

**PERANCANGAN KEAMANAN DATA MAHASISWA
FAKULTAS TEKNIK BERDASARKAN ISO/IEC 27001:2013
(Studi Kasus : Fakultas Teknik Universitas Pasundan Bandung)**

TUGAS AKHIR

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

oleh :

Rahayu Tiurna Andini
NRP : 13.304.0153



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

**LEMBAR PENGESAHAN
LAPORAN TUGAS AKHIR**

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari dan tanggal sidang sesuai berita acara sidang, tugas akhir dari :

Nama : Rahayu Tiurna Andini
Nrp : 13.304.0153

Dengan judul :

**“PERANCANGAN KEAMANAN DATA MAHASISWA FAKULTAS TEKNIK
BERDASARKAN ISO/IEC 27001:2013
(Studi Kasus : Fakultas Teknik Universitas Pasundan Bandung)”**

Bandung, 12 September 2017

Menyetujui,

Pembimbing Utama,

Pembimbing Pendamping,

(Doddy Ferdiansyah, ST., MT)

(Iwan Kurniawan, ST., MT)

LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

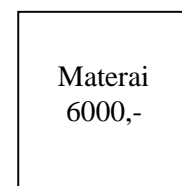
Saya menyatakan dengan sesungguhnya bahwa :

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 sanksi akademik, termasuk pencabutan gelar akademik yang saya sandang sesuai dengan norma yang berlaku di Universitas Pasundan, serta perundang-undangan lainnya

Bandung, 12 September 2017

Yang membuat pernyataan,



(**Rahayu Tiurna Andini**)

NRP. 13.304.0153

ABSTRAK

Keamanan informasi pada saat ini menjadi hal yang sangat penting terutama terhadap organisasi yang menggunakan Teknologi Informasi (TI) sebagai pendukung proses bisnisnya. Kinerja TI akan terganggu jika keamanan informasi sebagai aspek penting dari keamanan informasi mengalami masalah terkait kerahasiaannya (*confidentiality*), keutuhannya (*integrity*), dan ketersediaannya (*availability*). Keamanan informasi merupakan suatu usaha untuk memberikan rasa aman terhadap informasi dari seluruh ancaman yang mungkin terjadi, sehingga dapat menjamin kelanjutan bisnis, serta memberikan keuntungan bagi organisasi (Riyanarto dan Irsyat, 2009).

Penelitian ini dilakukan untuk dapat membantu mengurangi masalah keamanan informasi di Fakultas Teknik Unpas, sehingga dapat meminimalisir terjadinya ancaman atau risiko yang dapat membahayakan atau merugikan Fakultas Teknik Unpas. Penelitian dilakukan dengan melakukan studi literatur dan melakukan eksplorasi, serta memahami konsep-konsep keamanan informasi. Selanjutnya dilakukan analisis risiko yaitu untuk mengetahui seberapa besar risiko yang akan diterima oleh organisasi dan merancang rekomendasi keamanan data mahasiswa Fakultas Teknik Unpas yang di dalamnya memaparkan tentang mekanisme penanganan keamanan terhadap setiap ancaman yang akan mengakibatkan risiko di kemudian hari.

Hasil akhir dari penelitian ini adalah sebuah rekomendasi keamanan data mahasiswa Fakultas Teknik Unpas berdasarkan standar ISO/IEC 27001:2013.

Kata Kunci : Keamanan Informasi, Teknologi Informasi, ISO/IEC 27001:2013.

ABSTRACT

Information security at this time becomes very important for organizations that use Information Technology (IT) as a supporter of its business processes. IT performance will be disrupted if the security of confidentiality, integrity, and availability. Information security is an effort to provide a secure sense of information of all things that can happen, so as to ensure business continuity, and benefit the organization (Riyanarto and Irsyat, 2009).

This research is conducted to help reduce the problem of information security at Faculty of Engineering Unpas, so it can minimize the occurrence of threat or risk that can harm or harm the Faculty of Engineering Unpas. Research is done by conducting literature studies and exploring, as well as understanding information security concepts. Furthermore, risk analysis is done to find out how big the risks will be accepted by the organization and to design the data security recommendations of the students of the Faculty of Engineering Unpas in which describes the mechanism of handling security against any threats that will lead to risk in the future.

The end result of this research is a recommendation of data security student of Faculty of Engineering Unpas based on ISO/IEC 27001:2013 standard.

Keywords : Information Security, Information Technology, ISO/IEC 27001:2013.

KATA PENGANTAR

Bismillahirrahmaanirrahim,

Alhamdulillah puji syukur penulis panjatkan kepada kehadiran Allah SWT yang telah melimpahkan rahmat, karunia serta hidayah-Nya. Serta shalawat dan salam selalu dilimpahkan kepada junjungan Nabi Besar Muhammad SAW, sehingga penulis dapat menyelesaikan Laporan Tugas Akhir dengan judul “Perancangan Keamanan Data Mahasiswa Fakultas Teknik Berdasarkan ISO/IEC 27001:2013 (Studi Kasus : Fakultas Teknik Universitas Pasundan Bandung)”.

Pembuatan Laporan Tugas Akhir ini bertujuan untuk memenuhi salah satu syarat untuk kelulusan Program Strata 1, di Program Studi Teknik Informatika Universitas Pasundan Bandung.

Penulis menyadari laporan ini dapat terwujud berkat bantuan dan dorongan dari berbagai pihak. Penulis ucapkan terima kasih yang tak terhingga, semoga Allah memberikan balasan kepada semua pihak yang telah bersedia membantu dan memberikan kebaikan kepada penulis dalam pembuatan Laporan Tugas Akhir ini. Dalam kesempatan ini pula penulis ingin mengucapkan terima kasih kepada :

1. Allah SWT yang telah memberikan anugerah serta rahmat-Nya sehingga penulis mampu menyelesaikan Tugas Akhir ini.
2. Kepada kedua Orang Tua tercinta yang selalu memberikan do'a tiada henti, motivasi serta semangat untuk terus berprestasi.
3. Kedua Pembimbing, Bapak Doddy Ferdiansyah, ST., MT dan Bapak Iwan Kurniawan, ST., MT yang telah membimbing penulis dalam menyelesaikan Tugas Akhir ini, terima kasih banyak telah meluangkan waktu untuk memberikan bimbingan, saran, dan nasehatnya selama penyusunan Laporan Tugas Akhir ini serta telah memberikan banyak ilmu selama penulis menimba ilmu.
4. Kepada Koordinator Tugas Akhir dan Kerja Praktek, Bapak Sali Alas Majapahit, S.ST., M.Kom terima kasih banyak telah memberikan ilmu serta telah mengantarkan penulis sampai titik ini.
5. Kepada Bapak Sandra Islama Putra, S.Si selaku Ketua Pusdatin yang telah memberikan izin kepada penulis untuk melakukan penelitian Tugas Akhir di Pusdatin.
6. Kepada Bapak Ferry Mulyanto, ST., M.Kom selaku dosen wali yang selama ini telah membantu penulis dalam menangani kelancaran studi.
7. Laboratorium Teknik Informatika yang telah memberikan kesempatan kepada penulis untuk menjadi bagian dari Asisten Laboratorium Teknik Informatika, terima kasih banyak telah memberikan ilmu serta pengalaman yang sangat berharga.
8. Seluruh civitas akademika Teknik Informatika di Universitas Pasundan Bandung yang telah memberikan bekal ilmu selama penulis menimba ilmu.
9. Kepada semua sahabat-sahabat Fams yang tidak dapat penulis sebutkan satu persatu.
10. Kepada semua teman-teman seperjuangan Teknik Informatika angkatan 2013 yang tidak dapat penulis sebutkan satu persatu.
11. Serta semua pihak yang telah turut membantu dalam penyusunan Laporan Tugas Akhir ini.

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 di masa yang akan datang.

Bandung, 12 September 2017

Penulis

DAFTAR ISI

ABSTRAK	i
ABSTRACT.....	ii
KATA PENGANTAR	iii
DAFTAR ISI.....	v
DAFTAR ISTILAH	viii
DAFTAR TABEL.....	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN.....	xi
DAFTAR SIMBOL.....	xii
BAB 1 PENDAHULUAN	1-1
1.1 Latar Belakang Masalah	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 Tugas Akhir	1-3
BAB 2 LANDASAN TEORI.....	2-1
2.1 Pengertian Data.....	2-1
2.2 Pengertian Keamanan Informasi.....	2-1
2.2.1 Fasilitas Informasi.....	2-2
2.2.2 Aspek Keamanan Informasi.....	2-2
2.2.3 Metode-metode Keamanan Informasi.....	2-4
2.3 Pengertian Sistem Manajemen Keamanan Informasi	2-4
2.4 ISO/IEC 27001:2013	2-5
2.5 ISO/IEC 27001	2-5
2.5.1 Metode Pendekatan Proses ISO/IEC 27001.....	2-7
2.5.2 Struktur Organisasi ISO/IEC 27001.....	2-8
2.6 Manajemen Risiko	2-11
2.6.1 Tujuan Manajemen Risiko	2-11
2.6.2 Penilaian Risiko (<i>Risk Assessment</i>).....	2-11
2.6.2.1 Identifikasi Aset (<i>Asset Identification</i>)	2-11
2.6.2.2 Identifikasi Ancaman (<i>Threat Identification</i>).....	2-13
2.6.2.3 Identifikasi Kelemahan (<i>Vulnerability Identification</i>).....	2-13
2.6.2.4 Menentukan Kemungkinan Ancaman (<i>Probabillity of Threat</i>).....	2-14
2.6.2.5 Analisa Dampak (<i>Impact Analysis</i>)	2-14

2.6.2.6	Menentukan Nilai Risiko	2-15
2.7	Teori Peluang (Probabilitas)	2-16
2.8	NIST 800-30	2-16
2.9	Diagram Sebab dan Akibat (<i>Cause and Effect Diagram</i>)	2-17
2.9.1	Karakteristik Diagram Sebab dan Akibat.....	2-17
2.9.2	Keuntungan Diagram Sebab dan Akibat	2-18
2.10	Penelitian Terdahulu	2-18
BAB 3	SKEMA ANALISIS.....	3-1
3.1	Rancangan Penelitian.....	3-1
3.2	Analisis Masalah dan Manfaat TA.....	3-3
3.3	Analisis.....	3-4
3.3.1	Peta Analisis	3-5
3.3.2	Kerangka Pemikiran Konsep.....	3-6
3.4	Tempat dan Objek Penelitian	3-9
3.4.1	Sejarah Fakultas Teknik	3-9
3.4.2	Struktur Organisasi.....	3-10
3.4.3	Deskripsi Tugas dan Tanggung Jawab.....	3-11
3.4.4	Gambaran Umum Data Mahasiswa Fakultas Teknik Unpas.....	3-12
BAB 4	ANALISIS RISIKO	4-1
4.1	Analisis Ancaman (<i>Threat Analysis</i>) Pada Data Mahasiswa Fakultas Teknik Unpas	4-1
4.2	Analisis Kelemahan (<i>Vulnerability Analysis</i>) Pada Data Mahasiswa Fakultas Teknik Unpas	4-1
4.3	Penilaian Risiko (<i>Risk Assessment</i>).....	4-2
4.3.1	Identifikasi Aset (<i>Asset Identification</i>).....	4-2
4.3.2	Identifikasi Ancaman (<i>Threat Identification</i>) dan Identifikasi Kelemahan (<i>Vulnerability Identification</i>).....	4-3
4.3.3	Menentukan Kemungkinan Gangguan Keamanan (<i>Probability of Occurrence</i>)	4-4
4.3.4	Identifikasi Risiko (<i>Risk Identification</i>)	4-4
4.3.5	Menentukan Kemungkinan Terjadinya Risiko (<i>Likelihood</i>)	4-5
4.3.6	Identifikasi Dampak (<i>Impact Identification</i>)	4-7
4.3.7	Analisa Dampak (<i>Impact Analysis</i>)	4-8
4.3.8	Menentukan Nilai Risiko.....	4-9
BAB 5	PERANCANGAN REKOMENDASI KEAMANAN DATA MAHASISWA FAKULTAS TEKNIK UNPAS	5-1
5.1	Rekomendasi Keamanan Data Mahasiswa Fakultas Teknik Unpas	5-1
BAB 6	KESIMPULAN DAN SARAN	6-1
6.1	Kesimpulan	6-1

6.2	Saran	6-1
6.3	Rekomendasi.....	6-1

DAFTAR PUSTAKA

DAFTAR ISTILAH

No	Istilah Asing	Istilah Indonesia
1	Aset	Segala sesuatu yang memiliki nilai bagi organisasi.
2	Availability	Aspek keamanan informasi yang menjamin bahwa pengguna yang berwenang dapat mengakses informasi saat dibutuhkan.
3	Backup	Suatu proses pembuatan salinan data dari database, sehingga salinan ini dapat digunakan untuk mengembalikan data semula dari peristiwa kehilangan data ataupun kerusakan data.
4	Confidentiality	Aspek keamanan informasi yang memastikan informasi hanya dapat diakses oleh pihak yang berkepentingan.
5	Fasilitas Informasi	Fasilitas yang terkait dengan pemrosesan informasi yang mencakup dokumen, perangkat keras, perangkat lunak, infrastruktur, dan bangunan yang melindunginya.
6	IEC	Suatu standarisasi internasional nirbala yang menyiapkan dan mempublikasikan standar internasional untuk semua teknologi elektrik, elektronika, dan teknologi lain yang terkait.
7	Informasi	Informasi adalah aset, yaitu sesuatu yang memiliki nilai bagi suatu organisasi sehingga pada akhirnya perlu untuk diamankan.
8	Integrity	Aspek keamanan informasi yang menjamin keakuratan dan kelengkapan informasi dan pengolahan informasi.
9	ISO	Salah satu standar internasional dalam sebuah sistem manajemen untuk pengukuran mutu organisasi.
10	Proses Bisnis	Suatu kumpulan aktivitas atau pekerjaan terstruktur yang saling terkait untuk menyelesaikan suatu masalah tertentu atau yang menghasilkan produk atau layanan demi meraih tujuan tertentu.
11	Risk Analysis	Kegiatan menganalisa suatu risiko untuk menentukan level risiko terjadi.
12	Risk Assessment	Kegiatan penilaian risiko untuk menentukan nilai risiko yang dimiliki oleh suatu organisasi.
13	Threat	Ancaman-ancaman yang dimiliki oleh informasi.
14	Vulnerability	Kelemahan-kelemahan yang dimiliki oleh informasi.

DAFTAR TABEL

Tabel 2.1 Nilai Aset Berdasarkan Aspek Keamanan [SAR09]	2-12
Tabel 2.2 Contoh Ancaman (<i>Threat</i>) [SAR09]	2-13
Tabel 2.3 Contoh Kelemahan (<i>Vulnerability</i>) [SAR09]	2-13
Tabel 2.4 Contoh Nilai BIA [SAR09]	2-14
Tabel 2.5 Identifikasi Dampak Bisnis Jika Terjadi Kegagalan Penjagaan Aspek Keamanan Informasi [SAR09]	2-15
Tabel 2.6 Penelitian Terdahulu	2-18
Tabel 3.1 Rancangan Penelitian	3-1
Tabel 3.2 Analisis Peran Keamanan Informasi Terhadap Data Mahasiswa Fakultas Teknik Unpas	3-4
Tabel 3.3 Langkah Analisis	3-6
Tabel 3.4 Kerangka Konsep	3-7
Tabel 3.5 Sejarah Pimpinan Fakultas Teknik	3-9
Tabel 3.6 Pendirian Jurusan di Lingkungan Fakultas Teknik	3-10
Tabel 3.7 Deskripsi Tugas dan Tanggung Jawab	3-11
Tabel 3.8 Atribut Data Mahasiswa Fakultas Teknik Unpas	3-12
Tabel 4.1 Kemungkinan Ancaman	4-1
Tabel 4.2 Kemungkinan Kelemahan	4-2
Tabel 4.3 Identifikasi Aset	4-2
Tabel 4.4 Perhitungan Nilai Aset	4-3
Tabel 4.5 Identifikasi Ancaman dan Kelemahan	4-3
Tabel 4.6 Kemungkinan Gangguan Keamanan	4-4
Tabel 4.7 Identifikasi Risiko	4-5
Tabel 4.8 Level Kemungkinan Terjadinya Risiko (<i>Likelihood</i>)	4-5
Tabel 4.9 Kemungkinan Risiko	4-6
Tabel 4.10 Identifikasi Dampak [SAR09]	4-7
Tabel 4.11 Level Dampak Risiko	4-8
Tabel 4.12 Dampak Risiko	4-8
Tabel 4.13 Matriks Level Risiko [STO02]	4-10
Tabel 4.14 Nilai Risiko	4-10
Tabel 5.1 Kontrol ISO	5-1


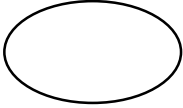
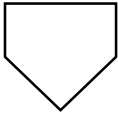

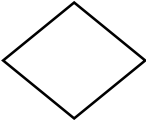
DAFTAR GAMBAR

Gambar 1.1 Metodologi Tugas Akhir	1-3
Gambar 2.1 Aspek Keamanan Informasi (Riyanarto dan Irsyat, 2009) [SAR09].....	2-4
Gambar 2.2 ISO/IEC 27000 <i>family</i> (Riyanarto dan Irsyat, 2009) [SAR09].....	2-5
Gambar 2.3 Model PDCA dalam aplikasi proses SMKI (Riyanarto dan Irsyat, 2009) [SAR09]	2-8
Gambar 2.4 Struktur Organisasi ISO/IEC 27001 (Riyanarto dan Irsyat, 2009) [SAR09].....	2-9
Gambar 2.5 Diagram Sebab dan Akibat [KEL95]	2-18
Gambar 3.1 <i>Fishbone Diagram</i>	3-4
Gambar 3.2 Peta Analisis	3-5
Gambar 3.3 Kerangka Konsep	3-7
Gambar 3.4 Struktur Organisasi	3-10

DAFTAR LAMPIRAN

Lampiran A. Surat Izin Penelitian Tugas Akhir (Pusdatin).....	A-1
Lampiran B. Surat Izin Penelitian Tugas Akhir (Wakil Dekan II).....	B-1
Lampiran C. Form Wawancara Pertemuan 1	C-1
Lampiran D. Form Wawancara Pertemuan 2	D-1
Lampiran E. Form Survey Pertemuan 3	E-1
Lampiran F. Form Wawancara Pertemuan 4.....	F-1
Lampiran G. Form Survey Pertemuan 4.....	G-1
Lampiran H. Form Wawancara Pertemuan 5	H-1

DAFTAR SIMBOL

No	Nama	Simbol	Deskripsi
1	Connector		Menggambarkan alur dari proses satu ke proses lainnya.
2	Input / Output		Menggambarkan sebuah input dan output yang saling berinteraksi dengan proses.
3	Off Page Connector		Menggambarkan keluar / masuk proses dalam lembar atau halaman yang berbeda.
4	Process		Menggambarkan sebuah langkah proses atau informasi.
5	Decision		Menggambarkan sebuah langkah pengambilan keputusan.