PENYUSUNAN STANDAR OPERASIONAL PROSEDUR KEAMANAN *HARDWARE* BERDASARKAN PENDEKATAN ISO 27001:2005

(STUDI KASUS FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN)

TUGAS AKHIR

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

oleh :

Sandy Muhammad Bahtiar
Nrp. 12.304.0040

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
NOVEMBER 2016

LEMBAR PENGESAHAN

LAPORAN TUGAS AKHIR

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari Rabu tanggal 03 November 2016, tugas akhir dari :

Nama : Sandy Muhammad Bahtiar

Nrp : 12.304.0040

Dengan judul :

"PENYUSUNAN STANDAR OPERASIONAL PROSEDUR KEAMANAN *HARDWARE* BERDASARKAN PENDEKATAN ISO 27001:2005 (Studi Kasus Fakultas Teknik Universitas Pasundan)"

Mengetahui,

Bandung, 03 November 2016

Menyetujui,

Pembimbing Utama	Pembimbing Pendamping
(Iwan Kurniawan ST.,MT)	(Rita Rijayanti, ST., MT)

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa :

1. Tugas akhir ini adalah benar-benar asli dan belum pernah diajukan untuk mendapatkan gelar akademik, baik di Universitas Pasundan Bandung maupun di Perguruan Tinggi lainnya
2. Tugas akhir ini merupakan gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain kecuali arahan dari tim Dosen Pembimbing
3. Dalam tugas akhir ini tidak terdapat karya atau pendapat orang lain, kecuali bagian-bagian tertentu dalam penulisan laporan Tugas Akhir yang saya kutip dari hasil karya orang lain telah dituliskan dalam sumbernya secara jelas sesuai dengan norma, kaidah, dan etika penulisan karya ilmiah, serta disebutkan dalam Daftar Pustaka pada tugas akhir ini
4. Kakas, perangkat lunak, dan alat bantu kerja lainnya yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab saya, bukan tanggung jawab Universitas Pasundan Bandung

Apabila di kemudian hari ditemukan seluruh atau sebagian laporan tugas akhir ini bukan hasil karya saya sendiri atau adanya plagiasi dalam bagian-bagian tertentu, saya bersedia menerima sangsi akademik, termasuk pencabutan gelar akademik yang saya sandang sesuai dengan norma yang berlaku di Universitas Pasundan, serta perundang-undangan lainnya

.

Bandung, 03 November 2016

Yang membuat pernyataan,

Materai
6000,-

(Sandy Muhammad Bahtiar)

NRP. 12.304.0040

ABSTRAK

Perkembangan teknologi informasi (TI) semakin canggih dan meluas, penggunaan TI tersebut sudah menjadi kebutuhan dan tuntutan disetiap lembaga manapun. Pemanfaatan TI tidak terlepas dari perangkat keras *(hardware)* komputer untuk menunjang berjalannya sebuah sistem. Semakin canggih teknologi informasi terkadang tidak diikuti dengan penerapan keamanan yang memadai. Begitu pula Fakultas Teknik Universitas Pasundan belum menerapkan aturan mengenai keamanan *hardware*, sehingga organisasi atau perusahaan dihadapkan pada sejumlah ancaman yang dapat mengganggu aktifitas bahkan menyebabkan terhentinya proses bisnis.

Standar Operasional Prosedur (SOP) keamanan *hardware* disusun sebagai keamanan informasi untuk mencegah dan meminimalisir sejumlah ancaman yang dapat menimbulkan resiko di Fakultas Teknik Universitas Pasundan. Penyusunan SOP ini melalui berbagai tahapan seperti pemahaman studi literatur atau referensi, mengidentifikasi permasalahan yang terjadi terkait keamanan *hardware*, menganalisis keamanan *hardware* di tempat penelitian, melakukan penilaian resiko, melakukan analisa gap, dan penyusunan SOP yang disesuaikan dengan pendekatan standar keamanan informasi, yaitu ISO27001:2005 pada klausa A.9.2 mengenai keamanan peralatan. Tujuan dari standar pada klausa keamanan peralatan untuk mencegah kehilangan, kerusakan, pencurian atau ketidakberesan aset dan gangguan terhadap aktifitas organisasi atau perusahaan.

Penelitian ini menghasilkan rekomendasi Standar Operasional Prosedur Keamanan *Hardware* Berdasarkan Pendekatan ISO 27001:2005. SOP ini diharapkan dapat mengimbangi peningkatan pemanfaatan teknologi informasi dalam hal keamanan informasi di Fakultas Teknik Universitas Pasundan.

Kata Kunci : Teknologi Informasi, Perangkat Keras *(Hardware)*, Standar Operasional Prosedur (SOP), ISO27001.

ABSTRACT

The development of information technology (IT) is becoming more sophisticated and extends, the IT usage has become a requirement and the demands of each of any institution. IT utilization can not be separated from the hardware to support the passage of a computer system. Increasingly sophisticated information technology are sometimes not followed by the application of adequate security. Similarly, Faculty of Engineering, University of Pasundan have not implemented rules regarding security hardware, so organizations or companies faced with a number of threats that could disrupt the activity even cause the cessation of the business process.

Standard Operating Procedure (SOP) security hardware is structured as security information to prevent and minimize the number of threats that could pose a risk in the Faculty of Engineering, University of Pasundan. the literature study or reference, identify the problems that occur related to security hardware, analyze the security of the hardware in the study, commit risk assessment, perform a gap analysis, and preparation of SOP customized approach to information security standards, namely ISO27001: 2005 in clause A.9.2 about the security equipment. The purpose of the standard equipment safety clause to prevent loss, damage, theft or irregularities assets and disruption to the activities of the organization or company.

This study generates recommendations Security Hardware Standard Operating Procedures Based Approach ISO 27001: 2005. SOP is expected to balance the increased use of information technology in terms of information security at the Faculty of Engineering, University of Pasundan.

Keywords: Information Technology, Hardware , Standard Operating Procedures (SOP), ISO27001.

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Assalamualaikum, Wr. Wb.

Puji syukur kehadirat Allah SWT karena berkat rahmat dan karunia-Nya, penulis dapat menyelesaikan laporan TUGAS AKHIR yang berjudul " PENYUSUNAN STANDAR OPERASIONAL PROSEDUR KEAMANAN *HARDWARE* BERDASARKAN PENDEKATAN *ISO* 27001:2005 ", untuk memenuhi syarat menyelesaikan matakuliah Tugas Akhir pada Program Studi Teknik Informatika.

Pada kesempatan yang baik ini, tak lupa penulis mengucapkan terimakasih kepada semua pihak yang telah memberikan bimbingan, pengarahan, nasehat dan pemikiran dalam penulisan laporan Tugas Akhir ini, terutama kepada :

1. Ibu Dr. Ayi Purbasari, ST., MT selaku Ketua Program Studi Teknik Informatika Universitas Pasundan.
2. Bapak Iwan Kurniawan, ST., M.T dan Ibu Rita Rijayanti, ST.,MT selaku pembimbing yang telah memberikan bimbingan, nasehat, pengarahan serta motivasi pada penelitian Tugas Akhir ini.
3. Seluruh Dosen Fakultas Teknik Universitas Pasundan khususnya bagian PUSDATIN dan Akademik Pengajaran yang telah memberikan ilmu pengetahuan dan bimbingannya.
4. Keluarga tercinta, Ayah, Ibu, adik-adikku serta keluarga besar yang telah memberikan dukungan moral maupun material yang tak ternilai harganya.
5. Sahabat-sahabatku terutama Santika Dewi Purwantin, Didik Kurniawan, Yuda Ardiyana, Yuhsyar Hariwijaya ST, Andreas Andryawan, Aditya Eka Putra ST., Andri Nurul, Hanif Firdaus, Arif Busthomi, Opik Sutisna, Ricky Mulyawan, Aziz F, Afif A, Rivaldi F, Tio GP, Tanto R, Rizky AF, Cahya Pangestu ST., dan kawan-kawanku yang telah memberikan dorongan dan masukan serta bantuan moril maupun materil.
6. Semua pihak yang membantu dukungan moril maupun materil pada pengerjaan Tugas Akhir ini.

Dalam penulisan laporan Tugas Akhir ini, tentunya masih jauh dari sempurna. Hal ini dikarenakan keterbatasan pengetahuan yang dimiliki. Oleh karena itu, dalam rangka melengkapi dan membangun kearah yang lebih baik, kritik dan saran sangat diperlukan.

Semoga penelitian ini dapat bermanfaat bagi kita khususnya bagi penulis.

Wassalamualaikum Wr.Wb

Bandung, 03 November 2016

Penulis

DAFTAR ISI

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR i
ABSTRAK ii
ABSTRACT iii
KATA PENGANTAR iv
DAFTAR ISI vi
DAFTAR ISTILAH viii
DAFTAR TABEL ix
DAFTAR GAMBAR x
DAFTAR LAMPIRAN xii
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 1-3
1.6. Sistematika Penulisan Tugas Akhir 1-5
BAB 2 LANDASAN TEORI 2-1
2.1. Penelitian Terdahulu 2-1
2.2. Standar Operasional Prosedur 2-1
2.2.1. Manfaat Standar Operasional Prosedur 2-1
2.2.2. Jenis Standar Operasional Prosedur 2-1
2.2.3. Format Standar Operasional Prosedur 2-2
2.2.4. Unsur Prosedur 2-2
2.3. Teknologi Informasi 2-3
2.3.1. Aset Teknologi Informasi 2-3
2.3.2. Infrastruktur Teknologi Informasi 2-3
2.3.3. Perangkat Komputer 2-4
2.4. Kejahatan Dibidang Teknologi Informasi 2-4
2.4.1. Kejahatan Komputer 2-5
2.4.2. Kejahatan Internet 2-5
2.4.3. Karakteristik Kejahatan 2-5
2.5. Keamanan Informasi 2-5
2.5.1. Fasilitas Informasi 2-5
2.5.2. Aspek Keamanan Informasi 2-6
2.5.3. Teknologi Keamanan Informasi 2-7
2.6. Manajemen Risiko 2-7

2.6.1. Ancaman 2-7
2.6.2. Penilaian Risiko 2-8
2.6.3. Matrix Risiko 2-9
2.7. ISO/IEC 27001 2-9
2.7.1. Alasan Pemilihan ISO/IEC 27001 2-10
2.7.2. Metode Pendekatan Proses 2-10
2.7.3. Struktur Organisasi ISO/IEC 27001 2-11
2.7.4. Keamanan Fisik 2-12
2.7.5. Klausul 9.2 Keamanan Peralatan 2-12
BAB 3 ANALISIS 3-1
3.1. Kerangka Tugas Akhir 3-1
3.2. Skema Analisis 3-2
3.3. Keadaan Fisik *Hardware* di Lingkungan FT UNPAS 3-3
3.4. Penilaian Resiko 3-5
3.4.1. Identifikasi Aset (*Asset Identifications*) 3-6
3.4.2. Identifikasi Ancaman (*Threat*) 3-6
3.4.3. Identifikasi Kelemahan (*Vulnerability*) 3-7
3.4.4. Kemungkinan Ancaman (*Probability*) 3-7
3.4.5. Analisa Dampak (*Impact*) 3-8
3.4.6. Nilai Resiko 3-9
3.4.7. Peringkat Nilai Resiko 3-10
3.4.8. Kesimpulan 3-11
BAB 4 PERANCANGAN 4-1
4.1. Analisis Gap 4-1
4.2. Standar Operasional Prosedur 4-3
4.2.1. Penentuan Prosedur 4-3
4.2.2. Daftar Prosedur 4-6
4.3. Penyusunan Standar Operasional Prosedur (SOP) 4-6
4.3.1. SOP Keamanan fisik hardware Komputer dan Perangkatnya 4-6
4.3.2. SOP Keamanan Fisik Mesin Fingerprint 4-13
4.3.3. SOP Keamanan Fisik Printer 4-16
4.3.4. 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

DAFTAR ISTILAH

NO	DAFTAR ISTILAH	KETERANGAN
1	Komputer (*PC*)	Alat yang dipakai untuk mengolah data menurut prosedur yang telah dirumuskan.
2	Mesin *Fingerprint*	Jenis mesin absensi biometrik yang menggunakan metode kehadiran / absensi karyawan dengan mendeteksi sidik jari.
3	*Printer*	Merupakan salah satu hardware output komputer yang berfungsi mencetak yang tampil dilayar monitor menjadi tampilan di lebar kertas.
4	*Peripheral*	Komponen tambahan yang berfungsi untuk mendukung kerja komputer sehingga fungsi kerja komputer menjadi maksimal.
5	*Media penghubung (kabel)*	Media untuk menyalurkan listrik(kabel listrik). Media untuk menyalurkan
6	*CCTV*	Perangkat yang digunakan untuk mengawasi dan merekam segala bentuk aktifitas dalam suatu area / lokasi
7	*Wiretapping*	Kegiatan menyadap pembicaraan melalui telepon maupun melalui internet,yang dilakukan oleh orang lain.
8	*Sabotase*	Tindakan pengrusakan yang dilakukan secara terencana, disengaja dan tersembunyi terhadap peralatan
9	*Aset*	Segala sesuatu milik organisasi yang mempunyai nilai
10	*Hardware*	peralatan fisik yang membentuk suatu sistem komputer dan segala perlengkapan yang berhubungan dengannya
11	*Risk / Risiko*	Peluang terjadinya sesuatu yang dapat memberikan dampak atau mengakibatkan terganngunya proses bisnis organisasi
12	*Staff/petugas*	Mereka yang memiliki tanggung jawab sebagai pemikir, perencana, pelaksana dan pengendali jalannya perusahaan
13	*Teknis*	Situasi yang bersifat teknis
14	*Standar Operasional Prosedur (SOP)*	Serangkaian instruksi tertulis yang dibakukan mengenai berbagai proses penyelenggaraan aktivitas organisasi
15	*Security/keamanan*	Kondisi yang terbebas dari ancaman atau bahaya

DAFTAR TABEL

Tabel 1. 1 Klausul 1-3
Tabel 2. 1 Penelitian Terdahulu 2-1
Tabel 3. 1 Kerangka Tugas Akhir 3-1
Tabel 3. 2 Skema Analisis 3-2
Tabel 3. 3 Penjelasan Skema Analisis 3-3
Tabel 3. 4 Kategori Pemakai Komputer 3-3
Tabel 3. 5 Keadaan Fisik *Hardware* FT UNPAS 3-5
Tabel 3. 6 Identifikasi Aset 3-6
Tabel 3. 7 Identifikasi Ancaman 3-6
Tabel 3. 8 Identifikasi Kelemahan 3-7
Tabel 3. 9 Klasifikasi Nilai Kemungkinan Terjadi [HAY13] 3-8
Tabel 3. 10 Kemungkinan Ancaman 3-8
Tabel 3. 11 Klasifikasi Nilai Dampak [HAY] 3-9
Tabel 3. 12 Analisa Dampak 3-9
Tabel 3. 13 Nilai Resiko 3-10
Tabel 3. 14 Peringkat Nilai Resiko 3-11
Tabel 4. 1 Analisis Gap 4-1
Tabel 4. 2 Daftar Prosedur 4-6
Tabel C. 1 Hasil Pengamatan Ancaman C-1
Tabel C. 2 Pengamatan Sumber Ancaman C-2
Tabel C. 3Analisa Resiko C-2

DAFTAR GAMBAR

Gambar 1. 1 Skema 1-3
Gambar 2. 1 Contoh Format SOP 2-2
Gambar 2. 2 Aspek Keamanan Informasi[SAR09] 2-6
Gambar 2. 3 Level Resiko [HAY13] 2-9
Gambar 2. 4 Model PDCA dalam aplikasi proses SMKI[BAD09] 2-10
Gambar 2. 5 Struktur Organisasi ISO/IEC 27001[SAR09] 2-11
Gambar 3. 1 Komputer Di Ruangan SBAP 3-4
Gambar 3. 2 Komputer Di Ruangan SBAP(2) 3-4
Gambar 3. 3 Komputer Di Ruangan SSC 3-4
Gambar 4. 1 SOP Penempatan Komputer dan Perangkat 4-7
Gambar 4. 2 SOP Penggunaan Komputer dan Perangkat 4-8
Gambar 4. 3 SOP Pemeliharaan Komputer dan Perangkat 4-9
Gambar 4. 4 SOP Pemeliharaan Komputer dan Perangkat(2) 4-10
Gambar 4. 5 SOP Pembuangan Komputer dan Perangkat 4-11
Gambar 4. 6 SOP Penggunaan kembali perangkat komputer 4-12
Gambar 4. 7 SOP Penempatan Mesin Fingerprint 4-13
Gambar 4. 8 SOP Penggunaan Mesin Fingerprint 4-14
Gambar 4. 9 SOP Pemeliharaan Mesin Fingerprint 4-15
Gambar 4. 10 SOP Penempatan Printer 4-16
Gambar 4. 11 SOP Penggunaan Printer 4-17
Gambar 4. 12 SOP Pemeliharaan Printer 4-18
Gambar 4. 13 SOP Penempatan Kabel 4-19
Gambar 4. 14 SOP Pemeliharaan Kabel 4-20
Gambar 4. 15 SOP Penggunaan Catudaya Listrik Cadangan 4-21
Gambar A. 1 Surat Izin Penelitian Tugas Akhir A-1
Gambar A. 2 Surat Permohonan Izin Observasi A-2
Gambar A. 3 Memo Permohonan Izin Survei A-3
Gambar B. 1 Berita AcaraWawancara B-1
Gambar B. 2 Berita Acara Wawancara (2) B-2
Gambar B. 3 Berita Acara Wawancara (3) B-3
Gambar B. 4 Berita Acara Survei B-4
Gambar B. 5 Berita Acara Wawancara B-5
Gambar B. 6 Berita Acara Wawancara B-6
Gambar B. 7 Berita Acara Wawancara(2) B-7
Gambar B. 8 Berita Acara Wawancara B-8
Gambar C. 1 Kondisi Fisik Ruang SSC C-3

Gambar C. 2 Kondisi Fisik Ruang SSC (2) C-3
Gambar C. 3 Kondisi Fisik Ruang SBAP C-3
Gambar C. 4 Kondisi Fisik Ruang SBAP (2).....C-3
Gambar C. 5 Kondisi Fisik Ruang DHMD C C-4
Gambar C. 6 Kondisi Fisik Ruang DHMD A C-4
Gambar C. 7 Kondisi Fisik Ruang DHMD A(2).....C-4
Gambar C. 8 Kondisi Fisik Ruang DHMD B C-4
Gambar C. 9 Kondisi mesin *Fingerprint* C-4
Gambar C. 10 Kondisi Kabel C-4

DAFTAR LAMPIRAN

LAMPIRAN A A-1
A.1 Surat Izin Penelitian A-1
A.2 Surat Permohonan Izin A-2
A.3 Memo Permohonan Izin Penelitian A-3
LAMPIRAN B B-1
B.1 Berita Acara Wawancara B-1
B.2 Berita Acara Wawancara(Lampiran) B-2
B.3 Berita Acara Observasi B-4
B.4 Berita Acara Wawancara B-5
B.5 Berita Acara Wawancara B-6
LAMPIRAN C C-1
C.1 Hasil Pengamatan Ancaman C-1
C.2 Hasil Pengamatan Identifikasi Ancaman C-2
C.3 Hasil Analisa resiko C-2
C.4 Foto Kondisi Lingkungan C-3