolaan perangkat TI
2.	Proses Perbaikan Hardware Secara Parsial				
2.1	Melakukan perbaikan hardware yang dilaporkan (perbaikan dilakukan sesuai dengan kebutuhan)				
2.2	Melakukan pencatatan kegiatan pemeliharaan hardware pada formulir pemeliharaan perangkat TI				FM-09 Formulir pemeliharaan perangkat TI
2.3	Memastikan hardware dapat digunakan kembali		1		

NO	SUB-AKTIVITAS	PELAKSANA			DOKUMEN TERKAIT
		Pengguna	Pegawai Divisi Personalia	Vendor	
2.4	Melapor kepada kabag personalia untuk melakukan validasi berita acara kerusakan				
2.5	Mencatat pada formulir laporan pengelolaan perangkat TI				FM-11 Formulir laporan pengelolaan perangkat TI
3.	Proses Perbaikan Hardware Secara Berkala				
3.1	Melakukan perawatan hardware dilakukan bersama dengan pihak vendor untuk melakukan pemeliharaan rutin hardware yang sudah ditentukan yaitu selama 6 bulan sekali				
3.2	Melakukan pencatatan kegiatan pemeliharaan hardware pada formulir pemeliharaan perangkat TI				FM-09 Formulir pemeliharaan TI
3.3	Memastikan hardware dapat digunakan kembali				
34	Melaporkan kepada kabag personalia untuk melakukan validasi formulir pemeliharaanTI				FM-09 Formulir pemeliharaan TI
3.5	Mencatat pada formulir laporan pengelolaan perangkat TI				FM-11 Formulir laporan pengelolaan perangkat TI

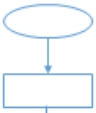
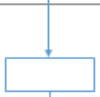
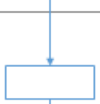
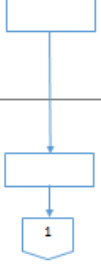
8. Prosedur keamanan kabel

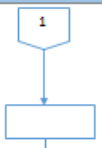
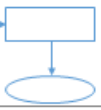
PO – 05. KEAMANAN KABEL

CV CEMPAKA TULUNGAGUNG	Nomor SOP	PO - 05
	Nomor Revisi	/ /
	Tanggal Berlaku	
	Nama SOP	KEAMANAN KABEL
	Disahkan oleh	(.....)

DESKRIPSI SOP	KUALIFIKASI DAN DAFTAR PELAKSANA
Prosedur keamanan kabel merupakan prosedur yang berguna untuk memastikan bahwa seluruh kabel telekomunikasi yang membawa data dan mendukung layanan informasi pada perusahaan diatur atau dikelola secara terstruktur sehingga terlindungi dari kerusakan	**DAFTAR PELAKSANA** - Pegawai Divisi Keamanan - Kepala Bagian Personalia **KUALIFIKASI PELAKSANA** - Memiliki pemahaman teknis dan kemampuan mengenai hardware - Memiliki kemampuan komunikasi yang baik
KETERKAITAN - Kebijakan Pengelolaan Hardware dan Jaringan	
REFERENSI	**PERLENGKAPAN / PERSYARATAN**
ISO27002:2013 – 11.2.3 *Cabling Security*	FM – 10 Formulir berita acara kerusakan FM – 09 Formulir pemeliharaan perangkat TI
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan, maka dapat mengakibatkan terganggunya proses bisnis yang sedang berjalan di perusahaan	**Pencatatan formulir berita acara kerusakan** Pencatatan formulir pemeliharaan perangkat TI

BAGAN ALUR – PO.05 KEAMANAN KABEL

NO	SUB-AKTIVITAS	PELAKSANA		DOKUMEN TERKAIT
		Pegawai Divisi Personalia	Kepala bagian personalia	
1	Proses Pemeliharaan Kabel Telekomunikasi			
1.1	Divisi Keamanan membuatkan perlindungan alternative untuk seluruh kabel yang ada pada CV Cempaka.			
1.2	Divisi Keamanan melakukan pelabelan sesuai fungsinya di setiap kabel pada CV Cempaka.			
1.3	Divisi Keamanan melakukan Pembedaan warna kabel untuk mempermudah proses *maintenance* dan pemasangan kabel.			
1.4	Divisi keamanan menempatkan kabel telekomunikasi dan kabel listrik di tempatkan pada tempat berbeda untuk menghindari terjadinya konsleting.			
1.5	Divisi keamanan membuat berita acara kerusakan terkait kendala perangkat jaringan pada setiap unit bisnis.			FM-10 Formulir berita acara kerusakan

NO	SUB-AKTIVITAS	PELAKSANA		DOKUMEN TERKAIT
		Pegawai Divisi Personalia	Kepala bagian personalia	
1.6	Melakukan maintenance perangkat jaringan oleh pihak ketiga yang sudah menjalin kerjasama dengan CV Cempaka Setiap 3 bulan sekali			FM-09 Formulir pemeliharaan perangkat TI
1.7	Divisi keamanan melaporkan hasil pemeliharaan kabel rutin kepada kabag personalia			FM-09 Formulir pemeliharaan perangkat TI

9. Prosedur pelatihan dan pengembangan

PO – 06. PELATIHAN DAN PENGEMBANGAN SDM

CV CEMPAKA TULUNGAGUNG	Nomor SOP	PO - 06
	Nomor Revisi	/ /
	Tanggal Berlaku	
	Nama SOP	PELATIHAN DAN PENGEMBANGAN SDM
	Disahkan oleh	(.....)

DESKRIPSI SOP	KUALIFIKASI DAN DAFTAR PELAKSANA
Prosedur Pelatihan dan Pengembangan SDM merupakan prosedur yang mengatur segala pelatihan atau edukasi terkait keamanan informasi untuk karyawan yang mampu meningkatkan kualitas baik secara intelektual maupun kepribadian, sehingga mampu menjaga aset informasi yang dimiliki oleh perusahaan	DAFTAR PELAKSANA - Pegawai Perusahaan - Kepala divisi kepegawaian - Pegawai divisi Kepegawaian - Kepala bagian personalia KUALIFIKASI PELAKSANA - Memiliki akses penggunaan data perusahaan - Memiliki kemampuan pemahaman proses bisnis yang baik - Memiliki kemampuan komunikasi yang baik
KETERKAITAN - Kebijakan *Human Resources Security*	
REFERENSI	**PERLENGKAPAN / PERSYARATAN**
ISO27002:2013 – 7.2.2 *Information security awareness, education and Training*	Surat Tugas FM – 12 Formulir data pegawai FM – 13 Formulir evaluasi kegiatan pengembangan kompetensi
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan, maka pegawai akan lebih mudah lalai dalam mengelola informasi perusahaan sehingga dapat mengakibatkan risiko hilangnya data serta dapat merusak citra perusahaan	Pencatatan formulir data pegawai Pencatatan formulir evaluasi kegiatan pengembangan kompetensi

BAGAN ALUR – PO.06 PELATIHAN DAN PENGEMBANGAN SDM

NO	SUB-AKTIVITAS	PELAKSANA				Dokumen Terkait
		Pegawai Divisi Kepegawaian	Kasi Kepegawaian	Kabag Personalia	Pegawai	
1	Proses Identifikasi Kebutuhan Pelatihan					
1.1	Membuat permintaan keikutsertaan kegiatan pengembangan kompetensi					
1.2	Membuat permohonan keikutsertaan dalam kegiatan tersebut					
	Apakah permohonan disetujui ?		Tidak Setuju / Setuju			
A1	**Disetujui** Melanjutkan proses					
A2	**Tidak disetujui** Melakukan kembali sub proses 1.2					
1.4	Memberikan informasi mengenai kegiatan pengembangan kompetensi yang akan diadakan					
2	Proses Persiapan Kegiatan Pelatihan					
2.1	Membuat persiapan dari kegiatan tersebut					
2.2	Pemberian surat tugas					
3	Proses Pelatihan					
3.1	Hadir pelatihan					
3.2	Membuat catatan semua kegiatan pelatihan dalam formulir data pegawai					FM-12 Formulir data pegawai

NO	SUB-AKTIVITAS	PELAKSANA				Dokumen Terkait
		Pegawai Divisi Kepegawaian	Kasi Kepegawaian	Kabag Personalia	Pegawai	
4	Proses Evaluasi Pelatihan					
4.1	Membuat laporan sebagai pertanggung jawaban ke pihak manajemen, paling lambant 1 bulan				1	
4.2	Melakukan evaluasi menggunakan formulir evaluasi kegiatan pengembangan kompetensi					FM-13 Formulir evaluasi pelatihan
4.3	Mempertimbangkan penilaian tahunan pegawai					

LAMPIRAN H
INSTRUKSI KERJA

Berikut ini adalah lampiran instruksi kerja yang dihasilkan dalam penelitian.

1. Instruksi perubahan hak akses sistem informasi

1. Pelaksana

Administrator

2. Rincian instruksi kerja

1. Tahap perubahan hak akses pada sistem informasi yang dimiliki perusahaan dimulai dengan login pada panel admin yang sudah disediakan.
   a. Masukan username dan password administrator
   b. Klik login
   c. Muncul tampilan form untuk kode rahasia masukan kode rahasia administrator
2. Setelah berhasil masuk pada pada panel home, pilih menu *management user* setelah ikuti langkah berikut sesuai dengan perubahan yang diinginkan :
   2.1 Penambahan hak akses baru
      a. Pilih menu tambah user (*New user*)
      b. Muncul tampilan form isikan form tersebut
      c. Masukan nama
      d. Masukan nip
      e. Masukan jabatan
      f. Masukan email
      g. Pilih akses yang diminta
      h. Setelah itu klik lanjutkan
      i. Setelah itu pilih akses pada aplikasi yang diminta
      j. Klik lanjutkan setelah itu muncul kolom kode aplikasi masukan kode aplikasi
      k. Klik simpan dan lanjutkan (save and continue) menunggu sampai muncul notifikasi penambahan user berhasil.
      l. Setelah itu akan muncul username dan password awal yang sesuai ketentuan.
   2.2 Penggantian hak akses

a. Pilih menu edit (*Edit user*)
b. Muncul tampilan tabel user yang sudah terdaftar, pilih user yang akan digantikan lalu klik edit
c. Muncul tampilan form yang sudah terisi, ganti isian form dengan user baru
d. Masukan nama
e. Masukan nip
f. Masukan jabatan
g. Masukan email
h. Pilih akses yang diminta
i. Klik simpan dan lanjutkan menunggu sampai muncul notifikasi pergantian berhasil.
j. Setelah itu akan muncul username dan password awal yang sesuai ketentuan.

2.3 Penghapusan hak akses

a. Pilih menu hapus (*Delete user*)
b. Muncul tampilan tabel user yang sudah terdaftar, pilih user yang akan dihapus lalu klik delete
c. Muncul tampilan notifikasi pilih ya
d. Muncul tampilan form untuk kode rahasia masukan kode rahasia administrator klik simpan dan lanjutkan (save and *continue*)
e. Menunggu sampai muncul notifikasi penghapusan berhasil.

3. Catatan perubahan instruksi

No	Tanggal Revisi	Uraian Revisi

2. Instruksi backup data dan file

1. Pelaksana

Administrator

2. Rincian instruksi kerja

1. Back up Database
   a. Mengaktifkan aplikasi ***Putty***
   b. Login dengan menggunakan IP database
   c. Masukan port : 22
   d. Pilih connection SSH
   e. Lalu pilih ***OPEN***
   f. Login dengan *username* dan *password* ***root***
   g. Layar akan menampilkan *user* dan *last login*
   h. Kemudian masukan *script back up* secara berurutan terdiri dari
      - Password
      - Lokasi direktori
      - Pesan berhasil
   i. Database akan ter back up pada file yang telah dibuat
   j. Selanjutnya lakukan penjadwalan back up data
      - Aktifkan aplikasi Crowntab
      - Masukan jadwal penjadwalan secara otomatis
   k. Klik Enter

2. Back up File
   a. Aktifkan software WDsmartware pada media back up
   b. Tekan tombol Back up
   c. Proses back up file akan secara otomatis berlangsung

3. Catatan perubahan instruksi

No	Tanggal Revisi	Uraian Revisi

3. Instruksi Restore data

1. Pelaksana

Administrator

2. Rincian instruksi kerja

1. Mengaktifkan aplikasi ***Putty***
2. Login dengan menggunakan IP database
3. Masukan port : 22
4. Pilih connection SSH
5. Lalu pilih ***OPEN***
6. Lakukan Create Database yang mau di restore
7. Masukkan *password* ***root***
8. Masukkan script restore yang didalamnya mengidentifikasi file Database yang barus saja di *create* dan file yang akan di *restore*
9. Masukkan kembali *password* ***root***
10. Klik Enter

3. Catatan perubahan instruksi

No	Tanggal Revisi	Uraian Revisi

4. Instruksi reset password

1. Pelaksana

Administrator

2. Rincian instruksi kerja

1. Mereset password pada sistem informasi yang dimiliki perusahaan dimulai dengan login pada panel admin yang sudah disediakan.
   a. Masukan username dan password administrator
   b. Klik login
   c. Muncul tampilan form untuk kode rahasia masukan kode rahasia administrator
2. Setelah berhasil masuk pada pada panel home, pilih menu *management password*
3. Akan muncul tampilan tabel yang berisikan user id, nama, jabatan, divisi, hak akses, dan password (tampilan disembunyikan) pilih sesuai dengan pelapor
4. Klik reset password
5. Lalu akan muncul notifikasi untuk mereset password klik Ya
6. Setelah itu akan muncul password baru setelah di reset.

3. Catatan perubahan instruksi

No	Tanggal Revisi	Uraian Revisi

LAMPIRAN I
FORMULIR

Berikut ini adalah lampiran formulir yang dihasilkan dalam penelitian.

Formulir Pengelolaan hak akses

FM – 01. FORMULIR PENGELOLAAN HAK AKSES

	CV CEMPAKA TULUNGAGUNG Bagian Operasional	
	FM-03	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PENGELOLAAN HAK AKSES	TANGGAL TERBIT : HALAMAN :
FORMULIR		

Tanggal :
Waktu :
Status :

JENIS PENGELOLAAN HAK AKSES ☐ Pemberian Hak Akses ☐ Penghapusan Hak Akses ☐ Penggantian Hak Akses	**SALURAN** ☐ E-mail ☐ Telepon ☐ Offline
IDENTITAS PEGAWAI	
Nama Pegawai	
NIP	
Jabatan	
Email	
No. Hp	
PERMINTAAN AKSES	**JENIS APLIKASI**
Beban saat ini : ☐ Administrator ☐ Manajemen Level I ☐ Manajemen Level II ☐ Pegawai Level I ☐ Pegawai Level II ☐ Pegawai Level III	☐ Sistem Informasi Keuangan ☐ Sistem Informasi Administrasi ☐ Sistem Informasi Pendataan dan Penjadwalan ☐ Sistem Informasi Pemasaran
CATATAN :	
Disetujui Oleh : *(ttd Kasi personalia)*	Diketahui Oleh : *(ttd Kabag Personalia dan umum)*

Formulir kontrak perjanjian hak akses

FM – 02. FORMULIR KONTRAK HAK AKSES

	CV CEMPAKA TULUNGAGUNG Bagian Operasional	
	FM-02	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR KONTRAK HAK AKSES	TANGGAL TERBIT : HALAMAN :
FORMULIR		

PERJANJIAN KERAHASIAAN ATAS HAK AKSES CV CEMPAKA TULUNGAGUNG

Nomor :

Perjanjian Kerahasiaan atas Hak Akses yang ada di CV Cempaka Tulungagung, selanjutnya disebut Perjanjian Kerahasiaan, dibuat pada hari ini, ... tanggal ..... bulan ..... tahun ..... di ..... *(lokasi)*, oleh dan antara:

I. Nama :
Jabatan :
Dalam hal ini disebut sebagai PIHAK PERTAMA yang bertindak sebagai penanggung jawab pemberian hak akses.

II. Nama :
Jabatan :
Dalam hal ini diseburt sebagai PIHAK KEDUA yang bertanggung jawab atas diberikanya hak akses dan menyetujui peraturan-peraturan sebagai berikut :

Pasal 1
Informasi Rahasia

1.1. Untuk kepentingan Perjanjian ini, definisi dari "**Informasi Rahasia**" adalah sebagai berikut:

1.1.1. Setiap informasi mengenai atau yang berhubungan dengan Pemberi, anak perusahaannya, pelanggannya, dan kegiatan usahanya serta operasionalnya, yang disampaikan atau diungkapkan oleh Pemberi kepada Penerima baik secara lisan, tertulis, grafik, magnetik, elektronik atau dalam bentuk lain, baik secara langsung maupun tidak langsung;

1.1.2. Setiap informasi mengenai atau yang berhubungan dengan Transaksi, ketentuan Transaksi, perjanjian yang mengatur Transaksi, ketentuan perjanjian yang mengatur Transaksi dan setiap dokumen yang terkait dengan Transaksi yang diberikan secara langsung ataupun tidak langsung, oleh Pemberi kepada Penerima sehubungan dengan atau dalam hal terkait dengan Transaksi; atau

1.1.3. Segala komunikasi antara Para Pihak, baik secara lisan maupun tulisan yang diketahui atau semestinya diketahui oleh Para Pihak untuk menjadi rahasia atau menjadi milik perusahaan secara alami, dan yang dibuat didalam serangkaian diskusi atau pekerjaan lain yang dilakukan diantara Para Pihak.

1.2. Informasi Rahasia tidak termasuk "Informasi yang Tidak Dilindungi" sebagaimana dijelaskan dalam Pasal 2 Perjanjian ini.

Pasal 2
Informasi yang Tidak Dilindungi

Untuk kepentingan Perjanjian ini, yang dimaksud dengan "**Informasi yang Tidak Dilindungi**" adalah sebagai berikut:

1.1. Informasi yang pada saat penyampaiannya atau pengungkapannya, sudah berada pada kepemilikan yang sah dari Penerima atau tersedia pada Penerima dari sumber lain yang tidak memiliki kewajiban untuk tidak menyampaikan atau mengungkapkannya; atau

1.2. Informasi yang merupakan, atau setiap saat setelah ini menjadi, tersedia untuk umum selain dari pelanggaran Perjanjian ini oleh Penerima.

Pasal 3
Lingkup Perjanjian

2.1. Penerima setuju untuk setiap saat:

2.1.1. Tidak akan mengungkapkan Informasi Rahasia kepada pihak manapun;

2.1.2. Mengambil seluruh tindakan yang diperlukan untuk melindungi kerahasiaan dari Informasi Rahasia; dan

2.1.3. Menghindari pengungkapan atau penyalahgunaan dari Informasi Rahasia,

Demikian Perjanjian Kerahasiaan atas hak akses ini dibuat dan ditandatangani oleh PIHAK PERTAMA dan PIHAK KEDUA di tempat dan pada tanggal tersebut di atas, dalam rangkap 2 (dua) asli bermaterai cukup, masing-masing pihak telah menandatangani Perjanjian ini melalui wakil yang ditunjuk.

Pihak Pertama	**Pihak Kedua**
Tanda Tangan: _____	Tanda Tangan: _____
Dicetak Nama: _____	Dicetak Nama: _____

Formulir log pengelolaan hak akses

FM – 03. FORMULIR LOG PENGELOLAAN HAK AKSES

	CV CEMPAKA TULUNGAGUNG Bagian Operasional	
	FM-03	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR LOG PENGELOLAAN HAK AKSES	TANGGAL TERBIT : HALAMAN :
FORMULIR		

No	NIP	Nama Pegawai	Tanggal	Jam	Jenis Akses	Status Verifikasi
						☐
						☐
						☐
						☐
						☐
						☐
						☐
						☐
						☐
						☐
						☐
						☐

Keterangan :

*Status Verifikasi diisi centang (v) apabila telah terverifikasi dan silang (x) apabila belum terverifikasi

Formulir perbaikan sistem informasi

FM – 04. FORMULIR PERBAIKAN SISTEM INFORMASI

	CV CEMPAKA TULUNGAGUNG Bagian Personalia	
	FM-03	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PERBAIKAN SISTEM INFORMASI	TANGGAL TERBIT : HALAMAN :
FORMULIR		

Laporan Perbaikan Sistem Informasi
Tanggal ..... Bulan .....Tahun .....

Tanggal	*(tanggal permintaan perbaikan sistem informasi)*	Pukul	
Nama	*(nama pihak terkait yang melakukan permintaan perbaikan sistem)*		
Unit Kerja	*(unit kerja terkait yang melakukan permintaan perbaikan sistem)*		
Menu & Submenu yang diperbaiki	*(keterangan menu/sub menu/ fitur)*		
Uraian Perbaikan	*(keterangan perbaikan sistem informasi)*		
REALISASI KERJA			
Analisis/Tinjuan *(disii oleh Operasional)*	*(keterangan analisis perbaikan sistem informasi yang akan dilakukan)*		
Perbaikan *(disii oleh Operasional)*	*(keterangan perbaikan sistem informasi yang berhasil dilakukan)*		
Tanggal Mulai	*(tanggal mulai perbaikan sistem informasi)*	Pukul	
Tanggal Selesai	*(tanggal berkahirnya perbaikan sistem informasi)*	Pukul	

Mengetahui,
Kepala Bagian Personalia

(*Nama Lengkap Kepala Bagian Operasional*)
NIP .....

(Lokasi) , (Tanggal – Bulan – Tahun)
Administrator,

(*Nama Lengkap Pegawai Bagian Operasional*)
NIP .....

Formulir permintaan pergantian password

FM – 05. FORMULIR PERMINTAAN PERGANTIAN PASSWORD

	CV CEMPAKA TULUNGAGUNG Bagian Personalia	
	FM-04	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PERMINTAAN PERGANTIAN PASSWORD	TANGGAL TERBIT : HALAMAN :
FORMULIR		

FORMULIR PERMINTAAN PERGANTIAN PASSWORD

Nomor FM-04 - ... / ... / ...

Pemohon	
Tanggal :	Tanda Tangan :
Nama :	
NIP :	
Jabatan :	
Divisi :	
Email aktif :	
Keterangan *(diisi dengan alasan permintaan pergantian password)*	

(Lokasi) , (Tanggal – Bulan – Tahun)

Administrator,

(Nama Lengkap Pegawai Bagian Operasional)

NIP .....

Formulir klasifikasi data

FM – 06. FORMULIR KLASIFIKASI DATA

	CV CEMPAKA TULUNGAGUNG Bagian Personalia	
	FM-05	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR KLASIFIKASI DATA	TANGGAL TERBIT : HALAMAN :
FORMULIR		

FORMULIR DAFTAR KLASIFIKASI DATA

Periode ..... Tahun .....

DAFTAR KLASIFIKASI DATA ATAU INFORMASI

No	Jenis Data	Klasifikasi	Kritikalitas
1.	**Data Produksi**		
	a. Total penjualan pertahun	*Rahasia*	*Tinggi*
	b. Total produkasi pertahun	*Rahasia*	*Tinggi*
2.	**(Klasifikasi Kelompok Data)**		
	a. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	b. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	c. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	d. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	e. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	f. (*data*)	*(klasifikasi)*	*(kritikalitas)*
2.	**(Klasifikasi Kelompok Data)**		
	a. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	b. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	c. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	d. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	e. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	f. (*data*)	*(klasifikasi)*	*(kritikalitas)*
3.	**(Klasifikasi Kelompok Data)**		
	a. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	b. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	c. (*data*)	*(klasifikasi)*	*(kritikalitas)*
	d. (*data*)	*(klasifikasi)*	*(kritikalitas)*

(Lokasi) , (Tanggal – Bulan – Tahun)

Mengetahui,

Kepala Bagian Personalia

(Nama Lengkap Kepala Bagian

Formulir log backup data

FM – 07. FORMULIR LOG BACK UP DATA

	CV CEMPAKA TULUNGAGUNG Bagian Personalia	
	FM-06	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR BACK UP DATA	TANGGAL TERBIT : HALAMAN :
FORMULIR		

Log Backup Sheet
Bulan ..... Tahun .....

Log ke -	*I*	*II*	*III*	*IV*	*dst..*
Tanggal *(1)*					
Waktu *(2)*					
Metode Backup *(3)*					
Jumlah Media *(4)*					
Nama Media Backup *(5)*					
Isi Media Backup *(6)*					
Status Backup *(7)*					
Keterangan *(8)*					

Keterangan Pengisian :

(1) Diisi dengan tanggal backup
(2) Diisi dengan waktu backup berhasil dilakukan (*backup completed*)
(3) Diisi dengan metode backup yang dilakukan
(4) Diisi dengan jumlah media backup
(5) Diisi dengan nama media backup
(6) Diisi dengan keterangan data/file dalam media backup
(7) Diisi dengan status backup
(8) Diisi dengan keterangan dari status backup (data yang berhasil/data yang tidak di-backup, eror yang terjadi, dll)

(Lokasi) , (Tanggal – Bulan – Tahun)
Administrator,

(Nama Lengkap Pegawai Bagian Personalia)
NIP .....

Formulir restore data

FM – 08. FORMULIR RESTORE DATA

	CV CEMPAKA TULUNGAGUNG Bagian Personalia	
	FM-07	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR RESTORE DATA	TANGGAL TERBIT : HALAMAN :
FORMULIR		

FORMULIR RESTORE DATA	
Tanggal Backup	*Tanggal melakukan backup data*
Nama Staff	*Nama pegawai yang melakukan restore data*
Sumber Data	*Keterangan terkait sumber data backup*
Data yang di Restore	*Keterangan terkait data yang di restore*
Tipe Back up	☐ **Full Backup** ☐ **Partial/Incremental Backup**
Media Back up	*Media yang digunakan unuk penyimpanan data backup*
Recovery point of objective	*Keterangan bagian data yang akan di restore setelah pemulihan layanan teknologi informasi*
Catatan :	
	(Lokasi) , (Tanggal – Bulan – Tahun) **Administrator,** *(Nama Lengkap Administrator)* **NIP** .....

Formulir pemeliharaan perangkat TI

FM – 09. FORMULIR PEMELIHARAAN PERANGKAT TI

	CV CEMPAKA TULUNGAGUNG Bagian Personalia	
	FM-08	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PEMELIHARAAN PERANGKAT TI	TANGGAL TERBIT : HALAMAN :
FORMULIR		

No. Form :
Tanggal :

Jenis Perangkat Teknologi informasi : (*Jenis perangkat yang di lakukan pemeliharaan*)

Jumlah : (*Jumlah perangkat yang di lakukan pemeliharaan*)

Pemeliharaan yang dilakukan:

(Log *Aktivitas pemeliharaan yang dilakukan*)

Tanggal Pemeliharaan	Waktu	Pelaksana	Keterangan

(Lokasi , Tanggal – Bulan – Tahun)

Pegawai yang bertugas,

(*Nama Lengkap pegawai*)

NIP.

Diketahui Oleh,
Kepala Bagian Personalia

NIP.

Formulir berita acara kerusakan

FM – 10. FORMULIR BERITA ACARA KERUSAKAN

	CV CEMPAKA TULUNGAGUNG Bagian Personalia	
	FM-09	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR BERITA ACARA KERUSAKAN	TANGGAL TERBIT : HALAMAN :
	FORMULIR	

No. Form :
No. Berita Acara :
Tanggal :

Kerusakan :
☐ Personal Computer (PC)
☐ Router / Hub
☐ Wireless
☐ LCD Proyektor
☐ Access Point
☐ Kabel Telekomunikasi
☐ Printer

Penyebab Kerusakan :

Perbaikan / Pergantian Material
Nama Barang :
Type :
S/N :
Jumlah :

Tanggal Perbaikan	Waktu	Pelaksana	Keterangan

Pengguna

(Lokasi , Tanggal – Bulan – Tahun)
Diketahui Oleh,
Kepala Bagian Personalia

NIP.

NIP.

Formulir laporan evaluasi pengelolaan perangkat TI

FM – 11. FORMULIR LAPORAN EVALUASI PENGELOLAAN PERANGKAT TI

	CV CEMPAKA TULUNGAGUNG Bagian Personalia	
	FM-10	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR **LAPORAN EVALUASI PENGELOLAAN PERANGKAT TI**	TANGGAL TERBIT : HALAMAN :
FORMULIR		

FORMULIR EVALUASI PENGELOLAAN PERANGKAT TI

No.	Jenis Perangkat	Kerusakan	Tanggal Kerusakan	Tanggal Pemiliharaan	Keterangan	Pegawai yang bertugas
	(Jenis perangkat yang dilakukan pengelolaan)	*(jenis kerusakan)*	*(Tanggal – Bulan – Tahun)*	*(Tanggal – Bulan – Tahun)*	*(Status Perangkat)*	*(Nama pegawai)*

(Lokasi , Tanggal – Bulan – Tahun)
Diketahui Oleh,
Kepala Bagian Personalia

NIP.

Formulir data pegawai

FM – 12. FORMULIR DATA PEGAWAI

	CV CEMPAKA TULUNGAGUNG Bagian Operasional	
	FM-12	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR DATA PEGAWAI	TANGGAL TERBIT : HALAMAN :
FORMULIR		

Formulir Kehadiran Pegawai

Tanggal :

Topik :

Instruktur :

Tempat :

NO	Nama Peserta	Departemen	Jabatan	Tanda Tangan	Keterangan

(Lokasi) , (Tanggal – Bulan – Tahun)

Pegawai Divisi Kepegawaian,

(Nama Lengkap Pegawai Divisi Kepegawaian)

NIP .....

Formulir evaluasi kegiatan pengembangan kompetensi

FM – 13. FORMULIR EVALUASI KEGIATAN PENGEMBANGAN KOMPETENSI

	CV CEMPAKA TULUNGAGUNG Bagian Operasional	
	FM-10	NO. RILIS : 00 NO. REVISI : 00
	FORMULIR PEMELIHARAAN IT	TANGGAL TERBIT : HALAMAN :
FORMULIR		

Formulir Evaluasi Pelatihan

Nama : ..... Jabatan : .....

Divisi : ..... Departemen : .....

Judul Materi : ..... Tgl Pelatihan : .....

Sasaran Pelatihan : .....

.....

.....

Evaluasi Pelatihan :

☐ Langsung setelah pelatihan ☐ 1 Bulan setelah pelatihan

☐ 2 Bulan setelah pelatihan ☐ 3 Bulan setelah pelatihan

☐ Lain - lain .....

Metode Evaluasi :

☐ Tes / Ujian ☐ Observasi / Pengamatan

Point Evaluasi : *(Lingkari huruf sesuai penilaian)*

☐ Pengetahuan
Mampu menjelaskan isi / materi training Y - N
Mampu menjelaskan konsep-konsep yang ada pada training Y - N

☐ Sikap
Menunjukkan Sikap sesuai dengan konsep dari training Y - N

☐ Ketrampilan *(dapat melakukan ketrampilan seperti yang diajarkan dalam pelatihan)*

1 ..... Y - N
2 ..... Y - N
3 ..... Y - N
4 ..... Y - N
5 ..... Y - N

Tindak lanjut Dari Evaluasi :

.....

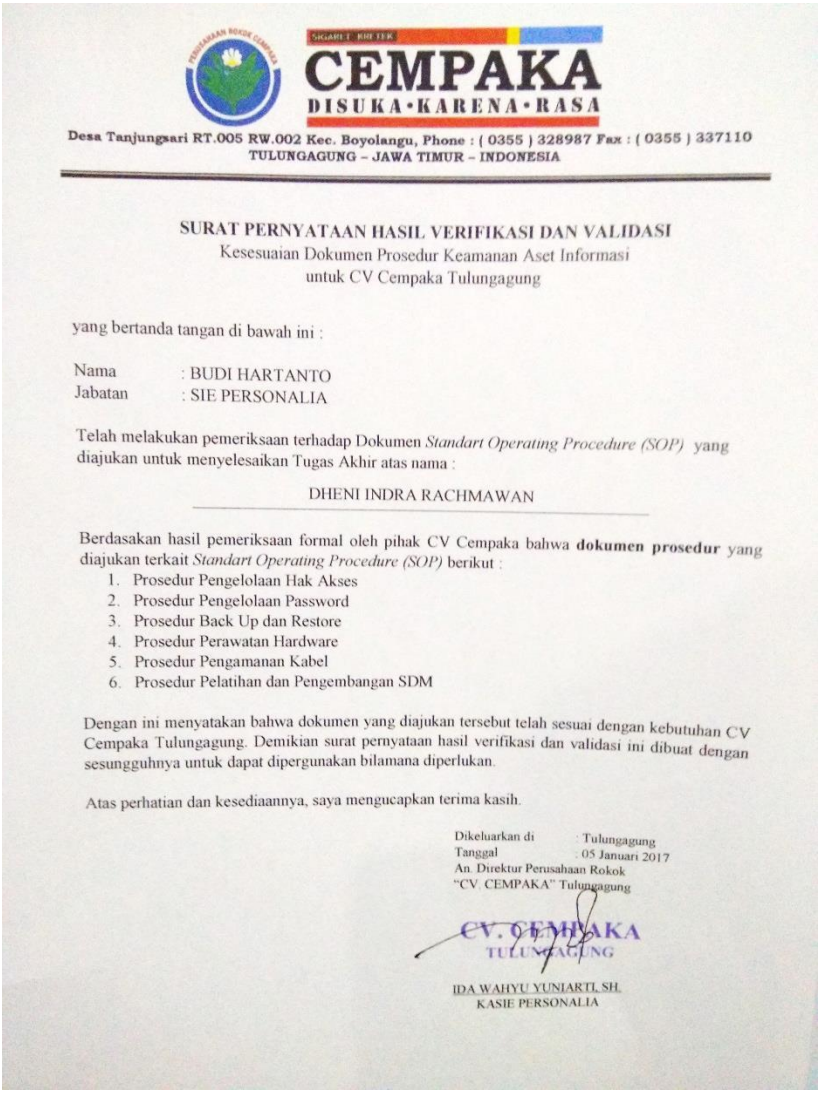
Tulungagung, ...
Dievaluasi oleh, Diketahui oleh,

Kasi Kepegawaian Kabag Personalia

LAMPIRAN J
KONFIRMASI VERIFFIKASI DAN VALIDASI

Berikut ini adalah lampiran verifikasi dan validasi pihak CV Cempaka terkait prosedur dan kebijakan yang di hasilkan dan surat keterangan telah melakukan penelitian.

Verifikasi dan validasi ini dilakukan kepada Kasie personalia CV Cempaka untuk memastikan hasil akhir dari dokumen SOP Kemanan aset informasi ini telah sesuai dengan kondisi di perusahan CV Cempaka Tulungagung.



CEMPAKA
DISUKA•KARENA•RASA
Desa Tanjungsari RT.005 RW.002 Kec. Boyolangu, Phone : (0355) 328987 Fax : (0355) 337110
TULUNGAGUNG – JAWA TIMUR – INDONESIA

SURAT PERNYATAAN HASIL VERIFIKASI DAN VALIDASI
Kesesuaian Dokumen Prosedur Keamanan Aset Informasi
untuk CV Cempaka Tulungagung

yang bertanda tangan di bawah ini :

Nama : BUDI HARTANTO
Jabatan : SIE PERSONALIA

Telah melakukan pemeriksaan terhadap Dokumen *Standart Operating Procedure (SOP)* yang diajukan untuk menyelesaikan Tugas Akhir atas nama :

DHENI INDRA RACHMAWAN

Berdasakan hasil pemeriksaan formal oleh pihak CV Cempaka bahwa **dokumen prosedur** yang diajukan terkait *Standart Operating Procedure (SOP)* berikut :

1. Prosedur Pengelolaan Hak Akses
2. Prosedur Pengelolaan Password
3. Prosedur Back Up dan Restore
4. Prosedur Perawatan Hardware
5. Prosedur Pengamanan Kabel
6. Prosedur Pelatihan dan Pengembangan SDM

Dengan ini menyatakan bahwa dokumen yang diajukan tersebut telah sesuai dengan kebutuhan CV Cempaka Tulungagung. Demikian surat pernyataan hasil verifikasi dan validasi ini dibuat dengan sesungguhnya untuk dapat dipergunakan bilamana diperlukan.

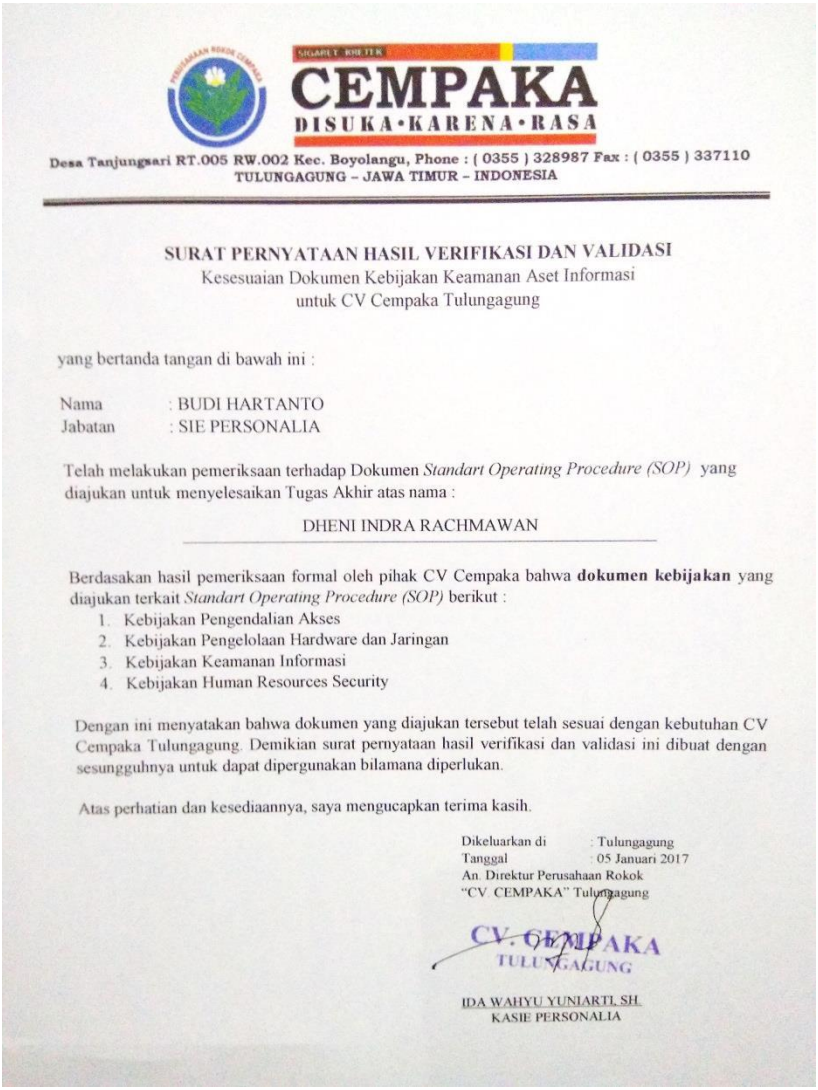
Atas perhatian dan kesediaannya, saya mengucapkan terima kasih.

Dikeluarkan di : Tulungagung
Tanggal : 05 Januari 2017
An. Direktur Perusahaan Rokok
"CV. CEMPAKA" Tulungagung

CV. CEMPAKA
TULUNGAGUNG

IDA WAHYU YUNIARTI, SH.
KASIE PERSONALIA

Gambar J.1 konfirmasi verifikasi validasi hasil prosedur



CEMPAKA
DISUKA·KARENA·RASA
Desa Tanjungsari RT.005 RW.002 Kec. Boyolangu, Phone : (0355) 328987 Fax : (0355) 337110
TULUNGAGUNG – JAWA TIMUR – INDONESIA

SURAT PERNYATAAN HASIL VERIFIKASI DAN VALIDASI
Kesesuaian Dokumen Kebijakan Keamanan Aset Informasi
untuk CV Cempaka Tulungagung

yang bertanda tangan di bawah ini :

Nama : BUDI HARTANTO
Jabatan : SIE PERSONALIA

Telah melakukan pemeriksaan terhadap Dokumen *Standart Operating Procedure (SOP)* yang diajukan untuk menyelesaikan Tugas Akhir atas nama :

DHENI INDRA RACHMAWAN

Berdasakan hasil pemeriksaan formal oleh pihak CV Cempaka bahwa **dokumen kebijakan** yang diajukan terkait *Standart Operating Procedure (SOP)* berikut :

1. Kebijakan Pengendalian Akses
2. Kebijakan Pengelolaan Hardware dan Jaringan
3. Kebijakan Keamanan Informasi
4. Kebijakan Human Resources Security

Dengan ini menyatakan bahwa dokumen yang diajukan tersebut telah sesuai dengan kebutuhan CV Cempaka Tulungagung. Demikian surat pernyataan hasil verifikasi dan validasi ini dibuat dengan sesungguhnya untuk dapat dipergunakan bilamana diperlukan.

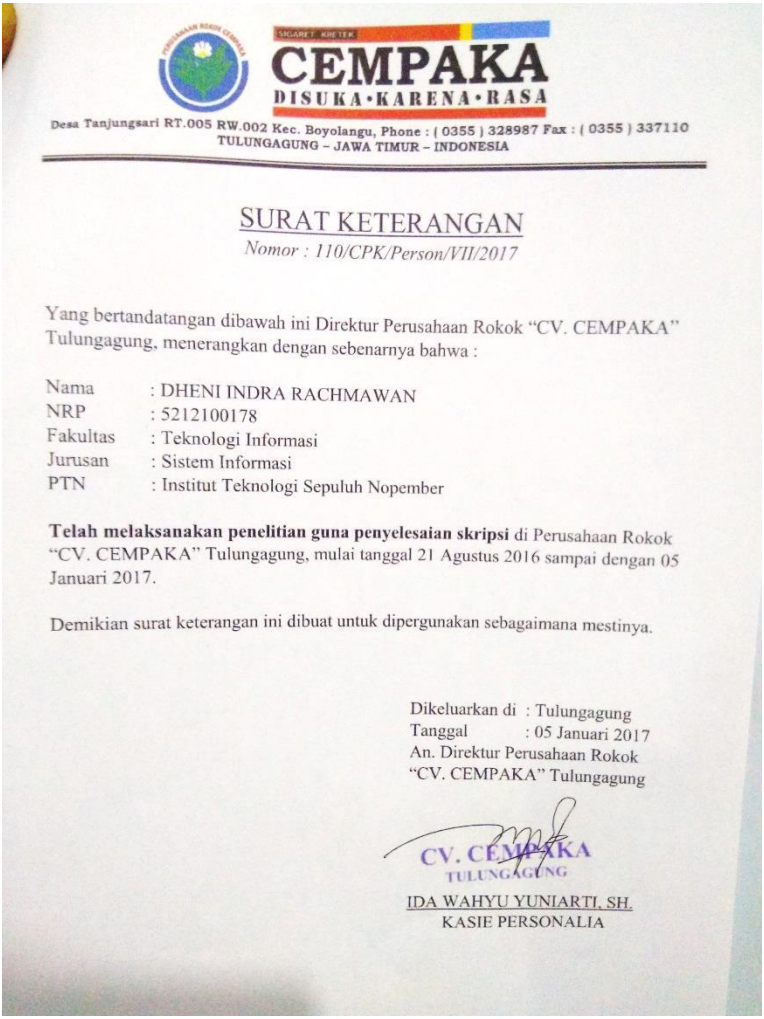
Atas perhatian dan kesediaannya, saya mengucapkan terima kasih.

Dikeluarkan di : Tulungagung
Tanggal : 05 Januari 2017
An. Direktur Perusahaan Rokok
"CV. CEMPAKA" Tulungagung

CV. CEMPAKA
TULUNGAGUNG

IDA WAHYU YUNIARTI, SH
KASIE PERSONALIA

Gambar J.2 Konfirmasi verifikasi validasi hasil kebijakan



CEMPAKA
DISUKA•KARENA•RASA
Desa Tanjungsari RT.005 RW.002 Kec. Boyolangu, Phone : (0355) 328987 Fax : (0355) 337110
TULUNGAGUNG – JAWA TIMUR – INDONESIA

SURAT KETERANGAN
Nomor : 110/CPK/Person/VII/2017

Yang bertandatangan dibawah ini Direktur Perusahaan Rokok "CV. CEMPAKA" Tulungagung, menerangkan dengan sebenarnya bahwa :

Nama	: DHENI INDRA RACHMAWAN
NRP	: 5212100178
Fakultas	: Teknologi Informasi
Jurusan	: Sistem Informasi
PTN	: Institut Teknologi Sepuluh Nopember

Telah melaksanakan penelitian guna penyelesaian skripsi di Perusahaan Rokok "CV. CEMPAKA" Tulungagung, mulai tanggal 21 Agustus 2016 sampai dengan 05 Januari 2017.

Demikian surat keterangan ini dibuat untuk dipergunakan sebagaimana mestinya.

Dikeluarkan di : Tulungagung
Tanggal : 05 Januari 2017
An. Direktur Perusahaan Rokok
"CV. CEMPAKA" Tulungagung

CV. CEMPAKA
TULUNGAGUNG

IDA WAHYU YUNIARTI, SH.
KASIE PERSONALIA

Gambar J.3 Surat pernyataan melakukan penelitian pada perusahaan rokok CV Cempaka