PERANCANGAN STANDAR OPERASIONAL PROSEDUR KEAMANAN *TELEWORKING*

(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 :

Andreas Andryawan
Nrp. 12.304.0013

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS PASUNDAN BANDUNG
SEPTEMBER 2019

LEMBAR PENGESAHAN

LAPORAN TUGAS AKHIR

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari Kamis tanggal 26 September 2019, tugas akhir dari :

Nama : Andreas Andryawan

Nrp : 123040013

Dengan judul :

"PERANCANGAN STANDAR OPERASIONAL PROSEDUR KEAMANAN *TELEWORKING* (Studi Kasus Fakultas Teknik Universitas Pasundan)"

Mengetahui,

Bandung, 26 September 2019

Menyetujui,

Pembimbing Utama

(Anggor Ari Nurcahyo ST.,M.Kom)

ABSTRAK

Keamanan informasi saat melakukan kegiatan *teleworking* haruslah dijaga. Fakultas Teknik Universitas Pasundan belum menerapkan prosedur tertulis untuk mengelola keamanan kegiatan *teleworking*, sehingga memungkinkan terjadi hal yang merugikan seperti, akses oleh pihak yang tidak berwenang, pencurian pada perangkat saat dipakai diluar intansi.

Dalam penelitian tugas ini dilakukan beberapa tahapan yaitu mengidentifikasi masalah, studi literatur, menganalisis ancaman-ancaman yang mungkin dapat mengganggu kegiatan *teleworking*, dan menyusun Standar Operasional Prosedur mengenai keamanan *teleworking*. Standar Operasional Prosedur ini dirancang untuk membantu menerapkan keamanan *teleworking* Fakultas Teknik Universitas Pasundan, sehingga dapat meminimalisir ancaman atau risiko yang membahayakan keamanan *teleworking.*

Hasil dari tugas akhir ini merupakan rekomendasi rancangan Standar Operasional Prosedur Pengamanan *teleworking* dan menghasilkan nilai risiko Berdasarkan ISO 27001:2005. Standar Operasional Prosedur ini dapat membantu Fakultas Teknik Universitas Pasundan untuk menjaga keamanan informasi, serta dapat mengurangi ancaman atau risiko yang dapat membahayakan keamanan *teleworking*.

Kata kunci: Fakultas Teknik Universitas Pasundan, Standar Operasional Prosedur, *teleworking*, Risiko, Keamanan informasi

ABSTRACT

Information security when doing teleworking activities must be maintained, The Pasundan University Faculty of Engineering has not yet implemented written procedures to manage the security of teleworking activities, making it possible for harmful things to happen like, access by unauthorized parties, theft of the device when used outside the company.

In this final project research performed several stages of identifying the problem, literature study, analyzing threats that might interfere with teleworking activities, and prepare Standard Operating Procedure. Standard Operating Procedure is designed to help implement teleworking security, in order to minimize the threat or risk teleworking security.

The results of this final project is a Standard Operating Procedures of teleworking security and the risk value result based on iso Based on ISO 27001:2005. Standard Operating Procedure may help maintaining information security, and reduce threats or risks that could endanger the teleworking security.

Keywords: Engineering Faculty Pasundan University, Standard Operating Procedures, teleworking Risk, Information Security

DAFTAR ISI

BAB 1

PENDAHULUAN

Dalam bab ini menjelaskan mengenai latar belakang, identifikasi masalah, tujuan penelitian, lingkup tugas akhir, metodologi tugas akhir, dan sistematika penulisan tugas akhir.

1.1. Latar Belakang

Perkembangan teknologi informasi semakin canggih dan meluas, penggunaan teknologi informasi saat ini sudah menjadi kebutuhan dan tuntunan disetiap instansi manapun. Maraknya penggunaan teknologi informasi menuntut sebuah perusahaan atau organisasi untuk meningkatkan produktivitas kerja dengan memanfaatkan teknologi informasi semaksimal mungkin.

Fakultas Teknik Universitas Pasundan Bandung merupakan sebuah instansi di bidang akademik yang sedang menjalankan penerapan teknologi informasi untuk meningkatkan produktivitas kegiatan akademis maupun non akademis. Kegiatan-kegiatan di lingkungan kampus Fakultas Teknik Universitas Pasundan Bandung telah di dukung dengan aplikasi berbasis *web* dimana dosen, asisten dosen, maupun para pekerja bisa melakukan transaksi-transaksi diluar instansi. Tentunya hal ini mempermudah dalam melakukan pekerjaan dimana dosen, asisten dosen, maupun para pekerja tidak selamanya harus melakukan transaksi di dalam instansinya.

Fakultas Teknik Universitas Pasundan Bandung belum menerapkan aturan yang sesuai standar untuk mengelola keamanan informasi diluar instansi. Karena pekerjaan yang menggunakan konsep *teleworking* yg dimana pekerjaan bisa di dikerjakan di luar instansi sehingga dapat menimbulkan kebocoran informasi ataupun manipulasi informasi. Perangkat yang digunakanpun perangkat milik pegawai itu sendiri, sehingga yang mengakses perangkat tidak hanya pegawai itu sendiri namun bisa juga keluarga ataupun teman dari pegawai tersebut. Keamanan informasi sangat penting untuk mengurangi terjadinya hal-hal yang dapat merugikan instansi, oleh karena itu perlu disesuaikan dengan resiko apa saja yang akan menjadi ancaman pada saat melakukan pekerjaan diluar instansi. Tentunya keamanan informasi harus mengikuti standar yang ada agar tidak menimbulkan resiko yang besar terhadap instansi.

1.2. Identifikasi Masalah

Berdasarkan uraian latar belakang masalah maka dapat disimpulkan bahwa terdapat masalah-masalah diantaranya :

1. Bagaimana merancang prosedur keamanan terhadap *teleworking* yang sesuai standar
2. Risiko yang bisa menjadi ancaman terhadap kegiatan *teleworking*

1.3. Tujuan Tugas Akhir

Tujuan dari perancangan ini adalah sebagai berikut :

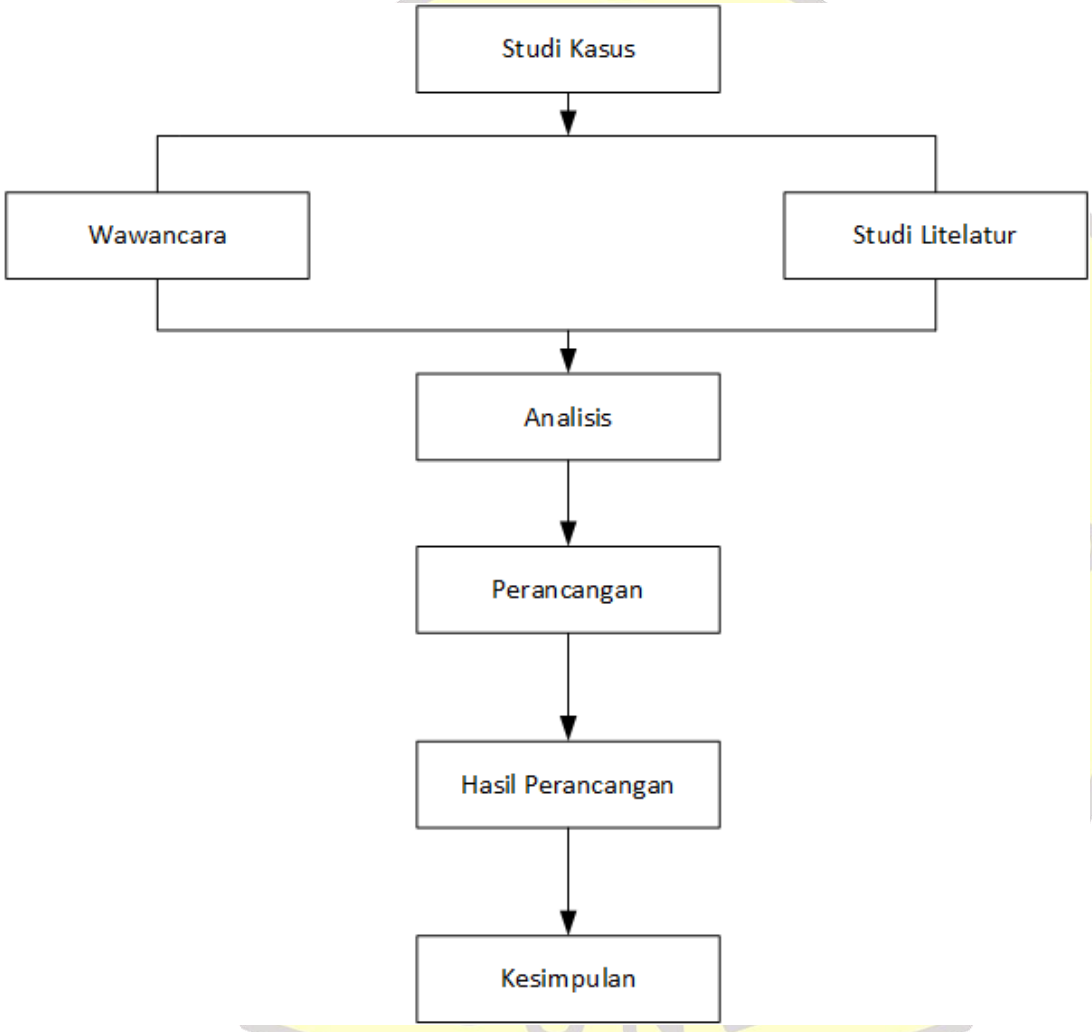
1. Menghasilkan rekomendasi standar operasional prosedur mengenai kegiatan *teleworking*
2. Menghasilkan identifikasi risiko yang menjadi ancaman terhadap kegiatan *teleworking*

1.4. Lingkup Tugas Akhir

Dari permasalahan yang timbul maka penulis membatasi beberapa permasalahan diantaranya:

1. Penelitian dilakukan di Fakultas Teknik Universitas Pasundan Bandung bagian *IT Support*
2. Mengidentifikasi resiko-resiko yang menjadi ancaman keamanan kegiatan *teleworking* pada infrastruktur teknologi informasi
3. Pendekatan yang digunakan berdasarkan pendekatan standar yang sudah diakui yaitu ISO 27001:2005 pada klausa A.11.7

1.5. Metodologi Tugas Akhir



Gambar 1.1 Skema

Untuk memperoleh data dan bahan, penulis menggunakan teknik pengumpulan data melalui:

1. Studi Kasus

   Pembahasan studi kasus pada penelitian yang akan dilakukan.

2. Studi Literatur

   Pengumpulan data dengan mengadakan studi penelaahan terhadap buku-buku, literatur-literatur, catatan-catatan dan laporan-laporan yang ada hubungannya mengenai masalah yang akan diselesaikan.

3. Wawancara

   Mengumpulkan data dengan melakukan sesi tanya jawab kepada beberapa narasumber atau pihak yang terkait di bidang teknologi informasi khususnya pada kegiatan *teleworking* di Fakultas Teknik.

4. Analisis

   Pada tahap ini mengumpulkan data-data atau fakta yang terjadi dilapangan dan dilakukan analisa terhadap data yang telah diperoleh sehingga dapat diproses untuk menghasilkan informasi yang digunakan pada tahap perancangan .

5. Perancangan

   Pada tahap ini dilakukan perancangan penelitian yang akan diselesaikan dengan menggunakan hasil analisis dan pendekatan standar yang ada. Serta disesuaikan dengan idetifikasi masalah dan tujuan penelitian.

6. Hasil Rancangan

   Hasil rancangan dari penelitian tugas akhir ini yaitu Rekomendasi Standar Operasional Prosedur Keamanan *teleworking* pada Infrastruktur Teknologi Informasi.

1.6. Sistematika Penulisan Tugas Akhir

Dalam sistematika penilisan laporan tugas akhir ini terdiri dari beberapa materi pembahasan yang saling berkaitan, yaitu :

BAB 1 PENDAHULUAN

Dalam bab ini menjelaskan mengenai latar belakang, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi pengerjaan tugas akhir, dan sistematika penulisan tugas akhir.

BAB 2 LANDASAN TEORI

Dalam bab ini berisi tentang definisi-definisi, teori-teori dan konsep yang diambil dari berbagai sumber pustaka sebagai bahan referensi untuk menganaisis gejala atau situasi yang diteliti.

BAB 3 ANALISIS

Dalam bab ini membahas tentang analisis mengenai keadaan keamanan area fisik ruang server di Fakultas Teknik Univeristas Pasundan Bandung.

BAB 4 PERANCANGAN

Dalam bab ini berisi tentang perancangan dari hasil analisis, perancangan tersebut disesuaikan dengan batasan dan kebutuhan.

BAB 5 KESIMPULAN

Dalam bab ini berisikan tentang kesimpulan dan saran yang didapat dari hasil pengerjaan tugas akhir.

BAB 5
PENUTUP

Pada bab ini terdapat dua bagian, yaitu kesimpulan yang berisi jawaban terhadap pertanyaan atau pernyataan kebutuhan yang dikemukakan sebelumnya di bab 1 tentang identifikasi masalah dan bagian saran atau usulan yang dikemukakan untuk dipertimbangkan.

5.1. Kesimpulan

Berdasarkan hasil analisis dan perancangan pada penelitian di Fakultas Teknik Universitas Pasundan bagian *IT Support* mengenai keamanan kegiatan *teleworking*, dapat disimpulkan hal-hal sebagai berikut :

1. Terdapat beberapa ancaman yang membahayakan pada kegiatan *teleworking* di Fakultas Teknik Universitas Pasundan bagian *IT Support*, dengan demikian perlunya dilakukan tindakan pencegahan terhadap ancaman tersebut.
2. Melakukan perancangan Standar Operasional Prosedur untuk mencegah dan meminimalisir terjadinya sejumlah ancaman yang dapat menimbulkan resiko terhadap keamanan kegiatan *teleworking*.
3. Penelitian ini menghasilkan rekomendasi Standar Operasional Prosedur yang diharapkan dapat mengimbangi peningkatan pemanfaatan teknologi informasi dalam hal pengamanan kegiatan *teleworking* di Fakultas Teknik Universitas Pasundan bagian *IT Support*.

5.2. Saran

Berdasarkan penelitian yang dilakukan di Fakultas Teknik Universitas Pasundan terdapat beberapa saran yang diharapkan menjadi pertimbangan untuk perbaikan dan pendukung agar hasil penelitian ini menjadi lebih baik.

Perlu penerapan keamanan informasi khususnya pada keamanan kegiatan *teleworking* sesuai standar ISO 27001 secara bertahap dan secara berkala dilakukan audit internal oleh pihak Fakultas Teknik Universitas Pasundan, hal ini untuk menjamin apakah pengelolaannya telah dilakukan dengan benar.

5.3. Rekomendasi

Untuk penelitian lebih lanjut mengenai manajemen risiko keamanan kegiatan *teleworking* dapat menggunakan semua klausul keamanan komputerisasi bergerak dan kerja di lain tempat lebih menyeluruh.yang sesuai standar ISO 27001.

DAFTAR PUSTAKA

[ABU12] Abubakar, Azwar., "Pedoman Penyusunan Standar Operasional Prosedur Admnistrasi Pemerintahan", Menteri Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi Republik Indonesia, 2012

[ARY16] Arya Sentra, "Contoh SOP, Format SOP, dan Bentuk SOP", tersedia: Agustus 2016, http://aryasentraconsulting.com/konsultasi-sop/contoh-sop-format-sop-konsultan-sop-consultant-penyusunan-sop-bisnis, Januari 2019

[BAD09] Badan Standarisasi Nasional, "Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan (SNI ISO/IEC 27001:2009)", 2009.

[DJO03] Djojosoedarso, S. "Prinsip-prinsip manajemen risiko dan asuransi", 2003.

[HAY13] Hayati, Mardhiya., Abidarin R., M.Rudyanto A., "*Risk Assessment & Business Impact Analysis* Sebagai Dasar Penyusunan DRP", STMIK Amikom, 2013.

[KEM12] Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Tahun 2012, "Pedoman Penyususnan Standar Operasional Prosedur Administrasi Pemerintahan", Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Indonesia, 2012.

[MON02] Mongkareng, Donny "ICT in Workplace (Telecommuting)", 2002.

[SAR09] Sarno, Riyanarto & Isyarf Iffano ,"Sistem Manajemen Keamanan Informasi", ITSPress, Surabaya, 2009.

[SUR10] Sutriadi. R, Marendraputra.P. "Telecommuting": Bekerja di Rumah! Optimalkan Pemanfaatan Handphone dan Internet. Opsi bagi Penyelesaian Permasalahan Kota Besar",2010.

[TAT15] Tathagati Arini, "*Step by Step* Membuat SOP *Standard Operating Procedure*", Efata Publising, Yogyakarta, 2015.