

**PEMBUATAN STANDARD OPERASIONAL PROSEDUR (SOP)
KEAMANAN *HARDWARE* BERDASARKAN ISO/IEC 27001:2013**

(Studi kasus : Jurusan Teknik Informatika Universitas Pasundan)

TUGAS AKHIR

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

oleh :

Kurnia Ijtihadi
NRP : 12.304.0407



**PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
JUNI 2017**

DAFTAR ISI

ABSTRAK.....	i
ABSTRACT.....	ii
KATA PENGANTAR	iii
DAFTAR ISI.....	iv
DAFTAR ISTILAH	vii
DAFTAR TABEL.....	viii
DAFTAR GAMBAR	ix
DAFTAR SIMBOL.....	x
DAFTAR LAMPIRAN	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 Pengerjaan Tugas Akhir	1-2
1.6 Sistematika Penulisan Tugas Akhir	1-3
BAB 2 LANDASAN TEORI.....	2-1
2.1 Standar Operasional Prosedur.....	2-1
2.1.1 Manfaat Standar Operasional Prosedur.....	2-1
2.1.2 Format Standar Operasional Prosedur	2-1
2.1.2.1 Jenis Format Standar Operasional Prosedur.....	2-2
2.1.2.2 Contoh Format Standar Operasional Prosedur	2-2
2.2 Teknologi Informasi	2-3
2.2.1 Infrastruktur Teknologi Informasi	2-3
2.2.1.1 Hardware	2-3
2.2.1.2 Software	2-3
2.2.2 Aset Teknologi Informasi	2-4
2.3 Keamanan Informasi	2-4
2.3.1 Fasilitas Informasi	2-4
2.3.2 Aspek Keamanan Informasi.....	2-5
2.3.3 Teknologi Keamanan Informasi	2-5
2.4 Manajemen Risiko.....	2-5
2.4.1 Analisis Risiko	2-5
2.4.2 Penilaian Risiko.....	2-6
2.4.3 Matrix Risiko.....	2-8

2.5	ISO/IEC 27001	2-8
2.5.1	Metode Pendekatan Proses	2-8
2.5.2	Keamanan Fisik	2-9
2.5.3	Klausul A.11.2 Keamanan Peralatan	2-9
2.6	Penelitian Terdahulu.....	2-9
BAB 3 SKEMA PENELITIAN.....		3-1
3.1	Kerangka Tugas Akhir	3-1
3.2	Peta Analisis.....	3-2
3.3	Analisis.....	3-4
3.3.1	Analisis Solusi.....	3-4
3.3.2	Analisis Penggunaan Konsep.....	3-4
3.3.3	Analisis Relevansi Solusi	3-5
3.3.4	Analisis Manfaat Tugas Akhir	3-5
3.4	Objek dan Kerangka Pemikiran Teoritis.....	3-6
3.5	Tempat dan Objek Penelitian.....	3-6
BAB 4 ANALISIS DAN PERANCANGAN		4-1
4.1	Hasil wawancara.....	4-1
4.2	Analisis.....	4-1
4.2.1	Gambaran Umum ISO/IEC 27001:2013 (A.11.2).....	4-1
4.2.2	Keadaan Fisik <i>Hardware</i> di Lingkungan Jurusan Teknik Informatika UNPAS	4-2
4.2.3	Analisis Risiko	4-4
4.2.3.1	Identifikasi Aset (Asset Identification)	4-4
4.2.3.2	Identifikasi Kelemahan (Vulnerability Identification)	4-5
4.2.3.3	Identifikasi Ancaman (Threat Identification).....	4-5
4.2.3.4	Dampak	4-6
4.2.4	Penilaian Risiko.....	4-7
4.2.4.1	Identifikasi Nilai Kelemahan	4-7
4.2.4.2	Kemungkinan Ancaman	4-7
4.2.4.3	Analisis Dampak.....	4-8
4.2.4.4	Nilai Risiko.....	4-9
4.2.5	Kesimpulan Analisis	4-10
4.3	Standar Operasional Prosedur (SOP).....	4-11
4.3.1	Penentuan Prosedur	4-11
4.3.2	Daftar Prosedur.....	4-12
4.3.3	Penyusunan Standar Operasional Prosedur (SOP).....	4-12
4.3.3.1	SOP Keamanan Fisik Hardware Switch	4-13
4.3.3.2	SOP Keamanan Fisik Hardware Router.....	4-16

4.3.3.3	SOP Keamanan Sarana Pendukung	4-19
BAB 5 KESIMPULAN DAN SARAN		5-1
5.1	Kesimpulan	5-1
5.2	Saran.....	5-1
DAFTAR PUSTAKA		
LAMPIRAN-LAMPIRAN		

DAFTAR ISTILAH

No	Istilah	Penjelasan
1	TI	Singkatan dari teknologi informasi
2	SMKI	Singkatan dari sistem manajemen keamanan informasi
3	Hardware	Perangkat keras
4	Software	Perangkat lunak atau sebuah aplikasi
5	Platform	Arsitektur <i>hardware</i> dengan sebuah kerangka kerja <i>software</i>
6	Human error	Kesalahan manusia
7	Vulnerability	Kelemahan
8	Simple	Sederhana
9	Hierarchical	Berurutan
10	Steps	Langkah
11	Flowcharts	Diagram alur
12	Asset	Kekayaan atau kepemilikan
13	Critical	Sebuah hal yang serius
14	Security	Keamanan
15	Siklus PDCA	Singkatan dari Plan-Do-Check-Act siklus yang digunakan untuk proses SMKI
16	Threat	Ancaman
17	Identifikasi	Suatu langkah untuk mengenal dan memasukan data yang ada tubuh manusia kedalam komputer seperti Sidik Jari, Iris Mata, dan diolah kedalam bentuk angka dan dimasukan kedalam komputer.

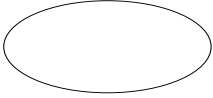
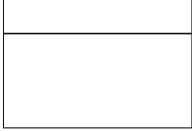



DAFTAR TABEL

Tabel 2.1 Contoh Tabel Identifikasi Nilai Kelemahan	2-6
Tabel 2.2 Contoh Tabel Identifikasi Nilai Kelemahan	2-7
Tabel 2.3 Contoh Menentukan Nilai Risiko[SAR09]	2-7
Tabel 2.4 Level Risiko [SAR09]	2-8
Tabel 2.5 Klausul A.11.2 Keamanan Peralatan[NOR13]	2-9
Tabel 3.1 Kerangka Tugas Akhir	3-1
Tabel 3.2 Langkah Analisis	3-3
Tabel 3.3 Penelitian Terdahulu	3-5
Tabel 3.4 Analisis Relevansi Solusi	3-5
Tabel 4.1 Klausul A.11.2 Keamanan Peralatan	4-1
Tabel 4.2 Hasil Observasi di Jurusan Teknik Informatika UNPAS	4-4
Tabel 4.3 Identifikasi Aset	4-4
Tabel 4.4 Identifikasi Kelemahan.....	4-5
Tabel 4.5 Identifikasi Ancaman	4-5
Tabel 4.6 Keterkaitan Identifikasi Kelemahan dan Sumber Ancaman	4-6
Tabel 4.7 Analisis Dampak	4-6
Tabel 4.8 Identifikasi Nilai Kelemahan.....	4-7
Tabel 4.9 Nilai Kelemahan yang Mungkin Terjadi	4-7
Tabel 4.10 Klasifikasi Nilai Kemungkinan Terjadi [SAR09]	4-8
Tabel 4.11 Kemungkinan Ancaman	4-8
Tabel 4.12 Klasifikasi Nilai Dampak [SAR09]	4-8
Tabel 4.13 Analisa Dampak	4-9
Tabel 4.14 Nilai Risiko	4-10
Tabel 4.15 Daftar Kode SOP.....	4-12

DAFTAR GAMBAR

Gambar 1.1 Metodologi Penelitian.....	1-3
Gambar 2.1 Contoh Format SOP.....	2-2
Gambar 3.1 Peta Analisis Tugas Akhir	3-3
Gambar 3.2 Diagram <i>Fishbone</i>	3-6
Gambar 4.1 <i>Switch</i> di Basement (<i>Switch A</i>).....	4-2
Gambar 4.2 <i>Switch</i> di Basement (<i>Switch B</i>).....	4-2
Gambar 4.3 <i>Switch</i> di Ruang Server (<i>Switch C</i>).....	4-3
Gambar 4.4 <i>Switch</i> di Ruang Server (<i>Switch D</i>).....	4-3
Gambar 4.5 <i>Router</i> di Ruang Server (<i>Router A</i> dan <i>Router B</i>)	4-3
Gambar 4.6 <i>Switch</i> dan <i>Router</i> di Ruang Lab SB604 (<i>Switch F</i>),(<i>Router C</i>).....	4-3
Gambar 4.7 <i>Switch</i> di Ruang Jurusan (<i>Switch E</i>)	4-3
Gambar 4.8 <i>Switch</i> di Ruang Lab SB603 (<i>Switch G</i>)	4-3
Gambar 4.9 <i>Switch</i> dan <i>router</i> di Ruang Lab SB601 (<i>Switch H</i> dan <i>Router D</i>)	4-3

DAFTAR SIMBOL

No.	Simbol	Deskripsi
1		Menggambarkan masukan (<i>input</i>) untuk melakukan analisis dan menggambarkan keluaran (<i>output</i>) yang peroleh dari hasil analisis.
2		Menggambarkan bagian, elemen, atau objek yang dianalisis dari sistem yang sedang digunakan, yang didalamnya terdapat langkah-langkah analisis yang dilakukan.
3		Menggambarkan langkah atau kegiatan analisis yang dilakukan untuk menghasilkan keluaran (<i>output</i>)
4		<i>Off page reference</i> merupakan simbol yang berfungsi untuk menggambarkan perpindahan aktifitas dari satu halaman ke halaman selanjutnya.
5		Menggambarkan arah masukan dari <i>input</i> ke langkah analisis dan dari langkah analisis ke keluaran (<i>output</i>).

DAFTAR LAMPIRAN

Lampiran A-1 Surat Izin Penelitian.....	A-1
Lampiran A-2 Hasil Wawancara	A-2
Lampiran A-3 Hasil Wawancara Nilai Risiko	A-5