

**PERANCANGAN SOP (*STANDARD OPERATING PROCEDURE*)  
KEAMANAN INFORMASI PENGELOLAAN DATA  
KEHADIRAN PEGAWAI DI FAKULTAS TEKNIK  
UNIVERSITAS PASUNDAN BANDUNG**

**TUGAS AKHIR**

Disusun sebagai salah satu syarat untuk kelulusan  
Program Strata 1, Program Studi Teknik Informatika,  
Universitas Pasundan Bandung

oleh :

Dinda Putri Wahyuni  
NRP.10.304.0176



**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS PASUNDAN BANDUNG  
MEI 2015**



**LEMBAR PENGESAHAN  
LAPORAN TUGAS AKHIR**

Telah disetujui dan disahkan, Laporan Tugas Akhir, dari :

Nama : Dinda Putri Wahyuni

Nrp : 10.304.0176

Dengan judul :

“PERANCANGAN SOP (STANDARD OPERATING PROCEDURE)  
KEAMANAN INFORMASI PENGELOLAAN DATA  
KEHADIRAN PEGAWAI DI FAKULTAS TEKNIK  
UNIVERSITAS PASUNDAN BANDUNG”

Bandung, Mei 2015

Menyetujui,

Pembimbing Utama,

Pembimbing Pendamping,

(Ririn Dwi Agustin, ST.,MT.)

(Muhammad Tirta Mulia, ST., MT.)



## **KATA PENGANTAR**

Ucapan dan rasa syukur penulis layangkan ke hadirat Ilahi Robbi, yang telah berkenan menguatkan penulis untuk membuat Laporan Tugas Akhir dengan judul “Perancangan SOP (*Standard Operating Procedure*) Keamanan Informasi Pengelolaan Data Kehadiran Pegawai Di Fakultas Teknik Universitas Pasundan Bandung ”

Adapun penulisan laporan ini bertujuan untuk memenuhi salah satu syarat kelulusan Program Strata 1, di Program Studi Teknik Informatika Universitas Pasundan.

Penulis menyadari laporan ini dapat terwujud berkat bantuan dan dorongan dari berbagai pihak. Maka pada kesempatan ini penulis sampaikan terima kasih yang sebesar-besarnya atas segala bantuan yang penulis terima baik secara moril maupun materil, sehingga penulis dapat menyelesaikan laporan ini kepada :

1. Allah SWT, atas anugerah serta rahmat-Nya sehingga penulis mampu menyelesaikan Tugas Akhir ini
2. Kedua pembimbing, Ibu Ririn Dwi Agustin,ST,MT dan Bapak Muhammad Tirta Mulia,ST, MT yang telah membimbing penulis dalam menyelesaikan tugas akhir ini.
3. Kepada Orang Tua dan keluarga yang selalu memberikan motivasi serta do'anya dalam pembuatan tugas akhir ini.
4. Kepada Ibu Heni , Bapak Sali Alas, Bapak Adi dan Bapak Aji yang telah membantu penulis dalam memberikan penjelasan mengenai pengelolaan data pegawai.
5. Seluruh civitas akademika Teknik Informatika di Universitas Pasundan Bandung yang telah memberikan bekal ilmu selama penulis menimba ilmu.
6. Kepada teman-teman seperjuangan Universitas Pasundan Bandung yang tidak bisa semua penulis sebutkan satu per satu.

Tiada gading yang tak retak, tiada gelombang tanpa ombak, segala kesalahan merupakan kelemahan dan kekurangan penulis. oleh karena itu, penulis harapkan kritik dan saran dari semua pihak demi perbaikan di masa yang akan datang. Akhir kata, semoga penulisan laporan ini dapat bermanfaat bagi penulis dan bagi perkembangan ilmu Teknologi dimasa yang akan datang.

Bandung, Mei 2015

Penulis



## DAFTAR ISI

ABSTRAK .....	<b>Error! Bookmark not defined.</b>
ABSTRACT .....	<b>Error! Bookmark not defined.</b>
KATA PENGANTAR .....	i
DAFTAR ISI .....	iv
DAFTAR ISTILAH .....	vii
DAFTAR TABEL .....	viii
DAFTAR GAMBAR .....	ix
DAFTAR LAMPIRAN .....	x
DAFTAR SIMBOL .....	xi
BAB 1 PENDAHULUAN .....	1-1
1.1 Latar Belakang .....	1-1
1.2 Identifikasi Masalah .....	1-2
1.3 Tujuan Tugas Akhir .....	1-2
1.4 Lingkup Tugas Akhir .....	1-2
1.5 Metodologi Tugas Akhir .....	1-2
1.6 Sistematika Penulisan .....	1-3
BAB 2 LANDASAN TEORI .....	2-1
2.1 Pengertian SOP ( <i>Standard Operating Procedure</i> ) .....	2-1
2.1.1 Prinsip Penyusunan SOP ( <i>Standard Operating Procedure</i> ) .....	2-1
2.1.2 Prinsip Penerapan SOP ( <i>Standard Operating Procedure</i> ) .....	2-2
2.1.3 Manfaat SOP ( <i>Standard Operating Procedure</i> ) Bagi Organisasi Bisnis .....	2-2
2.1.4 Format SOP ( <i>Standard Operating Procedure</i> ) .....	2-3
2.1.4.1 Langkah Sederhana ( <i>Simple Steps</i> ) .....	2-4
2.1.4.2 Tahapan Berurutan ( <i>Hierarchical Steps</i> ) .....	2-4
2.1.4.3 Grafik ( <i>Graphic</i> ) .....	2-5
2.1.4.4 Diagram Alir ( <i>Flowchart</i> ) .....	2-6
2.2 Pengertian Keamanan Informasi .....	2-7
2.2.1 Fasilitas Informasi .....	2-8
2.2.2 Aspek Keamanan Informasi .....	2-8
2.2.3 Metode- Metode Keamanan Informasi .....	2-10
2.3 ISO/IEC 27001 .....	2-10
2.3.1 Metode Pendekatan Proses ( ISO/IEC 27001) .....	2-12
2.3.2 Struktur Organisasi ISO/IEC 27001 .....	2-13
2.4 Manajemen Resiko .....	2-16

2.4.1 Tujuan Manajemen Resiko.....	2-16
2.4.2 Penilaian Resiko (Risk Assessment) .....	2-16
2.4.2.1 Identifikasi Aset.....	2-16
2.4.2.2 Identifikasi Ancaman (Threat).....	2-18
2.4.2.3 Identifikasi Kelemahan (vulnerability).....	2-18
2.4.2.4 Menentukan kemungkinan ancaman (probability) .....	2-19
2.4.2.5 Analisa Dampak (impact analysis) .....	2-19
2.4.2.6 Menentukan nilai resiko .....	2-20
<b>BAB 3 ANALISIS RESIKO .....</b>	<b>3-1</b>
3.1 Kerangka Tugas Akhir .....	3-1
3.2 Skema Analisis .....	3-2
3.3 Gambaran Umum Tentang Pengelolaan Data Kehadiran Pegawai Fakultas Teknik .....	3-2
3.3.1 Struktur Organisasi Kepegawaian Fakultas Teknik .....	3-3
3.3.2 Deskripsi Wewenang dan Tangungjawab .....	3-4
3.3.3 Aturan Jam Kerja Pada Absensi Pegawai Fakultas Teknik.....	3-7
3.4 Analisis Teknologi Pengelolaan Data Kehadiran Pegawai Fakultas Teknik.....	3-8
3.4.1 Perangkat Keras ( <i>Hardware</i> ).....	3-8
3.4.2 Perangkat Lunak ( <i>Software</i> ) .....	3-8
3.4.3 Infrastruktur Pengelolaan Data Kehadiran .....	3-8
3.5 Penilaian Resiko .....	3-9
3.5.1 Identifikasi Aset.....	3-9
3.5.2 Identifikasi Ancaman ( <i>Threat Identification</i> ).....	3-10
3.5.3 Identifikasi Kelemahan ( <i>Vulnerability Identification</i> ).....	3-10
3.5.4 Kemungkinan Gangguan Keamanan (Probability of Occurrence) .....	3-12
3.5.5 Menghitung Nilai Business Impact Analysis (BIA).....	3-13
3.5.6 Menentukan nilai Resiko .....	3-14
3.6 Evaluasi Gangguan Keamanan Informasi Terhadap Aset.....	3-15
<b>BAB 4 PERANCANGAN SOP (<i>STANDARD OPERATING PROCEDURE</i>).....</b>	<b>4-1</b>
4.1 Persiapan Perancangan SOP(Standard Operating Procedure) .....	4-1
4.2 Perancangan Dokumen SOP (Standard Operating Procedure).....	4-1
4.2.1.1 SOP (Standard Operating Procedure) Keamanan Data Kehadiran Pegawai .....	4-1
4.2.1.2 SOP (Standard Operating Procedure) Keamanan Fisik Pengelolaan Data Kehadiran Pegawai.....	4-3
4.2.1.3 SOP Keamanan Sumber Daya Manusia .....	4-4
<b>BAB 5 PENUTUP.....</b>	<b>5-1</b>
5.1 Kesimpulan.....	5-1



5.2 Saran..... 5-1



## DAFTAR ISTILAH

<b>Aset</b>	Segala sesuatu milik organisasi yang memiliki nilai contoh: data base, file, aset perangkat lunak, aset fisik, aset yang tidak terukur (intangible)
<b>Ancaman Keamanan informasi</b>	Berbagai model serangan terhadap keamanan informasi yang berupaya untuk mengakses tanpa hak , menghilangkannya atau merusak
<b>Availability</b>	Aspek Keamanan Informasi yang menjamin pengguna dapat mengakses informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang tak bisa digunakan. Pengguna, dalam hal ini bisa jadi manusia atau komputer yang tentunya dalam hal ini memiliki otorisasi untuk mengakses informasi.
<b>Confidentiality</b>	Aspek keamanan informasi yang harus bisa menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses informasi tertentu
<b>Fasilitas Informasi</b>	Fasilitas yang terkait dengan pemrosesan Informasi yang mencakup dokumen, perangkat keras, perangkat lunak, infrastruktur, dan bangunan yang melindunginya
<b>Informasi</b>	Yang memiliki nilai sehingga merupakan sebuah aset yang perlu diamankan. Informasi tersebut diwadahi oleh fasilitas informasi
<b>Integrity</b>	Aspek keamanan informasi yang harus menjamin kelengkapan informasi dan menjaga dari korupsi, kerusakan, atau ancaman lain yang menyebabkannya berubah informasi dari aslinya
<b>Risk Analysis</b>	Kegiatan menganalisa suatu resiko untuk menentukan level resiko yang terjadi
<b>Risk Assesment</b>	Kegiatan penilaian resiko untuk menentukan nilai resiko yang dimiliki oleh suatu organisasi
<b>Risk Management</b>	Kegiatan mengelola resiko yang terdiri dari risk analysis, risk assesment, dan risk evaluation
<b>Vulnerability</b>	Kelemahan – kelemahan yang dimiliki oleh informasi.

## DAFTAR TABEL

Tabel 2.1 Format SOP Langkah Sederhana ( <i>Simple Steps</i> ) .....	2-4
Tabel 2.2 Format SOP Tahapan Berurutan ( <i>Hierarchical Steps</i> ).....	2-5
Tabel 2.3 Format SOP Grafik ( <i>Graphic</i> ) .....	2-6
Tabel 2.4 Format SOP Diagram Alir ( <i>Flowchart</i> ) .....	2-7
Tabel 2.5 Nilai Aset Berdasarkan Aspek Keamanan .....	2-17
Tabel 2.6 Identifikasi Ancaman (Threat) .....	2-18
Tabel 2.7 Identifikasi Kelemahan (vulnerability) .....	2-19
Tabel 2.8 Kriteria Nilai BIA .....	2-19
Tabel 3.1 Deskripsi dan Tangung Jawab.....	3-4
Tabel 3.2 Aturan Jam Kerja .....	3-7
Tabel 3.3 Perangkat Keras .....	3-8
Tabel 3.4 Perangkat Lunak.....	3-8
Tabel 3.5 Identifikasi Aset .....	3-9
Tabel 3.6 Perhitungan Nilai Aset .....	3-10
Tabel 3.7 Identifikasi Ancaman .....	3-10
Tabel 3.8 Identifikasi Kelemahan .....	3-11
Tabel 3.9 Kemungkinan Gangguan Keamanan (Probability of Occurrence).....	3-12
Tabel 3.10 Nilai BIA(Business Impact Analysis) Batas Toleransi Gangguan Keamanan.....	3-13
Tabel 3.11 Bobot Level Resiko Berdasarkan Probabilitas Terjadinya Ancaman .....	3-13
Tabel 3.12 Bobot Level Resiko Berdasarkan Dampak Terjadinya Resiko .....	3-13
Tabel 3.13 Matrik Level Resiko.....	3-14
Tabel 3.14 Nilai BIA Aset.....	3-14
Tabel 3.15 Nilai Resiko.....	3-14
Tabel 3.16 Evaluasi Gangguan Keamanan Informasi Terhadap Aset.....	3-15
Tabel 4.1 Persiapan Perancangan SOP(Standard Operating Procedure).....	4-1
Tabel 4.2 SOP Keamanan Data Kehadiran Pegawai .....	4-1
Tabel 4.3 SOP Keamanan Fisik Pengelolaan Data Kehadiran Pegawai .....	4-3
Tabel 4.4 SOP Sumber Daya Manusia.....	4-4




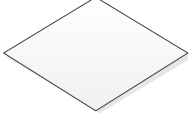

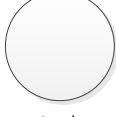



## DAFTAR GAMBAR

Gambar 1.1 Metodologi Pengerjaan Tugas Akhir .....	1-2
Gambar 2.1 CIA Keamanan Informasi (Riyanarto dan Irsyat. 2009).....	2-9
Gambar 2.2 ISO/ IEC 27000 <i>family</i> (Riyanarto dan Irsyat. 2009) .....	2-11
Gambar 2.3 Siklus PDCA (Plan-Do-Check-Act) (Riyanarto dan Irsyat. 2009).....	2-13
Gambar 2.4 Struktur Organisasi ISO/IEC 27001 (Riyanarto dan Irsyat. 2009) .....	2-14
Gambar 3.1 Kerangka Tugas Akhir.....	3-1
Gambar 3.2 Skema Analisis .....	3-2
Gambar 3.3 Alur Rekap Data Kehadiran Pegawai .....	3-3
Gambar 3.4 Struktur Organisasi Fakultas Teknik Universitas Bandung.....	3-4
Gambar 3.5 Infrastruktur Pengelolaan Data kehadiran .....	3-9

## DAFTAR LAMPIRAN

LAMPIRAN A.....	A-1
-----------------	-----

## DAFTAR SIMBOL

Nama Simbol	Deskripsi
 Connector	Tanda Panah yang menunjukkan arah aliran dari proses satu ke proses lainnya
 Proceess	Simbol untuk menunjukan sebuah langkah proses atau operasi. Umumnya menggunakan kata kerja dalam deskripsi yang singkat an jelas.
 Subprocess	Simbol untuk menunjukan bahwa dalam langkah yang dimaksud terdapat flowchart lain yang menggambarkan langkah tersebut lebih terperinci
 Decision	Simbol menunjukan sebuah langkah pengambilan keputusan. Umumnya menggunakan bentuk pertanyaan dan jawaban biasanya terdiri dari "ya" atau tidak""
 Input/output	Simbol untuk menunjukan data yang menjadi input atau output proses
 Connector (on page)	Simbol untuk menunjukan keluar / masuk proses dalam lembar atau halaman yang sama
 Off page connector	Simbol untuk menunjukan keluar / masuk proses dalam lembar atau halaman yang berbeda
 Document	Simbol ini untuk meunjukan proses atau keberadaan dokumen
 Terminator	Simbol ini menunjukan untuk awal atau akhir dari aliran proses