PERANCANGAN SOP (STANDAR OPERASIONAL PROSEDUR) MANAJEMEN KEAMANAN ASET INFORMASI PADA PT. GUBAH ESTETIKA TATA SINERGI (GETS ARCHITECTS) BERDASARKAN KONTROL KERANGKA KERJA ISO27002:2013

Tugas Akhir

Diajukan untuk memenuhi persyaratan mencapai derajat Sarjana Sistem Informasi

Nadia Magdalena Margaretha Sihombing

NPM: 171709492

PROGRAM STUDI SISTEM INFORMASI

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ATMA JAYA YOGYAKARTA

2020

HALAMAN PENGESAHAN

Tugas Akhir Berjudul

PERANCANGAN SOP (STANDAR OPERASIONAL PROSEDUR) MANAJEMEN KEAMANAN ASET INFORMASI PADA PT. GUBAH ESTETIKA TATA SINERGI (GETS ARCHITECTS) BERDASARKAN KONTROL KERANGKA KERJA ISO27002:2013

yang disusun oleh

NADIA MAGDALENA MARGARETHA SIHOMBING 171709492

dinyatakan telah memenuhi syarat pada tanggal 11 Januari 2021

		Keterangan
Dosen Pembimbing 1	: Putri Nastiti, S.Kom., M.Eng	Telah menyetujui
Dosen Pembimbing 2	: Putri Nastiti, S.Kom., M.Eng	Telah menyetujui
Tim Penguji		
Penguji 1	: Putri Nastiti, S.Kom., M.Eng	Telah menyetujui
Penguji 2	: Aloysius Bagas Pradipta Irianto, S.Kom., M.Eng.	Telah menyetujui
Penguji 3	: Clara Hetty Primasari, S.T., M.Cs	Telah menyetujui

Yogyakarta, 11 Januari 2021 Universitas Atma Jaya Yogyakarta Fakultas Teknologi Industri

Dekan ttd

Dr. A. Teguh Siswantoro, M.Sc

LEMBAR PERNYATAAN
Orisinalitas & Publikasi Ilmiah

Saya yang bertanda tangan di bawah ini:

Nama Lengkap	: Nadia Magdalena Margaretha Sihombing
NPM	171709492
Program Studi	: Sistem Informasi
Fakultas	: Teknologi Industri
Judul Penelitian	: Perancangan Standar Operasional Prosedur (SOP) Manajemen Keamanan Aset Informasi pada PT. Gubah Estetika Tata Sinergi (GeTs Architects) berdasarkan Kontrol Kerangka Kerja ISO27002:2013

Menyatakan dengan ini:
1. Skripsi ini adalah benar merupakan hasil karya sendiri dan tidak merupakan salinan sebagian atau keseluruhan dari karya orang lain.
2. Memberikan kepada Universitas Atma Jaya Yogyakarta, berupa Hak Bebas Royalti non eksklusif (*Non-Exclusive-Royalty-Free Right*) atas Penelitian ini, dan berhak menyimpan, mengelola dalam pangkalan data, mendistribusikan, serta menampilkan untuk kepentingan akademis, tanpa perlu meminta izin selama tetap mencantumkan nama penulis.
3. Bersedia menanggung secara pribadi segala bentuk tuntutan hukum yang mengikuti atas pelanggaran Hak Cipta dalam pembuatan Skripsi ini.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 22 Januari 2021
Yang menyatakan,

Nadia Magdalena Margaretha S
171709492

LEMBAR PERNYATAAN

Persetujuan dari Instansi Asal Penelitian

(Jika penelitian membutuhkan akses data organisasi eksternal)

Saya yang bertanda tangan di bawah ini:

Nama Lengkap Pembimbing : Lusiana Tambunan
Jabatan : Kepala Divisi
Departemen : Finance & GA

Menyatakan dengan ini:
Nama Lengkap : Nadia Magdalena Margaretha Sihombing
NPM 171709492
Program Studi : Sistem Informasi
Fakultas : Teknologi Industri
Judul Penelitian : Perancangan Standar Operasional Prosedur (SOP) Manajemen Keamanan Aset Informasi pada PT. Gubah Estetika Tata Sinergi (GeTs Architects) berdasarkan Kontrol Kerangka Kerja ISO27002:2013

1. Penelitian telah selesai dilaksanakan pada perusahaan, dan telah diaplikasikan pada sistem terkait.
2. Perusahaan telah melakukan sidang internal berupa kelayakan penelitian ini dan akan mencantumkan lembar penilaian secara tertutup kepada pihak universitas sebagai bagian dari nilai akhir mahasiswa.
3. Memberikan kepada perusahaan berupa Hak Bebas Royalti non eksklusif (*Non-Exclusive-Royalty-Free Right*) atas penelitian ini, dan berhak menyimpan, mengelola dalam pangkalan data, tanpa perlu meminta izin selama tetap mencantumkan nama penulis.

Demikianlah pernyataan ini dibuat dan dapat dipergunakan sebagaimana mestinya.

Jakarta, 28 Desember 2020
Yang menyatakan,

Lusiana Tambunan
Kepala Divisi Finance & GA

PRAKATA

Puji serta syukur penulis panjatan ke hadirat Tuhan Yang Maha Esa atas pertolongan dan penyertaan-Nya penulis dapat menyelesaikan tugas akhir yang berjudul **Perancangan Standar Operasional Prosedur (SOP) Manajemen Keamanan Aset Informasi pada PT. Gubah Estetika Tata Sinergi (GeTs Architects) berdasarkan Kontrol Kerangka Kerja ISO27002:2013**. Tugas akhir ini disusun sebagai syarat dalam kelulusan Program Studi Sistem Informasi Fakultas Teknologi Industri Universitas Atma Jaya Yogyakarta. Selama proses penyusunan tugas akhir ini tentu tidak lepas dari pihak yang telah memberikan dukungan dan bantuan kepada penulis, sehingga tugas akhir ini dapat terselesaikan dengan baik dan tepat waktu. Penulis mengucapkan terimakasih kepada :

1. Ibu Putri Nastiti, S.Kom.,M.Eng selaku dosen pembimbing yang telah mendukung dan membantu penulis dalam menyusun tugas akhir ini, terimakasih atas waktu dan motivasi yang telah diberikan kepada penulis.
2. Ibu Lusiana Tambunan selaku Kepala Divisi GA & Finance di GeTs Architects, terimakasih atas waktu dan bantuan yang sudah diberikan selama proses penelitian.
3. Bapak Gerard Tambunan selaku Pemimpin di GeTs Architects yang sudah menyediakan tempat penelitian serta dukungan kepada penulis selama proses penelitian.
4. Seluruh dosen Program Studi Sistem Informasi yang telah memberikan ilmu, motivasi, dan dukungan sehingga penulis dapat menyelesaikan tugas akhir ini.
5. Orang tua dan adik terkasih yang telah memberikan doa, semangat, bantuan, dan inspirasi kepada penulis selama masa perkuliahan dan penulisan tugas akhir ini. Tugas akhir ini saya dedikasikan kepada kedua orang tua saya atas dukungan dan doa selama ini kepada penulis.
6. Untuk teman seperjuangan I Dewa Putu Ferdy Yoga Pratama, I Putu Setyo Syahindra, dan Johannes Grant. yang selalu memberikan semangat dan

bantuan dalam melewati masa perkuliahan. Terimakasih teman-teman Angkatan 2016 dan 2017 yang sudah memberikan inspirasi dan bantuan selama masa perkuliahan.

7. Farid Noor Mahendra yang selalu memberikan semangat, bantuan, doa, dan motivasi yang berarti bagi penulis selama proses penyelesaian tugas akhir ini.
8. Seluruh pihak yang telah mendukung dan membantu penulis sehingga tugas akhir ini dapat terselesaikan dengan baik dan tepat waktu.

Penulis menyadari bahwa tugas akhir ini masih memiliki banyak kekurangan, maka dari itu mohon maaf apabila ada kesalahan atau kekeliruan dalam tugas akhir ini. Semoga tugas akhir ini dapat bermanfaat bagi seluruh pembaca.

ABSTRAK

PT. Gubah Estetika Tata Sinergi (GeTs Architects) merupakan sebuah perusahaan yang bergerak dalam bidang arsitektur. Dalam mendukung proses bisnisnya, perusahaan tentu membutuhkan teknologi informasi untuk mendukung dan memaksimalkan hasil dari proses bisnis tersebut. PT. Gubah Estetika Tata Sinergi (GeTs Architects) sudah menggunakan teknologi informasi untuk mendukung efektivitas dan efisiensi proses bisnis perusahaan. Namun, penggunaan teknologi informasi ini belum di dukung oleh prosedur manajemen aset informasi yang baik dan benar. Sehingga perusahaan sering mengalami risiko berupa kerusakan dan kegagalan sistem informasi yang menimbulkan dampak terhambatnya proses bisnis dan kerugian secara financial. Maka dalam membantu perusahaan dalam meminimalisir terjadinya risiko dan memenuhi kebutuhan perusahaan akan keamanan aset informasi diperlukan adanya SOP (standar operasional prosedur) keamanan aset informasi.

Hasil akhir yang diharapkan dalam tugas akhir ini yaitu sebuah dokumen SOP (standar operasional prosedur) manajemen keamanan aset informasi berdasarkan kontrol kerangka kerja ISO27002:2013 yang didukung dengan kebijakan dan formulir kerja. Metode yang digunakan yaitu OCTAVE untuk pendekatan dalam melakukan analisis risiko yang ada pada perusahaan lalu risiko tersebut akan diolah dan dilakukan penilaian risiko dengan menggunakan metode FMEA. Rekomendasi dan justifikasi kebutuhan kontrol atas risiko tersebut berdasarkan ISO27002:2013.

Kata kunci : Manajemen Risiko, Keamanan Aset, Standar Operasional Prosedur, ISO27002:2013.

ABSTRACT

In supporting its business processes, the company certainly needs information technology to support and maximize the results of these business processes. PT. Gubah Estetika Tata Sinergi (GeTs Architects) is a company engaged in architecture. The company has used information technology to support the effectiveness and efficiency of the company's business processes. However, the use of this information technology has not been supported by good and correct information asset management procedures. Therefore, companies often experience risks in the form of damage and failure of information systems that cause the impact of hampering business processes, decreased performance, and financial losses. So in assisting the company in minimizing the occurrence of risks and meeting the company's need for information asset security, it is necessary to have sop (standard operational procedure) for information asset security.

The expected final result in this final task is an information asset security management SOP (standard procedure) document based on ISO27002:2013 framework controls supported by policies and work forms. The method used is OCTAVE to approach in conducting risk analysis in the company and then the risk will be processed and carried out a risk assessment using the FMEA method. Recommendations and justifications for the need for control over such risks are based on ISO27002:2013.

Keyword : Risk Management, Asset Security, Standard Operating Procedure, ISO27002:2013.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi informasi kini sudah kian meningkat, seperti di Indonesia sendiri pemanfaatan teknologi informasi merupakan sebuah kebutuhan yang perannya sangat penting dalam mendukung setiap pekerjaan di segala bidang. Salah satu pemanfaatan teknologi yang cukup besar yaitu dalam bidang bisnis. Hadirnya teknologi informasi berhasil merubah setiap proses bisnis menjadi lebih efektif dan efisien. Pemanfaatan teknologi informasi sudah menjadi faktor penting untuk membantu menciptakan keunggulan kompetitif. Maka, hal ini menjadi sebuah pendorong bagi setiap bisnis untuk menjadikan keamanan aset atas informasi menjadi sesuatu yang penting untuk mendukung pemanfaatan teknologi informasi. Namun, kenyataannya tidak sedikit perusahaan yang masih kurang menaruh perhatian atas manajemen keamanan aset informasi. Saat ini, banyak dari manajemen tingkat atas perusahaan yang sering kali mengesampingkan manajemen keamanan aset informasi. Hal ini didukung dengan hasil survei yang dilakukan oleh *Information Security Breaches Surveys* (ISBS), bahwa pelanggaran keamanan informasi naik sebesar 60% pada tahun 2014 menjadi sebesar 74% persen pada tahun 2015 [1]. Selain itu index tingkat komitmen dalam keamanan sistem belum cukup tinggi, Indonesia menduduki peringkat 41 secara global serta posisinya masih dibawah Malaysia dan Singapura[2]. Kenyataannya hal tersebut belum juga meningkatkan kesadaran perusahaan khususnya perusahaan kecil dan menengah untuk pengelolaan manajemen keamanan aset informasi yang lebih baik. Perusahaan sering kali fokus pada pengelolaan sistem informasi saja, sehingga cenderung mengesampingkan masalah pengelolaan keamanan sistem informasinya.

Manajemen keamanan aset informasi hanya akan menjadi perhatian perusahaan apabila ancaman sudah terjadi. IBM melakukan sebuah survei yang melibatkan 244 pimpinan perusahaan yang ada di seluruh dunia melalui internet, dari hasil survei ini menyatakan bahwa sebesar 92% perusahaan tidak siap apabila mengalami kegagalan atau serangan baik disengaja maupun tidak disengaja [3] dan hanya sebesar 25% perusahaan yang mampu untuk menjalankan bisnis mereka apabila terkena dampak bencana [4]. Maka, seharusnya perusahaan mulai fokus dalam pengelolaan keamanan aset atas informasi, bukan hanya fokus dengan solusi teknologinya saja namun mencakup sumber daya manusia juga.

Dalam era pandemi Covid-19 saat ini, sudah banyak perusahaan yang memanfaatkan teknologi informasi untuk membantu menjalankan proses bisnis agar dapat berjalan normal tanpa harus ke kantor. Salah satunya adalah PT. Gubah Estetika Tata Sinergi (GeTs Architects) yang merupakan sebuah perusahaan bidang arsitektur. Perusahaan ini berada di Jakarta Selatan yaitu di Jl. Bungur 1 No 4 RT 002/001 Jakarta Selatan, Jakarta 12240 dan dipimpin oleh Gerard Tambunan yang merupakan seorang arsitektur. GeTs Architects mulai berdiri pada tahun 2017.

Perusahaan ini memiliki proses bisnis yaitu memasarkan desain, bertemu klien, proses pembuatan desain bangunan, proses pembangunan desain yang sudah dirancang di lapangan, memantau jalannya pembangunan, dan evaluasi. Proses bisnis ini merupakan proses utama perusahaan ini sebagai jasa arsitektur di Indonesia. Perusahaan ini bukan hanya menghasilkan desain bangunan residensial namun kini sudah melaju ke tahap desain bangunan komersial, dan proyek lainnya. Peran teknologi informasi digunakan untuk membantu arsitek dalam merancang sebuah bangunan, mengelola website, menyimpan data penting perusahaan, mencatat laporan keuangan, mencatat laporan fasilitas kantor, mencatat laporan bulanan, mencatat jadwal dan kinerja karyawan.

Namun, pemanfaatan teknologi informasi ini tidak didukung dengan manajemen keamanan manajemen aset informasi yang baik dan benar

akibatnya, perusahaan pernah mengalami hilangnya data sehingga arsitek tidak bisa mencari referensi dan memaksimalkan pelayanan apabila klien melakukan renovasi rumah, terjadinya korsleting karena kondisi kabel yang berantakan dan terlilit menyebabkan banyak kabel yang sudah terkelupas, kerusakan UPS yang disebabkan tata letak yang salah, kurangnya perhatian dari karyawan akibatnya server sering mengalami gangguan, serta tidak dilakukan *backup* berkala serta pemilihan data yang benar-benar penting.

Kontrol keamanan aset yang sudah dilakukan hanya sebatas pemasangan CCTV, pemasangan anti virus, melakukan *backup* data namun tidak berkala. Perusahaan memiliki ancaman yang berisiko untuk merusak aset informasi akibatnya biaya yang dikeluarkan perusahaan juga tidak sedikit dalam *maintenance* dan pengadaan fasilitas teknologi apabila terjadi kerusakan. Hal ini menunjukkan perlunya manajemen keamanan aset yang terdokumentasi, sesuai dengan kebutuhan perusahaan, serta sesuai dengan risiko yang mengancam perusahaan sehingga dapat meminimalisir risiko yang terjadi.

Dengan demikian, dalam membantu memberi dukungan bagi perusahaan dalam mengelola keamanan aset informasi peneliti akan menghasilkan sebuah prosedur yang terdokumentasi dengan baik dalam bentuk dokumen SOP (Standar Operasional Prosedur) keamanan aset informasi. Diharapkan SOP dapat membantu perusahaan dalam meminimalisir risiko yang mungkin terjadi. SOP sendiri dapat berguna untuk mendefinisikan seluruh konsep, teknik, dan persyaratan dalam menjalankan suatu proses yang dituliskan dalam suatu dokumen yang digunakan langsung oleh pegawai atau karyawan yang berwenang dalam menjalankan proses bisnisnya [5].

Sebelumnya sudah ada beberapa penelitian yang merancang sebuah SOP mengenai manajemen keamanan aset, seperti penelitian Dheni Indra Rachmawan mengenai SOP keamanan aset CV. Cempaka Tulung Agung yang mengacu pada kontrol kerja ISO 27002:2013 [6], penelitian Prasetya dkk yang merancang sebuah SOP keamanan sistem informasi Fakultas

Teknik Universitas Diponegoro menggunakan kerangka kerja ISO 27001 [6], penelitian Aulia Nur Fatimah yang merancang SOP keamanan data menggunakan kontrol kerangka kerja COBIT 5 dan ISO 27002:2013 [7].

Proses penelitian ini akan menggunakan kerangka kerja ISO 27002:2013 sebagai acuan dalam penerapan keamanan informasi. Dalam hal ini ISO 27002 tidak mengharuskan dalam bentuk kontrol tertentu, namun dapat menerapkan kontrol sesuai kebutuhan dengan pertimbangan hasil analisa risiko.

1.2. Perumusan Masalah

Pemanfaatan TI dalam bidang bisnis khususnya bagi perusahaan GeTs Architects terbilang meningkat. Pemanfaatan TI ini tentu dapat membantu proses bisnis perusahaan lebih efektif dan efisien. Namun, pengadaan dan pemanfaatan TI ini belum didukung dengan tingkat kesadaran atau komitmen dalam menerapkan manajemen keamanan aset informasi yang baik dan benar sehingga perusahaan yang menerapkan manajemen keamanan informasi di masih rendah, salah satunya yaitu GeTs Architects. Hal ini mengakibatkan aset informasi dan aset TI sering mengalami risiko berupa kegagalan keamanan aset informasi yang tentu berdampak pada proses bisnis perusahaan dan kerugian secara finansial. Risiko yang terjadi masih belum dapat ditangani dengan baik sehingga masih terus terjadi. Dampak dari permasalahan inilah yang dapat merugikan dan menghentikan proses bisnis perusahaan.

1.3. Pertanyaan Penelitian

Dari pemaparan perumusan di atas maka pertanyaan penelitian yang dihasilkan dari rumusan masalah diatas sebagai berikut:

1. Bagaimana hasil analisis risiko untuk keamanan aset informasi pada PT. Gubah Estetika Tata Sinergi (GeTs Architects)?
2. Bagaimana hasil perancangan dokumen SOP (Standar Operasional Prosedur) Manajemen Keamanan Aset Informasi Berdasarkan Kontrol Kerangka Kerja ISO 27002:2013 pada perusahaan PT. Gubah Estetika Tata Sinergi (GeTs Architects)?
3. Apakah hasil perancangan dokumen SOP (Standar Operasional Prosedur) Manajemen Keamanan Aset Informasi Berdasarkan Kontrol Kerangka Kerja ISO 27002:2013 pada perusahaan PT. Gubah Estetika Tata Sinergi (GeTs Architects) sudah sesuai dengan kebutuhan perusahaan?

1.4. Batasan Masalah

Dari pemaparan permasalahan diatas maka batasan masalah dalam penelitian ini sebagai berikut:

1. Pada penelitian ini yang menjadi fokus utama yaitu perancangan dokumen SOP (Standar Operasional Prosedur) Manajemen Keamanan Aset Informasi Berdasarkan Kontrol Kerangka Kerja ISO 27002:2013 pada perusahaan PT. Gubah Estetika Tata Sinergi (GeTs Architects).
2. Penelitian ini hanya mencakup aset informasi yang ada di PT. Gubah Estetika Tata Sinergi (GeTs Architects).
3. Risiko yang diberikan rekomendasi kontrol terbatas kepada risiko aset informasi yang memiliki kategori *very high, high,* dan *medium* dari hasil penilaian risiko.
4. Penelitian ini hanya sampai kepada proses perancangan sebuah dokumen SOP dan verifikasi SOP, tidak sampai kepada tahap simulasi uji coba SOP.

5. Penelitian ini menggunakan kontrol kerangka kerja dari ISO 27002:2013 sebagai pedoman dalam perancangan SOP.

1.5. Tujuan Penelitian

Berdasarkan pemaparan rumusan masalah dan pertanyaan penelitian diatas maka hasil yang akan dicapai dalam penelitian ini sebagai berikut:

1. Menghasilkan identifikasi risiko berupa gambaran risiko serta penilaian prioritas risiko yang dapat mengganggu proses bisnis perusahaan serta mengetahui penanganan yang tepat atas risiko keamanan aset informasi pada PT. Gubah Estetika Tata Sinergi (GeTs Architects).
2. Menghasilkan dokumen SOP (Standar Operasional Prosedur) Manajemen Keamanan Aset Berdasarkan Kontrol Kerangka Kerja ISO 27002:2013 pada perusahaan PT. Gubah Estetika Tata Sinergi (GeTs Architects) berdasarkan hasil analisis resiko.
3. Mengetahui hasil dari verifikasi dan validasi dokumen SOP agar dapat digunakan oleh PT. Gubah Estetika Tata Sinergi (GeTs Architects) guna mendukung manajemen keamanan aset informasi perusahaan.

1.6. Manfaat Penelitian

Bagi Keilmuan

1. Peneliti dapat berkontribusi dalam penyusunan SOP (Standar Operasional Prosedur) keamanan aset informasi menggunakan kontrol kerangka kerja ISO 27002:2013 pada perusahaan PT. Gubah Estetika Tata Sinergi (GeTs Architects).
2. Peneliti menjadi mengerti mengerti aset informasi yang penting pada perusahaan arsitektur, di mana semua aset ini merupakan pendukung utama dalam proses bisnis.

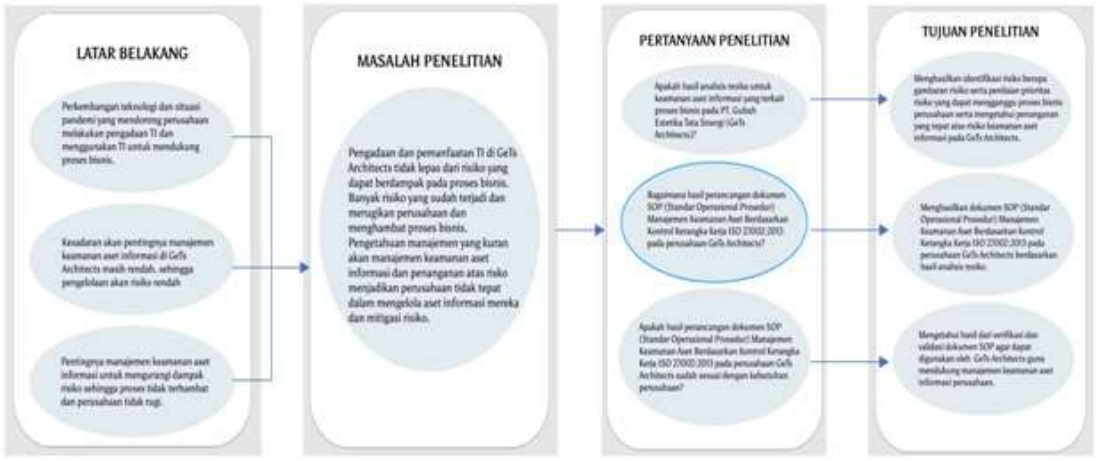
3. Peneliti mendapatkan wawasan mengenai risiko-risiko dari aset informasi pada perusahaan arsitektur.

Bagi Praktisi

1. Perusahaan mendapatkan dokumen SOP (Standar Operasional Prosedur) Manajemen Keamanan Aset Berdasarkan Kontrol Kerangka Kerja ISO 27002:2013, yang diharapkan akan menjadi pedoman bagi perusahaan dalam mengelola keamanan aset informasi.
2. Perusahaan mengetahui risisko-risiko yang dapat menghambat jalannya proses bisnis khususnya pada risiko keamanan aset informasi, serta penanganan yang tepat untuk meminimalisir risiko.

1.7. Bagan Keterkaitan

Berdasarkan pemamparan diatas maka inti dari perancangan tugas akhir ini dibuat kedalam bentuk bagan keterkaitan yang digambarkan pada bagan dibawah ini.



Gambar 1.7 Bagan Keterkaitan

BAB II
TINJAUAN PUSTAKA

2.1. Studi Sebelumnya

Dalam pengerjaan tugas akhir ini tentu terdapat beberapa penelitian yang dijadikan sebagai acuan referensi oleh peneliti, beberapa penelitian sebelumnya akan diuraikan sebagai berikut:

Tabel 2.1 Studi Sebelumnya

No	Peneliti	Tahun	Tujuan	Metode	Hasil
1.	Dea Anjani	2015	Membuat perencanaan mitigasi risiko keamanan informasi pada aplikasi Aplikasi Healty Plus Modul Rekam Medis di RSU Haji Surabaya	OCTAVE dan FMEA	Dokumen hasil dari indentifikasi risiko, analisis risiko, penilaian risiko, dan perencanaan pengelolaan mitigasi risiko
2.	Aulia Nur Fatimah	2016	Bertujuan untuk membantu dalam memanajemen pengelolaan keamanan data pada STIE PERBANAS	OCTAVE dan FMEA	Dokumen SOP keamanan data STIE PERBANAS berdasarkan kontrol kerangka kerja

			melalui perancangan SOP		COBIT 5 dan ISO27002:2013
3.	Dheni Indra Rachmawan	2017	Bertujuan dalam membantu CV Cempaka Tulungagung dalam mengelola keamanan aset informasi dengan pembuatan SOP	OCTAVE dan FMEA	Dokumen SOP keamanan aset informasi CV Cempaka Tulungagung berdasarkan kontrol kerangka kerja ISO27002:2013
4.	Apol Pribadi Subriadi dan Nina Fadilah Najwa	2019	Bertujuan dalam mengembangkan dan mengkaji kembali metode FMEA yang digunakan untuk mengukur dan penilaian risiko sehingga menjadi lebih kompleks	*Action Research Cycle*	Menghasilkan metode FMEA yang sudah dikembangkan dan sudah di uji konsitensinya dalam melakukan pengukuran dan penilaian risiko

2.2. Dasar Teori

Pada bagian ini, berisikan mengenai teori-teori yang digunakan oleh peneliti dalam pengerjaan tugas akhir ini. Adapun teori yang digunakan yakni sebagai berikut :

2.2.1. Aset

Aset merupakan sebuah sumber daya ekonomi yang dikuasai atau dimiliki oleh pemerintah akibat dari peristiwa masa lalu yang

diharapkan manfaat ekonomi dan sosial dimasa mendatang dapat diperoleh baik oleh pemerintah atau masyarakat, aset dapat diukur dengan satuan uang termaksud sumber daya non-keuangan yang dimanfaatkan dalam penyediaan jasa bagi masyarakat [8]. Aset dapat diartikan juga sebagai sumber daya yang dimiliki oleh sebuah perusahaan, dimana di dalam aset juga terdapat pembebanan yang ditunda yang dinilai sesuai prinsip ekonomi .

2.2.2. Aset Informasi

Aset informasi merupakan sebuah bagian dari aset teknologi informasi. Aset informasi juga merupakan informasi yang terdefinisi, disimpan, dikelola, serta sesuatu yang berharga bagi perusahaan. Terdapat beberapa komponen dalam sistem informasi meliputi : sumber daya manusia (*people*), perangkat lunak (*software*), perangkat keras (*hardware*), data, dan jaringan (*network*). Komponen tersebut saling berinteraksi dan membentuk satu kesatuan dalam penyediaan kebutuhan informasi serta membantu perusahaan dalam mengambil keputusan. Komponen tersebut dijabarkan sebagai berikut :

1. **Sumber daya manusia (*people*)**

   Sumber daya manusia merupakan orang yang menggunakan sistem informasi, mengoperasikan, mengelola, dan mengembangkan sistem informasi. Selain itu, sumber daya manusia juga merupakan orang yang menggunakan informasi baik dari bagian TI maupun non TI. Sumber daya manusia di GeTs Architects sendiri yaitu seluruh karyawan dan staff.

2. **Perangkat lunak (*software*)**

   Perangkat lunak (*software*) dapat diartikan sebagai sebuah instruksi yang dikirimkan pengguna yang di mana

akan dieksekusi dan mempengaruhi sistem kinerja komputer [9]. Tujuan dari perangkat lunak ini yaitu mengelola, menghitung, dan manipulasi data agar bisa menghasilkan sebuah informasi.

3. Perangkat keras (*hardware*)

Perangkat keras merupakan sebuah komponen fisik yang digunakan dalam memproses informasi serta menjalankan semua perintah yang diberikan. Perangkat keras meliputi monitor, printer, *mouse*, *keyboard*, *harddisk*, dsb. Dalam perusahaan sendiri perangkat keras bertujuan untuk penyimpanan informasi atau data penting perusahaan.

4. Data

Data merupakan sebuah fakta mentah yang belum diolah[10]. Data dalam teknologi informasi merupakan bagian dari *database*, di mana data ini disimpan dan bertujuan untuk mendukung kegiatan operasional perusahaan.

5.* Jaringan (*network)

Jaringan merupakan sebuah penghubung sejumlah perangkat agar dapat saling berkomunikasi satu sama lain. [11]. Jaringan juga bertujuan untuk memudahkan dalam berbagai informasi, membantu akses informasi, memberikan akses informasi, membantu pertukaran data, dsb secara cepat dan akurat.

2.2.3. Risiko SI/TI

Kamus Besar Bahasa Indonesia (KBBI) menjelaskan bahwa risiko merupakan sebuah akibat yang kurang menyenangkan (merugikan, membahayakan) dari sebuah tindakan atau perbuatan. Risiko juga dapat diartikan sebagai besarnya penyimpangan antara tingkat pengembalian yang diharapkan dengan tingkat pengembalian aktual[12]. Risiko juga dapat diartikan sebagai kejadian yang tidak pasti dan tidak dapat diprediksi sehingga apabila terjadi dapat menimbulkan dampak[13]. Pengaruh teknologi informasi yang kini meningkat dapat juga berpengaruh terhadap peningkatan terjadinya risiko. Risiko teknologi informasi merupakan sebuah risiko yang tidak direncanakan serta berdampak bagi aspek teknologi informasi[14]. Risiko teknologi informasi dapat berdampak buruk bagi operasional perusahaan dan dapat menimbulkan kerugian bagi perusahaan. Risiko teknologi informasi dapat dikategorikan menjadi risiko nilai atau keuntungan dalam penggunaan teknologi informasi, risiko pelaksanaan program dan proyek, dan risiko pengantaran operasional dan layanan teknologi informasi[15]. Maka perusahaan harus mampu dalam mengidentifikasi dan menganalisis semua kemungkinan terjadinya risiko agar dapat meminimalisir semua risiko yang terjadi.

2.2.4. Manajemen Risiko Teknologi Informasi

Manajemen risiko adalah rangkaian proses identifikasi risiko, penilaian risiko, mitigasi risiko, dan penyusunan rangkaian penanganan risiko agar dapat berada pada level dapat diterima oleh perusahaan [16]. Manajemen risiko dapat membantu perusahaan dalam mengindentifikasi ancaman, hambatan, dan gangguan yang dapat berpotensi menimbulkan risiko, implementasi manajemen risiko

mendukung perusahaan dalam membuat keputusan untuk mengatasi risiko sejak dini. Tujuan dari manajemen risiko sendiri yaitu melindungi aset dan meminimalisir risiko pada teknologi informasi perusahaan. Terdapat 4 katagori tindakan dalam penanganan risiko yakni :

1. ***Risk avoidance***

   Tindakan ini merupakan penanganan risiko yang bertujuan untuk menghentikan tindakan yang menyebabkan risiko terjadi.

2. ***Risk reduction***

   Tindakan ini merupakan upaya penanganan risiko yang bertujuan untuk mengurangi dampak atau kemungkinan dari risiko yang terjadi.

3. ***Risk transfer***

   Tindakan ini merupakan upaya penanganan risiko yang bertujuan untuk mengalihkan beberapa risiko melalui asuransi perusahaan.

4. ***Risk acceptance***

   Pada kasus risiko yang terlalu berdampak besar bagi perusahaan dan terbilang masih sangat ringan, maka perusahaan tidak perlu mengambil tindakan dalam penanganan risiko, melainkan menerima risiko.

Maka manajemen risiko merupakan sebuah rangkaian proses dalam pengelolaan risiko serta penanganannya, di mana bertujuan untuk mengurangi dampak dari risiko tersebut.

2.2.5. Keterkaitan Antara Keamanan Informasi dengan Risiko TI

Informasi merupakan bagian dari aset yang harus dilindungi oleh semua *stakeholder* dalam perusahaan. Tujuan dari keamanan informasi sendiri yaitu mencegah kebocoran data, kerusakan data, kehilangan data, dan manipulasi data yang berpengaruh terhadap keberlangsungan bisnis. Risiko TI sendiri merupakan risiko yang berhubungan dengan risiko operasional yang dapat berdampak pada aset informasi atau aset kritis perusahaan. Risiko TI kerap berpengaruh kepada 3 aspek utama keamanan informasi yaitu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*avaibility*). Maka, kaitan keamanan informasi dan risiko TI yaitu perusahaan dapat melindungi asetnya yaitu informasi dengan melakukan pengelolaan atas risiko TI yang ada pada ketiga aspek keamanan informasi, serta perusahaan dapat meminimalisir kerugian akibat dampak dari risiko TI khususnya dalam keamanan aset berupa informasi.

2.2.6. Pendekatan Manajemen Risiko Menggunakan Kerangka Kerja ISO 27002:2013

ISO 27001:2013 merupakan sebuah standar yang bertujuan memberikan pedoman dalam melakukan manajemen informasi untuk digunakan oleh para *stakeholder* yang bertanggung jawab dalam inisiasi, implementasi, atau pengelolaan keamanan informasi pada perusahaan. Standar ISO 27002:2013 merupakan sebuah standar yang memberikan pedoman dalam perencanaan program perlindungan aset informasi. Dalam standar ini memberikan sebuah fase dalam melakukan pendekatan untuk mengidentifikasi, menilai, dan pengelolaan risiko dalam perusahaan. Penelitian ini menggunakan kerangka kerja ISO 27002:2013 untuk proses pendekatan manajemen

risiko pada perusahaan serta pedoman dalam mengidentifikasi, menilai, dan penanganan atas risiko TI.

2.2.7. Kontrol Standar Pada Kerangka Kerja ISO 27002:2013

Pada penelitian ini kerangka kerja ISO 27002:2013 digunakan dalam pedoman pengelolaan risiko di mana pedoman tersebut disusun dalam kontrol standar yang sudah dikategorikan sesuai kebutuhan perusahaan. Berikut kontrol yang ada dalam ISO 27002:2013 [17] :

- **5** ***Security***
  - *1.1 Information security policy*
- **6** ***Organization of information security***
  - *6.1 Internal organization*
  - *6.2 Mobile devices and teleworking*
- **7** ***Human resource security***
  - *7.1 Prior to employment*
  - *7.2 During employment*
  - *7.3 Termination and change of employment*
- **8** ***Asset management***
  - *8.1 Responbility for assets*
  - *8.2 Information classification*
  - *8.3 Media handling*
- **9** ***Access control***
  - *9.1 Businness requirements of access control*
  - *9.2 User access management*
  - *9.3 User Responbilities*
- **10** ***Cryptography***
  - 10.1 *Cryptographic control*
- **11** ***Physical and environmental security***
  - *11.1 Secure areas*

11.2 Equipment

- **12** ***Operations security***
  - *12.1 Operational procedures and responbilities*
  - *12.2 Protection from malware*
  - *12.3 Backup*
  - *12.4 Logging and monitoring*
  - *12.5 Control of operational software*
  - *12.6 Technical vulnerability management*
  - *12.7 Information system audits considerstions*
- **13** ***Communications security***
  - *13.1 Network security management*
  - *13.2 Information transfer*
- **14** ***System acquisition, development, and maintenance***
  - *14.1 Security requirements of information systems*
  - *14.2 Security in development and support processes*
  - *14.3 Test data*
- **15** ***Supplier relationship***
  - *15.1 Information security in supplier relationship*
  - *15.2 Supplier service delivery management*
- **16** ***Information security incident management***
  - 16.1 *Management of information security incidents and improvements*
- **17** ***Information security aspects of business continuity management***
  - *17.1 Information security continuity*
  - *17.2 Redundancies*
- **18** ***Compliance***
  - *18.1 Compliance with legal and contractual requirements*
  - *18.2 Information Security reviews*

2.2.8. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability)

Metode OCTAVE merupakan metode yang dapat membantu organisasi dalam memilah-milah masalah teknologi untuk memahami dan mengatasi risiko keamanan informasinya. OCTAVE mendefinisikan sebuah pendekatan dalam melakukan evaluasi risiko keamanan yang komprehensif. Inti konsep dari metode OCTAVE adalah mendorong suatu organisasi untuk mengelola dan mengarahkan evaluasi risiko keamanan informasi untuk organisasi tersebut. Keamanan informasi merupakan tanggung jawab seluruh SDM yang ada dalam perusahaan bukan hanya divisi TI saja, sehingga penting bagi seluruh SDM memahami bagaimana mengakses dan menggunakan informasi tersebut. OCTAVE berfokus kepada operasional sistem atau TI digunakan untuk mendukung proses bisnis perusahaan dan bagaimana sistem dan TI tersebut memiliki potensi risiko karena ancaman keamanan. OCTAVE membantu perusahaan untuk menciptakan strategi perlindungan dan rencana mitigasi risiko untuk mengurangi risiko atas aset informasi perusahaan yang kritis. Terdapat 3 fase dalam metode OCTAVE yakni :

- **Fase 1** ***Build asset based threat profiles***

  Pada tahapan ini nantinya akan menghasilkan aset penting dalam perusahaan, kontrol keamanan informasi yang sedang dan sudah dilakukan, kekurangan dari kontrol keamanan informasi yang ada dalam perusahaan, serta kebutuhan akan keamanan informasi dalam perusahaan. Proses yang dilakukan yaitu mengidentifikasi pengetahuan dari manajemen puncak, manajemen operasional, staff, dan membuat profil ancaman yang dilakukan oleh tim analisis.

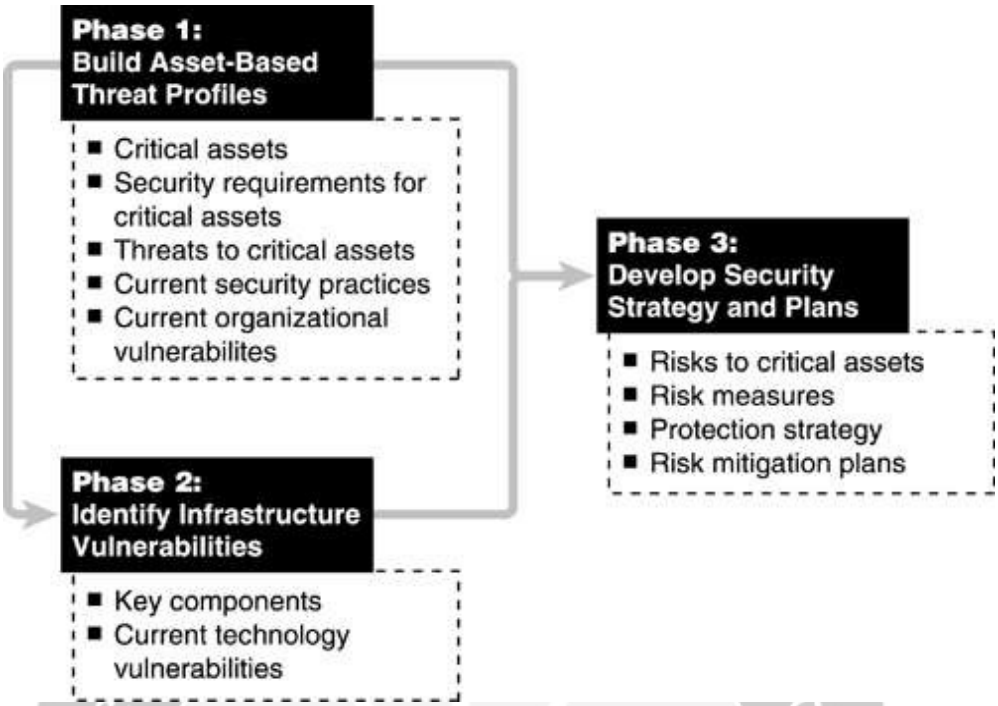
Proses pada tahapan ini dijelaskan pada gambar dibawah ini.

- **Fase 2** ***Identify infrastructure vulnerabilities***

  Pada tahapan ini akan menghasilkan daftar mengenai komponen penting dan infrastruktur teknologi informasi serta identifikasi kelemahannya. Proses yang dilakukan yakni mengidentifikasi komponen kunci dan mengidentifikasi kelemahan infrastruktur teknologi informasi yang ada dalam perusahaan.

- **Fase 3** ***Develop security strategy and plans***

  Pada tahapan ini akan menghasilkan sebuah pengukuran tingkat risiko, analisis risiko, pengelolaan penanganan atas risiko, mitigasi risiko, dan strategi keamanan. Proses yang dilakukan yakni melakukan analisis dan identifikasi terhadap risiko, lalu pengembangan strategi perlindungan terhadap aset, mitigasi risiko, dan tindakan penanganan risiko jangka pendek.



Gambar 2.2.8 Tahapan pada OCTAVE[18]

2.2.9. FMEA (*Failure Mode and Effect Analysis*)

FMEA merupakan metode yang digunakan dalam pengukuran risiko yang berfokus pada keamanan informasi dan data kritis perusahaan. FMEA membantu perusahaan dalam mengidentifikasi potensi kegagalan, penyebab kegagalan, dan perencanaan mitigasi risiko. FMEA menggunakan Teknik RPN (*risk priority number*) untuk menentukan dampak dari risiko (*severity*), kemungkinan terjadinya risiko (*occurrence*), dan peluang terjadinya risiko (*detection*). Hasil dari nilai RPN merupakan hasil perkalian dari 3 parameter diatas, di mana risiko yang memiliki nilai RPN tertinggi merupakan risiko yang harus diprioritaskan dalam pengelolaannya[19]. Tahapan dalam FMEA adalah sebagai berikut :

- Menentukan ruang lingkup penilaian risiko,
- Menentukan aset kritis yang dikategorikan sudah dikategorikan seperti perangkat keras, perangkat lunak, data, jaringan, dan SDM,

- Menentukan desain dokumen FMEA dan skala kriteria yang digunakan dalam penilaian risiko,
- Memahami dan mengerti langkah-langkah dalam menganalisis risiko dan menilai risiko dengan metode FMEA,
- Daftar risiko yang telah didapat dimasukkan ke dalam format dokumen FMEA,
- Menentukan parameter nilai *severity, occurrence,* dan *detection* pada setiap risiko yang sudah ada pada dokumen FMEA,
- Mengalkulasi nilai RPN (*risk priority number)* pada setiap risiko yang sudah diberikan parameter nilai,
- Mengurutkan risiko untuk mendapatkan hasil daftar risiko prioritas berdasarkan hasil nilai RPN,
- Menentukan dan memberikan rekomendasi penanganan dan pengelolaan pada setiap risiko.

2.2.10. SOP (Standar Operasional Prosedur)

SOP (Standar operasional prosedur) merupakan serangkaian instruksi tertulis yang mendokumentasikan kegiatan yang diikuti dalam sebuah perusahaan, SOP dapat membantu perusahaan dalam menyediakan informasi untuk melakukan pekerjaan dengan benar serta memfasilitasi dalam konsistensi dan integritas hasil akhir[20]. SOP juga dapat memberikan panduan yang terdokumentasi secara rinci dan jelas mengenai peran, tugas, dan tanggung jawab setiap individu yang ada dalam perusahaan. Penting bagi sebuah perusahaan dalam memiliki sebuah SOP sehingga setiap karyawan yang ada pada perusahaan mengerti peran dan tanggung jawabnya, di samping itu SOP membantu para pihak manajemen dalam mengambil sebuah keputusan penting

dalam perusahaan. Adapun kriteria dalam penyusunan SOP adalah [21]:

- Spesifik
- Lengkap, jelas, dan mudah dipahami
- Layak diterapkan
- *Changeable* dan *flexible*.

Penyusunan SOP harus memenuhi unsur dokumentasi dan unsur prosedur, di mana unsur dokumentasi berisikan halaman judul, daftar isi dokumen, dan deskripsi penggunaan SOP. Unsur prosedur sendiri berisikan bagian identitas seperti logo, nomor SOP, tanggal pembuatan, judul, pengesahan dokumen, dsb. Lalu, alur prosedur yaitu langkah-langkah dalam sebuah proses dalam perusahaan yang digambarkan dalam bentuk *flowchart*. Berkaitan dengan penelitian ini, maka pemaparan teori diatas digunakan sebagai pedoman dalam penyusunan dokumen SOP keamanan aset informasi pada GeTs Architects.

BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Kesimpulan pada bab ini berisikan mengenai jawaban hasil penelitian atas rumusan masalah yang sudah ditentukan dan dijabarkan pada bab sebelumnya. Kesimpulan yang didapatkan akan dipaparkan sebagai berikut.

5.1.1. Analisis Risiko Keamanan Aset Informasi PT. Gubah Estetika Tata Sinergi (GeTs Architects) berdasarkan Kontrol Kerangka Kerja ISO27002:2013.

Tahapan penelitian dalam melakukan analisis risiko keamanan aset informasi GeTs Architects dilakukan dengan menggunakan metode FMEA dan metode OCTAVE dalam melakukan pendekatan dalam mengidentifikasi risiko yang mungkin terjadi atau yang sudah terjadi pada aset informasi GeTs Architetcs. Analisis dilakukan pada 5 kategori aset yaitu perangkat keras, perangkat lunak, jaringan, data, dan sumber daya manusia, dari kelima kategori inilah didapati hasil analisis risiko dari masing-masing aset. Setiap risiko yang dianalisis akan dihitung dengan metode FMEA untuk mengetahui prioritas risiko yang memberikan dampak sangat tinggi bagi perusahaan. Dari hasil evaluasi risiko dilakukan penilaian atas risiko, didapati bahwa GeTs Architects memiliki beberapa potensi risiko yang sangat tinggi diantaranya potensi risiko kerusakan perangkat lunak dikarenakan oleh adanya virus dengan kelemahan tidak adanya perangkat anti virus, potensi risiko ini bernilai RPN 486 dan juga hilangnya data dikarenakan kelalaian dari SDM dengan kelemahan tidak adanya kontrol yang mengatur hak akses server, potensi risiko ini bernilai RPN 480. Dengan dilakukannya evaluasi risiko akan diketahui daftar risiko yang

menjadi prioritas tahap menentukan justifikasi kebutuhan dan rekomendasi kontrol untuk penanganan dan pengelolaan atas risiko.

5.1.2. Hasil Perancangan Dokumen SOP (Standar Operasional Prosedur) Manajemen Keamanan Aset Informasi Berdasarkan Kontrol Kerangka Kerja ISO 27002:2013 pada perusahaan PT. Gubah Estetika Tata Sinergi (GeTs Architects)

Berdasarkan hasil dari tahapan analisis risiko dan pengendalian risiko, dihasilkan mengenai daftar prioritas risiko yang memiliki dampak yang sangat tinggi hingga dampak sedang bagi proses bisnis perusahaan, selain itu dihasilkan pula kontrol rekomendasi atas masing-masing risiko tersebut berdasarkan kontrol kerangka kerja ISO27002:2013. Dari hasil tersebut maka didapatkan hasil usulan perancangan dokumen SOP yang terdiri dari 9 prosedur yang terdiri dari :

- SOP pemeliharaan peralatan dan ketersediaan sarana pendukung
- SOP manajemen *disaster recovery plan*
- SOP pengelolaan dan pengembangan SDM
- SOP manajemen keamanan lingkungan dan penempatan peralatan
- SOP b*ackup* data perusahaan dan pemusnahan media
- SOP manajemen keamanan terhadap *malware*
- SOP konfigurasi dan instalasi perangkat lunak
- SOP perawatan dan pengelolaan keamanan jaringan
- SOP pengelolaan keamanan hak akses server

Dari SOP tersebut memiliki dokumen pendukung berupa kebijakan dan formulir kerja yang memudahkan dalam pencatatan dalam melakukan

aktivitas manajemen keamanan aset informasi. Dokumen pendukung berupa formulir kerja tersebut terdiri dari :

- Formulir pemeliharaan peralatan TI
- Formulir perbaikan peralatan TI
- Formulir laporan kegagalan perangkat TI
- Formulir evaluasi pelatihan dan pengembangan SDM
- Formulir *backup* data
- Formulir berita acara pemusnahan media
- Formulir laporan kegagalan sistem informasi
- Formulir instalasi dan konfigurasi perangkat lunak
- Formulir pemeliharaan sistem dan aplikasi
- Formulir kontrak hak akses

Sedangkan untuk dokumen pendukung berupa kebijakan terdiri dari :

- Kebijakan pengelolaan keamanan perangkat keras dan jaringan
- Kebijakan *recovery disaster planning*
- Kebijakan pengelolaan SDM
- Kebijakan pengelolaan keamanan perangkat keras dan jaringan
- Kebijakan keamanan data dan informasi
- Kebijakan pengelolaan keamanan perangkat lunak

Seluruh hasil perancangan dokumen SOP ini akan dibukukan secara terpisah dari tugas akhir ini. Dokumen SOP ini akan menjadi produk yang akan diberikan kepada pihak GeTs Architects dengan judul Standar Operasional Prosedur (SOP) Manajemen Keamanan Aset Informasi.

5.1.3. Hasil Verifikasi Dokumen SOP (Standar Operasional Prosedur) Manajemen Keamanan Aset Informasi Berdasarkan Kontrol Kerangka Kerja ISO 27002:2013 pada perusahaan PT. Gubah Estetika Tata Sinergi (GeTs Architects)

Dokumen SOP yang dirancang akan diuji dengan melakukan verifikasi untuk memastikan bahwa perancangan dokumen SOP sudah sesuai dengan kebutuhan dan dapat dijalankan perusahaan. Verifikasi dilakukan dengan wawancara dengan kepala divisi *general affairs* dan mendapatkan hasil perubahan diantaranya :

1. **Perubahan pihak pelaksana pada keamanan kabel jaringan**.

   Pada perancangan SOP perawatan dan pengelolaan keamanan jaringan yang menjadi pihak pelaksana yaitu teknisi TI dan Kadiv GA, namun setelah dilakukan verifikasi pihak pelaksana menjadi teknisi TI digantikan oleh vendor, dimana pihak ketiga yang menyediakan dan melakukan pemeliharaan kabel jaringan pada perusahaan.

2. **Perubahan pelaksana pada alur proses persiapan melakukan *backup* data.**

   Pada perancangan dokumen SOP *backup* data perusahaan dan pemusnahan media. Pihak pelaksana pada aktivitas untuk menentukan tingkat kritikalitas data adalah karyawan dan kadiv GA. Setelah identifikasi lebih lanjut oleh kadiv GA maka perubahan untuk pelaksana dalam aktivitas tersebut hanyalah karyawan. Detail perubahan ditujukkan pada gambar dibawah ini.

Dari hasil verifikasi yang dilakukan menunjukkan bahwa dokumen SOP yang sudah dirancang sudah sesuai dengan kebutuhan perusahaan, sehingga diharapkan dapat membantu perusahaan dalam melakukan pengelolaan dan penanganan atas aset informasi.

5.2. Saran

Saran yang dapat diberikan peneliti lewat tugas akhir ini meliputi dua aspek yakni saran kepada pihak GeTs Architects dan saran bagi peneliti selanjutnya.

Saran yang dapat diberikan kepada pihak GeTs Architects yaitu :

1. Peneliti menyarankan agar dokumen SOP yang telah dirancang dan diberikan ke pihak GeTs Architects dapat benar-benar diterapkan dengan baik.
2. Peneliti menyarankan sebelum dilakukannya penerapan dokumen SOP sebaiknya dilakukan sosialisasi bagi seluruh SDM yang ada pada perusahaan.
3. Peneliti menyarankan bahwa tidak mengabaikan keamanan aset informasi perusahaan sehingga dapat mendukung proses bisnis berjalan dengan baik.
4. Peneliti menyarankan bahwa dokumen SOP dapat dikembangkan lebih lanjut menyesuaikan kebutuhan dan keadaan perusahaan.

Saran yang diberikan kepada peneliti selanjutnya yaitu :

1. Penelitian ini hanya sebatas pada tahapan pembuatan dokumen SOP dan verifikasi, tidak sampai kepada tahapan simulasi serta pemantauan implementasi dokumen SOP oleh perusahaan. Sehingga dapat dilakukan pengujian mengenai keefektifan

dokumen ini terhadap keamanan aset informasi pada GeTs Architects.

2. Dokumen ini masih dapat dikembangkan lebih lanjut menyesuaikan dengan perkembangan teknologi informasi saat ini dan kebutuhan perusahaan, sehingga perusahaan dapat terus menjalankan proses bisnisnya dengan baik.

DAFTAR PUSTAKA

[1] PWC, "Information Security Breaches Survey 2010 Technical Report," pp. 1–22, 2010.

[2] ITU, *Global Cybersecurity Index 2018*. 2019.

[3] B. Value, "Leading a sustainable enterprise," *Business*, 2009.

[4] K. Doughty, *Business continuity planning: Protecting your organization's life*. 2000.

[5] R. Stup, "Standard operational procedures: managing the human variables," *Natl. Mastit. Counc. Reg. Meet. Proceeding*, pp. 11–18, 2002.

[6] Dheni Indra Rachmawan, *Pembuatan Dokumen Sop Prosedur) Keamanan Aset Informasi Yang Mengacu Pada Kontrol Kerangka Kerja Iso 27002 : 2013 (Studi Kasus : Cv Cempaka Tulungagung) Developing Standard Operational Procedure (Sop) Document for Asset Information Security Refer To*, vol. 2013. 2017.

[7] A. N. Fatimah, "Pembuatan Dokumen Sop (Standard Operating Procedure) Keamanan Data Yang Mengacu Pada Kontrol Kerangka Kerja Cobit 5 Dan Iso27002:2013 (Studi Kasus: Stie Perbanas)," p. 300, 2016.

[8] R. Indonesia, "Peraturan Pemerintah No 71 Tahun 2010," pp. 1–413, 2010, doi: 10.1017/CBO9781107415324.004.

[9] H. Listiyono, "Fungsi Perencanaan pada Area Fungsional Jasa Informasi," *J. Teknol. Inf. Din.*, vol. XIII, no. 1, pp. 22–26, 2008.

[10] M. Mulyadi, "Transisi Data dan Informasi dalam Pengembangan Ilmu Pengetahuan," *Pustakaloka*, vol. 10, no. 1, p. 67, 2018, doi: 10.21154/pustakaloka.v10i1.1237.

[11] B. H. wanSari, Herlina, Latipa; Sudarsono, Aji; Hayadi, "Pengembangan Jaringan Local Area Network Menggunakan Sistem Operasi Linux Redhat 9," *J. Media Infotama*, vol. 9, no. 1, pp. 165–189, 2013.

[12] A. Mardhiyah, "Peranan Analisis Return Dan Risiko Dalam Investasi," *J. Ekon. Dan Bisnis Islam*, vol. 2, no. 1, pp. 1–17, 2017, doi: 10.32505/jebis.v2i1.120.

[13] D. S. dan W. H. Putri, “Manajemen Risiko dan Asuransi,” p. 98, 2017.

[14] G. Westerman and R. Hunter, “IT Risk,” *IT Risk. Harvard Bus. Sch. Press*, no. June, 2007.

[15] S. Kasus, B. Teknologi, and I. Pt, “Analisis Risiko Operasional Menggunakan Metode Cause-Effect Menggunakan Metode Cause-Effect,” pp. 1–15, 2014.

[16] G. Stoneburner, A. Goguen, and A. Feringa, “Risk Management Guide for Information Technology Systems [online]. Gaithersburg, MD: National Institute of Standards and Technology; 2002,” 2011.

[17] ISO and IEC, “Iso/Iec 27002:2005(E),” vol. 2005, pp. 25–27, 2013.

[18] C. J. Alberts and A. J. Dorofee, *Managing information security risks : the OCTAVE approach*. 2003.

[19] A. P. Subriadi and N. F. Najwa, “The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment,” *Heliyon*, vol. 6, no. 1, p. e03161, 2020, doi: 10.1016/j.heliyon.2020.e03161.

[20] M. P. Garcés Gómez, “6. Final,” *La Organ. del discurso*, no. April, pp. 155–158, 2019, doi: 10.31819/9783865278661-007.

[21] Ir . M . Budihardjo, “Judul Buku : Panduan Praktis Menyusun SOP Pengarang : Ir . M . Budihardjo Penerbit : Gadjah Mada University Press Tahun Terbit : ISBN : Tebal : 131 Halaman,” 2014.

[22] C. S. Carlson, “Failure Mode and Effects Analysis (FMEA) UNDERSTANDING THE FUNDAMENTAL DEFINITIONS AND,” *John Wiley Sons*, 2012.

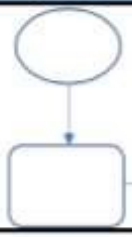
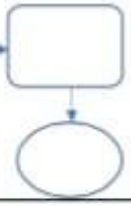
[23] Kemenpan RB RI, “Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan Kementerian Tahun 2012,” pp. 3–5, 2012.

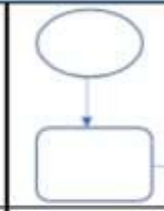
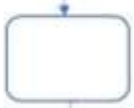
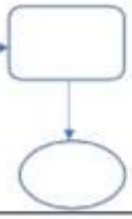
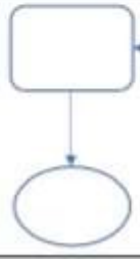
LAMPIRAN

PT. GUBAH ESTETIKA TATA SINERGI	NOMOR SOP	SOP - 01	TGL. PEMBUATAN	/ /
	PENANGGUNG JAWAB		TGL. REVISI	/ /
	NOMOR REVISI		TGL. TERBIT	/ /
	NAMA SOP	**Pemeliharaan peralatan dan ketersediaan sarana pendukung**		
	RUANG LINGKUP	Peralatan perangkat TI		

DESKRIPSI SOP	KUALIFIKASI PELAKSANA
Prosedur pemeliharaan peralatan dan ketersediaan sarana pendukung merupakan prosedur yang memastikan semua peralatan dapat digunakan tanpa ada kerusakan dan gangguan, sehingga proses bisnis dapat terus berjalan dengan baik	Memiliki pengetahuan dan keahlian dalam pengelolaan perangkat TI
TUJUAN SOP	**PERLENGKAPAN DAN PERALATAN**
Tujuan yaitu memastikan semua peralatan dapat digunakan, penjadwalan pemeliharaan peralatan dapat berjalan dengan baik, serta ketersedian sarana pendukung peralatan dapat tersedia dalam setiap proses bisnis perusahaan	
REFRENSI	**PIHAK PELAKSANA**
ISO 27002:2013 - 11.2.2 *Supporting utilities* - 11.2.4 *Equipment maintenance*	Kadiv GA, karyawan, dan teknisi TI (pihak ketiga)
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan maka akan mengakibatkan risiko berupa terhambatnya proses bisnis, penurunan kinerja, dan kerugian finansial	

KETERANGAN	DIBUAT OLEH	DISETUJUI OLEH	DISAHKAN OLEH
Nama			
Tanggal			
Tanda Tangan	(.....)	(.....)	(.....)

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Teknisi TI	Karyawan	Kadiv GA	
I.	**Proses pelaporan kerusakan peralatan TI**				
1.	Melaporkan keluhan kerusakan kepada kadiv GA				
2.	Melakukan proses pelaporan kerusakan kepada teknisi TI				
3.	Melakukan perbaikan sesuai dengan kerusakan yang dilaporkan sebelumnya				
4.	Melakukan pencatatan mengenai proses perbaikan pada form perbaikan peralatan TI				FORM/SOP/02
5.	Memastikan semua kerusakan benar-benar tertangani dengan baik dan melakukan konfirmasi kepada Kadiv GA				
6.	Melakukan uji coba selama 1 bulan untuk memastikan apakah kerusakan benar-benar tertangani atau tidak				
7.	Melakukan pencatatan form kegagalan peralatan TI				FORM/SOP/03

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Teknisi TI	Karyawan	Kadiv GA	
II.	**Proses pemeliharaan peralatan TI secara berkala**				
1.	Melakukan pemeliharaan dan kontrol peralatan TI 1 kali dalam 6 bulan				
2.	Menentukan penjadwalan untuk melakukan pemeliharaan peralatan TI				
5.	Melakukan kontrol dan memastikan semua peralatan TI apakah ada kelemahan atau tidak				
A	**Jika ada**, melakukan proses pelaporan untuk perbaikan				
B	**Jika Tidak**, melakukan pencatatan pada form pemeliharaan peralatan TI				**FORM/SOP/01**
7.	Memproses hasil dan melakukan evaluasi terhadap hasil pemeliharaan				
8.	Melakukan diskusi kepada *owner* dan Kadiv GA apabila ada perlakuan khusus yang harus dilakukan				

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. FORM	FORM/SOP/01	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA FORMULIR	Formulir pemeliharaan peralatan TI		
	PENANGGUNG JAWAB			
	WAKTU PELAKSANAAN	Tanggal :	Waktu :	

KETERANGAN PERANGKAT	
JENIS PERANGKAT TI	
JUMLAH PERANGKAT	

KETERANGAN PEMELIHARAAN	
URAIAN PEMELIHARAAN	

KONDISI PERANGKAT	
URAIAN KONDISI PERANGKAT	

Petugas Perbaikan

(Nama Lengkap)

Mengetahui,

Kepala Divisi General Affairs

(Nama Lengkap)

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. FORM	FORM/SOP/02	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA FORMULIR	Formulir perbaikan peralatan TI		
	PENANGGUNG JAWAB			
	WAKTU PELAKSANAAN	Tanggal :	Waktu :	

KETERANGAN KERUSAKAN	
URAIAN KERUSAKAN	
NAMA PERANGKAT	
ESTIMASI PERBAIKAN	

KETERANGAN PERBAIKAN	
URAIAN PERBAIKAN	

KETERANGAN PENGADAAN BARANG (Isi jika ada)	
KET. PERALATAN RUSAK	
KET. PENGADAAN PERALATAN	

Petugas Perbaikan

(Nama Lengkap)

Mengetahui,

Kepala Divisi General Affairs

(Nama Lengkap)

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. FORM	FORM/SOP/03	**TGL. REVISI**	/ /
	NOMOR REVISI	00	**TGL. TERBIT**	/ /
	NAMA FORMULIR	**Formulir laporan kegagalan perangkat TI**		
	PENANGGUNG JAWAB			
	WAKTU PELAKSANAAN	Bulan :	Tahun :	

No.	Deskripsi kegagalan	Jumlah kegagalan	Tanggal Kegagalan	Tindakan Penanganan	Tanggal Penanganan		Staff Penanganan	Status
					Mulai	Selesai		

Dibuat Oleh, Staff Divisi TI	Mengetahui, Kepala Divisi General Affairs
_____ (Nama Lengkap)	_____ (Nama Lengkap)

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. SURAT	KEB/SOP/01	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA KEBIJAKAN	Pengelolaan keamanan perangkat keras dan jaringan		
	PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan menjamin keamanan aset perangkat keras dan jaringan yang ada pada perusahaan agar dapat digunakan selama berjalannya proses bisnis tanpa adanya gangguan.

II. RUANG LINGKUP

Cakupan kebijakan ini yaitu berlaku bagi para pihak yang terkait dalam penggunaan, pengelolaan, pemeliharaan, dan pengamanan seluruh aset perangkat keras dan jaringan yang ada pada perusahaan. Adapun aset perangkat keras dan jaringan yang dimaksud terdiri dari :

- PC
- Server
- Printer
- Laptop
- *Mouse*
- *Speaker*
- *Keyboard*
- CPU
- UPS
- Proyektor

III. REFRENSI

Dalam penyusunan kebijakan ini tentu menggunakan refrensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan refrensi yaitu :

- 11.2.2 *Supporting utilities*
- 11.2.4 *Equipment maintenance*
- 11.2.1 *Equipment siting and protection*
- 11.2.3 *Cabling security*

IV. KEBIJAKAN

4.1 Pengelolaan keamanan perangkat keras

4.1.1 Segala bentuk kerusakan dan gangguan yang terjadi pada perangkat keras wajib untuk di laporkan kepada pihak yang bertanggung jawab.

4.1.2 Seluruh laporan kerusakan atau gangguan harus segera di proses dan ditangani dalam kurun waktu 2 x 24 jam oleh pihak teknisi TI.

4.1.3 Segala proses perbaikan atau pengadaan peralatan perangkat keras wajib dilakukan pencatatan dan dikonfirmasi paling lambat 1 x 24 jam oleh pihak teknisi TI.

4.1.4 Seluruh perangkat keras yang sudah rusak atau tidak digunakan kembali wajib ditempatkan di ruangan gudang penyimpanan yang sudah disediakan perusahaan.

4.1.5 Seluruh perangkat keras yang sudah rusak atau tidak digunakan kembali tidak boleh dibuang atau diperjual belikan tanpa keputusan pemusnahan media oleh perusahaan.

4.1.6 Dilarang merusak atau mengotak-atik peralatan TI secara sengaja atau tidak jika tidak diberikan izin atau arahan dari pihak teknisi TI yang bertanggung jawab.

4.1.7 Dilarang melakukan pengadaan perangkat keras tambahan jika tidak adanya izin atau perintah dari Kadiv GA.

4.1.8 Dilarang untuk membawa pulang seluruh peralatan perangkat keras dengan alasan apapun.

4.1.9 Pemeliharaan secara berkala wajib dijalankan 1 kali dalam 6 bulan dan tidak boleh menunda penjadwalan pemeliharaan yang sudah ditentukan.

4.1.10 Segala bentuk kerusakan dan pemeliharaan wajib ditangani oleh pihak yang ahli dalam perangkat keras yang ada di perusahaan.

4.1.11 Kadiv GA wajib melakukan kontrol atas proses penggunaan, perbaikan, dan pemeliharaan perangkat keras.

4.1.12 Teknisi TI yang telah ditunjuk wajib bertanggung jawab atas pemeliharaan dan perbaikan yang dilakukan, serta melakukan konfirmasi dan pencatatan pada setiap proses yang dilakukan.

4.1.13 Segala bentuk pengadaan barang wajib dikonfirmasi dan atas persetujuan *Owner* dan Kadiv GA.

4.1.14 Seluruh kegiatan pengelolaan, pemeliharaan, perbaikan, dan penggunaan perangkat keras harus sesuai dengan prosedur keamanan peralatan TI dan mengikuti kebijakan keamanan yang berlaku.

4.1.15 Peralatan TI yang ada diperusahaan hanya boleh digunakan dan dioperasikan oleh seluruh karyawan (kecuali OB) yang merupakan bagian dari perusahaan.

4.1.16 Penggunaan perangkat TI hanya boleh dilakukan pada jam kerja, apabila diluar itu harus melakukan konfirmasi izin kepada Kadiv GA.

4.1.17 Semua perangkat TI kritis dan sangat penting wajib diberikan perlindungan asuransi.

4.1.18 Seluruh perangkat TI wajib dimatikan jika sudah selesai digunakan, kecuali apabila ada kebutuhan mendesak yang mengharuskan PC tetap menyala seperti proses render desain. Namun harus melakukan konfirmasi kepada Kadiv GA

4.1.19 Dalam PC, laptop, dan server wajib dipasang sistem *log in* yang mengharuskan pengguna memasukan ID dan *password*.

4.1.20 Setiap karyawan dan Kadiv GA wajib melakukan kontrol ketersediaan sarana pendukung seperti UPS untuk memastikan proses bisnis terus berjalan.

4.1.21 Setiap perangkat TI harus memiliki perlindungan alternative, seperti adanya silikon pelindung *keyboard*, pelindung layer, dsb.

4.1.22 Apabila kerusakan dan gangguan terjadi maka seluruh karyawan wajib menerapkan kebijakan RDP dalam waktu maksimal 2 jam setelah kerusakan terjadi.

4.2 Pengelolaan keamanan lingkungan perangkat keras

4.2.1 Seluruh perangkat TI harus ditempatkan pada ruangan khusus, aman, dan layak sesuai dengan prosedur yang sudah ditentukan perusahaan.

4.2.2 Seluruh ruangan perangkat TI harus diberikan CCTV yang selalu menyala dan kunci ruangan yang dilakukan setelah jam operasional perusahaan selesai.

4.2.3 Seluruh ruangan yang berisikan aset TI harus diberikan diberikan pendingin ruangan dan sirkulasi udara yang baik untuk mencegah *overheating*.

4.2.4 Dilarang untuk memindahkan seluruh perangkat TI selain pihak yang bertanggung jawab.

4.2.5 Dilarang membawa minuman atau makanan yang bersifat cair kedalam ruangan perangkat TI.

4.2.6 Dilarang merokok dalam ruangan perangkat TI.

4.2.7 Selain staff dan karyawan GeTs Architects dilarang memasuki ruangan perangkat TI, terkecuali atas izin dari Kadiv GA.

4.2.8 Dilarang membawa peliharaan kedalam ruangan perangkat TI.

4.2.9 Ruangan perangkat TI harus selalu dirawat dan dibersihkan untuk menhindari debu dan hewan seperti tikus.

4.2.10 Ruangan perangkat TI harus mendapatkan matahari yang cukup untuk menhindari kelembapan ruangan.

4.3 Pengelolaan keamanan jaringan

4.3.1 Setiap kabel yang ada pada ruangan perangkat TI wajib diberikan pelabelan nama dan fungsi untuk memudahkan konfigurasi dan *maintenance*.

4.3.2 Setiap kabel pada ruang perangkat TI harus dilakukan pembedaan warna untuk memundahkan konfigurasi dan *maintenance*.

4.3.3 Setiap kabel yang ada pada perusahaan harus ditempatkan pada tata letak yang aman tidak terinjak-injak serta wajib diberikan perlindungan pelapisan kabel menggunakan pipa atau karet pelindung kabel.

4.3.4 Setiap kabel yang ada pada ruang perangkat TI tidak boleh terlilit dan harus tersusun dengan rapih untuk mencegah arus pendek.

4.3.5 Pihak Kadiv GA dan teknisi TI wajib melakukan kontrol jaringan dan kabel dalam waktu 1 kali dalam 6 bulan.

4.3.6 Jika ada kerusakan atau gangguan jaringan maka wajib memberikan konfirmasi kepada Kadiv GA.

4.3.7 Setiap proses pemeliharaan dan perbaikan harus dilakukan pencatatan.

4.3.8 Proses pemeliharaan dan *maintenance* wajib dilakukan oleh teknisi TI yang ahli dalam jaringan.

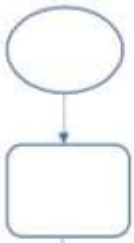
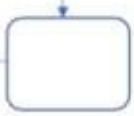
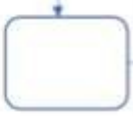
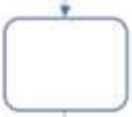
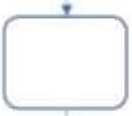
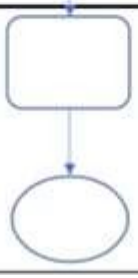
4.3.9 Dilarang menumpuk steker pada terminal listrik untuk mencegah terjadinya konsleting.

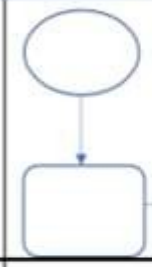
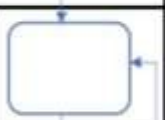
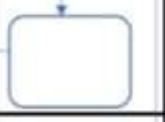
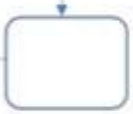
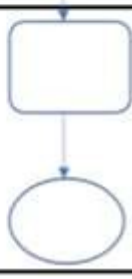
4.3.10 Penempatan kabel jaringan dan kabel listrik harus diletakan ditempat terpisah.

PT. GUBAH ESTETIKA TATA SINERGI	NOMOR SOP	SOP - 02	TGL. PEMBUATAN	/ /
	PENANGGUNG JAWAB		TGL. REVISI	/ /
	NOMOR REVISI		TGL. TERBIT	/ /
	NAMA SOP	**Manajemen *disaster recovery plan***		
	RUANG LINGKUP	Seluruh aset TI dan aset informasi		

DESKRIPSI SOP	KUALIFIKASI PELAKSANA
Prosedur manajemen *business continuity plan* merupakan prosedur yang memastikan perusahaan memiliki perencanaan pengamanan aset untuk insiden yang terjadi karena kelalaian SDM baik secara sengaja maupun tidak	Pelaksana merupakan seluruh karyawan yang memiliki tanggung jawab dan peran pada perusahaan.
TUJUAN SOP	**PERLENGKAPAN DAN PERALATAN**
Tujuannya yaitu membantu manajemen merencanakan kebijakan dan aktivitas untuk penanganan kejadian dan pencegahan terjadinya kejadian akibat kelalaian SDM	
REFRENSI	**PIHAK PELAKSANA**
ISO 27002:2013 - 17.1.1 *Planning information security continuity*	*Owner*, Kadiv GA, dan Karyawan
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan maka akan mengakibatkan risiko terhambatnya proses bisnis atau kerugian bagi perusahaan	

KETERANGAN	DIBUAT OLEH	DISETUJUI OLEH	DISAHKAN OLEH
Nama			
Tanggal			
Tanda Tangan	(.....)	(.....)	(.....)

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Onwer	Karyawan	Kadiv GA	
I.	**Proses perancangan penanganan DRP**				
1.	Mengindentifikasi laporan insiden yang sudah terjadi				
2.	Melakukan identifikasi cakupan aset yang harus dilindungi				
3.	Membentuk tim *recovery* yang bertanggung jawab atas pelaksanaan prosedur				
4.	Menentukan kebutuhan dan metode yang digunakan untuk keadaan darurat				
5.	Melakukan identifikasi peristiwa yang tidak terencanakan				
6.	Melakukan penyusunan aktivitas DRP				

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Owner	Karyawan	Kadiv GA	
II.	**Proses pengembangan DRP dan kontrol**				
1.	Melakukan evaluasi DRP yang sudah ada saat ini				
2.	Melakukan pembaharuan pada DRP				
3.	Melakukan pengujian penilaian terhadap DRP				
4.	Melakukan konfirmasi hasil evaluasi DRP apakah sudah layak atau tidak				
5.	Melakukan persetujuan untuk menjalankan DRP				
6.	Mengimplementasi perencanaan DRP yang sudah dibuat				
7.	Melakukan kontrol 6 bulan 1 kali terhadap implementasi DRP				
8.	DRP dapat diimplementasi lebih lanjut				

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. SURAT	KEB/SOP/02	**TGL. REVISI**	/ /
	NOMOR REVISI	00	**TGL. TERBIT**	/ /
	NAMA KEBIJAKAN	**Kebijakan *recovery disaster planning***		
	PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan menjamin proses bisnis dapat terus dijalankan secara berkelanjutan apabila terjadi insiden atau kejadian yang terjadi disebabkan oleh manusia atau alam.

II. RUANG LINGKUP

Cakupan kebijakan ini yaitu berlaku bagi para pihak yang terkait dalam perlindungan dan pengamanan seluruh aset TI dan aset informasi yang ada pada perusahaan. Adapun aset yang dimaksud terdiri dari :

- Perangkat keras
- Perangkat lunak
- Jaringan
- Data
- SDM

III. REFRENSI

Dalam penyusunan kebijakan ini tentu menggunakan refrensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan refrensi yaitu :

- 17.1.1 *Planning information security continuity*

IV. KEBIJAKAN

4.1 Perancangan DRP aset perusahaan

4.1.1 Pihak manajer dan pemilik perusahaan wajib membuat konsep perencanaan keberlangsungan proses bisnis pada semua aset yang dimiliki perusahaan.

4.1.2 Konsep perencanaan RDP wajib di evaluasi dan dikembangkan sesuai kebutuhan aset pada perusahaan.

4.1.3 Perencanaan RDP harus diuji cobakan secara terjadwal minimal 2 tahun 1 kali.

4.1.4 Semua pihak dalam perusahaan harus terlibat dalam uji coba pelaksanaan RDP.

4.1.5 Perusahaan wajib melaksanakan pelatihan dalam penanganan kondisi darurat minimal 1 tahun 1 kali.

4.1.6 Perusahaan wajib melakukan identifikasi aset berdasarkan jenis risiko bencana.

4.1.7 Seluruh SDM harus mendapatkan kompetensi dalam meningkatkan kesadaran akan bencana dan pencegahan terjadinya kejadian karena *man-man disaster*.

4.1.8 Perusahaan harus membangun sistem *backup* dan program *backup* yang dijalankan SDM secara berkala.

4.1.9 Perusahaan harus menyiapkan perencanaan perlindungan arsip data dan informasi yang terdokumentasi.

4.1.10 Teknisi TI harus melakukan enskripsi pada data-data kritis dan *password*.

4.1.11 Perusahaan harus melakukan perhitungan perkiraan kerugian atas kerusakan aset TI dan aset informasi.

4.1.12 Perusahaan harus memiliki daftar *supplier* yang dapat memasok perangkat TI dengan cepat dalam keadaan daruat.

4.1.13 Perusahaan harus menyediakan tempat cadangan untuk melindungi data dan informasi yang sudah terdokumentasi dan tempat evakuasi.

4.1.14 Perusahaan harus mengasuransikan seluruh SDM untuk pertolongan darurat karena bencana alam atau bencana yang disebabkan manusia dan lainnya.

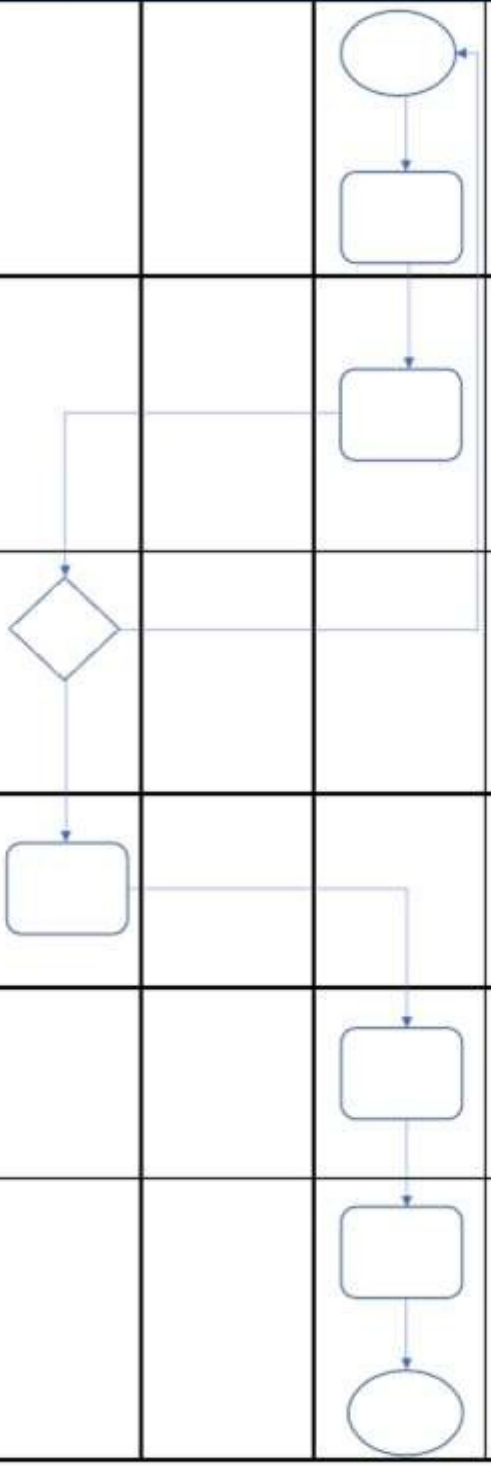
4.1.15 Perusahaan memastikan semua aset TI, aset informasi, dan perusahaan sudah diasuransikan untuk membantu perusahaan dalam memulihkan bisnis.

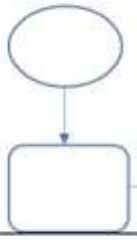
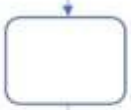
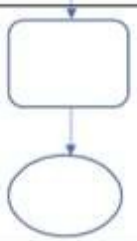
PT. GUBAH ESTETIKA TATA SINERGI	NOMOR SOP	SOP - 03	TGL. PEMBUATAN	/ /
	PENANGGUNG JAWAB		TGL. REVISI	/ /
	NOMOR REVISI		TGL. TERBIT	/ /
	NAMA SOP	**Pengelolaan dan pengembangan SDM**		
	RUANG LINGKUP	SDM		

DESKRIPSI SOP	KUALIFIKASI PELAKSANA
Prosedur pengelolaan dan pengembangan SDM merupakan prosedur yang membantu manajemen dalam mengelola SDM agar menerapkan kebijakan keamanan informasi	Pelaksana merupakan pihak yang memiliki jabatan manager atau lebih tinggi dibandingkan karyawan.
TUJUAN SOP	**PERLENGKAPAN DAN PERALATAN**
Tujuan dari SOP ini untuk membantu manajemen dalam melakukan pelatihan, pengembangan, dan kontrol SDM dalam menjalankan peran dan tanggung jawab	
REFRENSI	**PIHAK PELAKSANA**
ISO 27002:2013 - 7.2.1 *Management responsibilities* - 7.1.2 *Terms and conditions of employment* - 7.2.2 *Information security, awareness, education, and training*	Kadiv GA, karyawan, dan *owner*
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan maka akan mengakibatkan penurunan kinerja karyawan dan dapat menajadi ancaman bagi keamanan informasi sehingga proses bisnis terhambat	

KETERANGAN	DIBUAT OLEH	DISETUJUI OLEH	DISAHKAN OLEH
Nama			
Tanggal			
Tanda Tangan	(.....)	(.....)	(.....)

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Owner	Karyawan	Kadiv GA	
I.	**Proses identifikasi kebutuhan SDM**				
1.	Melakukan identifikasi pelatihan yang mendukung pengembangan SDM dalam menjalankan keamanan informasi				
2.	Melakukan pelaporan mengenai hasil identifikasi dan hasil program atau pelatihan yang akan diadakan				
2.	Memberikan konfirmasi apakah disetujui atau tidak atas program pelatihan yang akan diadakan sudah sesuai				
3	Memberikan informasi dan arahan mengenai pelatihan yang akan diadakan				
4.	Menentukan jadwal program atau pelatihan yang akan dilaksanakan				
5.	Memberikan informasi mengenai program atau pelatihan yang akan diadakan kepada karyawan dan staff				



No	Aktivitas	Pelaksana			Dokumen Pendukung
		Owner	Karyawan	Kadiv GA	
II.	**Proses pelaksanaan**				
1.	Mengikuti program atau pelatihan yang diadakan				
2.	Melakukan kontrol bahwa seluruh SDM mengikuti program dengan baik				
3.	Memastikan bahwa tujuan dari pelatihan benar-benar terlaksana				

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Owner	Karyawan	Kadiv GA	
III.	**Proses evaluasi**				
1.	Melakukan evaluasi dari pelatihan atau program yang diadakan				**FORM/SOP/04**
2.	Melakukan kontrol melalui observasi apakah pelatihan sudah memberikan hasil yang diharapkan				
A	**Jika tidak**, maka perlu dialukan identifikasi dan pelatihan kembali				
3.	Melakukan pertimbangan penilaian masing-masing karyawan				

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. FORM	FORM/SOP/04	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA FORMULIR	Formulir evaluasi pelatihan dan pengembangan SDM		
	PENANGGUNG JAWAB			
	WAKTU PELAKSANAAN	Tanggal :	Waktu :	

Nama	:	Tanggal pelatihan	:
Jabatan	:	Nama pelatihan	:
Divisi	:	Kegiatan pelatihan ke-	:

Tujuan Pelatihan	
Pencapaian yang diharapkan	
Metode evaluasi	☐ Tes tertulis ☐ Praktik ☐ Observasi

Lingkup penilaian		
Implementasi Mampu menerapkan pelatihan yang diberikan	☐ IYA	☐ TIDAK
Pengetahuan Memahami dan mengerti konsep yang diberikan	☐ IYA	☐ TIDAK
Sikap Mampu menjunkan arahan sikap yang diberikan	☐ IYA	☐ TIDAK
Keterampilan yang sudah diterapkan : 1) ..... 2) ..... 3) ..... 4) ..... 5)		
Hasil Evaluasi dan Saran :		

Kepala Divisi General Affairs	Mengetahui, Pemimpin GeTs Architects
_____ (Nama Lengkap)	_____ (Nama Lengkap)

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. SURAT	KEB/SOP/03	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA KEBIJAKAN	Kebijakan pengelolaan SDM		
	PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan untuk mengatur dan memastikan SDM ikut berperan aktif dalam menerapkan aktivitas prosedur keamanan informasi pada perusahaan.

II. RUANG LINGKUP

Cakupan kebijakan ini yaitu berlaku bagi seluruh pihak yang menggunakan seluruh aset TI dan aset informasi perusahaan baik pihak internal perusahaan dan pihak ketiga. Pihak yang dimaksud tersebut yaitu :

- Seluruh pegawai GeTs Architects
- Pihak ketiga / vendor
- Pegawai magang / bantuan kerja

III. REFRENSI

Dalam penyusunan kebijakan ini tentu menggunakan refrensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan refrensi yaitu :

- 7.2.1 *Management responsibilities*
- 7.1.2 *Terms and conditions of employment*
- 12.4.3 *Administrator & Operation logs*
- 7.2.2 *Information security, awareness, education, and training*

IV. KEBIJAKAN

4.1 Keamanan SDM dalam penggunaan aset TI dan aset informasi

4.1.1 Seluruh pegawai dan staff GeTs Architects wajib menandatangani kontrak komitmen dalam menerapkan dan menjaga keamanan aset informasi perusahaan.

4.1.2 Seluruh pegawai dan staff wajib diberikan pelatihan dan pengetahuan mengenai aktivitas keamanan informasi minimal 6 bulan 1 kali, sehingga pegawai dan staff memiliki kesadaran dan pengertian akan pentingnya menerapkan keamanan informasi pada perusahaan.

4.1.3 Seluruh pihak ketiga wajib melakukan tanda tangan komitmen kerahasiaan informasi dan penerapan aktivitas keamanan aset informasi pada perusahaan.

4.1.4 Seluruh pegawai magang atau bantuan kerja harus melakukan tanda tangan perjanjian untuk komitmen menerapkan aktivitas keamanan informasi serta menjaga kerahasiaan informasi.

4.1.5 Seluruh pegawai magang atau bantuan kerja wajib diberikan pelatihan dan pengetahuan mengenai aturan dan aktivitas keamanan informasi sebelum menggunakan seluruh aset TI dan aset informasi.

4.1.6 Kadiv GA wajib melakukan kontrol dan evaluasi atas kinerja karyawan dan staff dalam menerapkan aktivitas keamanan informasi minimal 3 bulan 1 kali.

4.1.7 Kadiv GA wajib memberikan sanksi atau peringatan bagi pihak yang melanggar kontrak dan aktivitas keamanan informasi

4.1.8 Seluruh pihak yang ada pada perusahaan wajib menjaga seluruh aset TI dan aset informasi.

4.1.9 Kadiv GA berhak dalam melakukan rotasi posisi apabila hasil evaluasi dan kontrol menunjukan karyawan dan staff tersebut tidak mampu atau tidak berkompenten dalam menjalankan aktivitas keamanan informasi.

4.1.10 Karyawan dilarang melakukan transaksi apapun mengatasnamakan data atau kepentingan perusahaan.

4.2 Keamanan SDM dalam hak akses

4.2.1 Seluruh karyawan yang diberikan hak akses tidak boleh melakukan penyalinan data atau memperbanyak data yang ada pada server tanpa seizin Kadiv GA dan admin dengan alasan apapun.

4.2.2 Seluruh karyawan wajib menjaga ID dan *password* akses server yang telah diberikan, apabila tersebarluaskan maka Kadiv GA berhak memberikan sanksi sesuai keputusan perusahaan.

4.2.3 Melakukan hak akses server hanya boleh dilakukan dalam lingkup perusahaan.

4.2.4 Pegawai magang atau bantuan kerja serta pihak ketiga tidak boleh memiliki hak akses server, apabila ingin melakukan akses harus didampingi oleh admin.

4.2.5 Seluruh data yang dan informasi yang ada pada server tidak boleh difoto, direkam, atau di *screenshoot* dengan alasan apapun.

4.2.6 Admin wajib bertanggung jawab atas kerahasiaan data, keaslian data, dan ketersediaan data.

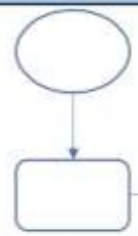
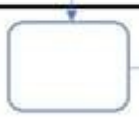
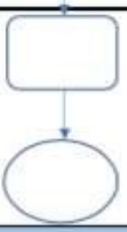
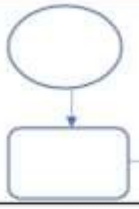
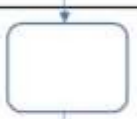
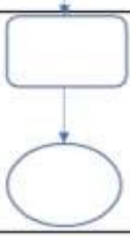
4.2.7 Admin dan Kadiv GA bertanggung jawab dalam pemberian hak akses server serta pemblokiran hak akses server.

PT. GUBAH ESTETIKA TATA SINERGI	NOMOR SOP	SOP - 04	TGL. PEMBUATAN	/ /
	PENANGGUNG JAWAB		TGL. REVISI	/ /
	NOMOR REVISI		TGL. TERBIT	/ /
	NAMA SOP	**Manajemen keamanan lingkungan dan penempatan peralatan**		
	RUANG LINGKUP	Peralatan perangkat TI		

DESKRIPSI SOP	KUALIFIKASI PELAKSANA
Prosedur manajemen keamanan dan penempatan peralatan merupakan prosedur yang memastikan manajemen keamanan seluaruh peralatan perangkat TI baik serta penempatan yang layak dan benar	Pelaksana harus pihak yang memiliki jabatan top manajer serta memiliki pengetahuan akan keamanan peralatan TI di perusahaan.
TUJUAN SOP	**PERLENGKAPAN DAN PERALATAN**
Tujuan dari SOP ini yaitu membantu manajemen dalam mengelola keamanan peralatan perangkat TI serta menempatkan ditempat yang aman dan benar untuk mencegah risiko kerusakan atau akses yang tidak sah	
REFRENSI	**PIHAK PELAKSANA**
ISO 27002:2013 - 11.2.1 *Equipment siting and protection*	Kadiv GA, *Owner*, dan Teknisi TI (pihak ketiga)
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan sebagaimana harusnya maka akan mengakibatkan kerusakan pada peralatan TI, penurunan kinerja karyawan, dan proses bisnis terhambat	

KETERANGAN	DIBUAT OLEH	DISETUJUI OLEH	DISAHKAN OLEH
Nama			
Tanggal			
Tanda Tangan	(.....)	(.....)	(.....)

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Teknisi TI	*Owner*	Kadiv GA	
I.	**Proses persiapan keamanan lingkungan**				
1.	Mengidentifikasi aset TI dan informasi yang ada di perusahaan				
2.	Melakukan pencatatan daftar aset TI dan aset informasi				
3.	Melakukan analisis peletakan semua aset TI dan aset informasi sesuai dengan kebutuhan proses bisnis				
5.	Memberikan konfirmasi terkait hasil analisis dan laporan yang sudah dilakukan				
6.	Melakukan cek apakah analisis dan laporan sudah sesuai atau tidak				
7.	Melakukan konfirmasi dan saran untuk pelaksanaan kepada Kadiv GA				
8.	Melakukan konfirmasi kepada teknisi TI untuk pelaksanaan sesuai dengan laporan perencanaan				

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Teknisi TI	*Owner*	Kadiv GA	
II.	**Proses penempatan dan perancangan ruangan keamanan aset**				
1.	Melakukan proses penempatan dan perancangan keamanan ruang aset				
2.	Melakukan kontrol pada proses pengerjaan				
3.	Melakukan konformasi terkait status pengerjaan				
4.	Memastikan semua proses sudah dilakukan sesuai dengan perencanaan				
III.	**Proses kontrol**				
1.	Melakukan pemeliharaan 1 kali dalam 6 bulan				
2.	Melakukan evaluasi atas keamanan lingkungan aset				
3.	Melakukan konfirmasi mengenai hasil evaluasi kepada pemimpin perushaan				
4.	Melakukan pengembangan jika dibutuhkan				

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. SURAT	KEB/SOP/01	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA KEBIJAKAN	**Pengelolaan keamanan perangkat keras dan jaringan**		
	PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan menjamin keamanan aset perangkat keras dan jaringan yang ada pada perusahaan agar dapat digunakan selama berjalannya proses bisnis tanpa adanya gangguan.

II. RUANG LINGKUP

Cakupan kebijakan ini yaitu berlaku bagi para pihak yang terkait dalam penggunaan, pengelolaan, pemeliharaan, dan pengamanan seluruh aset perangkat keras dan jaringan yang ada pada perusahaan. Adapun aset perangkat keras dan jaringan yang dimaksud terdiri dari :

- PC
- Server
- Printer
- Laptop
- *Mouse*
- *Speaker*
- *Keyboard*
- CPU
- UPS
- Proyektor

III. REFRENSI

Dalam penyusunan kebijakan ini tentu menggunakan refrensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan refrensi yaitu :

- 11.2.2 *Supporting utilities*
- 11.2.4 *Equipment maintenance*
- 11.2.1 *Equipment siting and protection*
- 11.2.3 *Cabling security*

IV. KEBIJAKAN

4.1 Pengelolaan keamanan perangkat keras

4.1.1 Segala bentuk kerusakan dan gangguan yang terjadi pada perangkat keras wajib untuk di laporkan kepada pihak yang bertanggung jawab.

4.1.2 Seluruh laporan kerusakan atau gangguan harus segera di proses dan ditangani dalam kurun waktu 2 x 24 jam oleh pihak teknisi TI.

4.1.3 Segala proses perbaikan atau pengadaan peralatan perangkat keras wajib dilakukan pencatatan dan dikonfimasi paling lambat 1 x 24 jam oleh pihak teknisi TI.

4.1.4 Seluruh perangkat keras yang sudah rusak atau tidak digunakan kembali wajib ditempatkan di ruangan gudang penyimpanan yang sudah disediakan perusahaan.

4.1.5 Seluruh perangkat keras yang sudah rusak atau tidak digunakan kembali tidak boleh dibuang atau diperjual belikan tanpa keputusan pemusnahan media oleh perusahaan.

4.1.6 Dilarang merusak atau mengotak-atik peralatan TI secara sengaja atau tidak jika tidak diberikan izin atau arahan dari pihak teknisi TI yang bertanggung jawab.

4.1.7 Dilarang melakukan pengadaan perangkat keras tambahan jika tidak adanya izin atau perintah dari Kadiv GA.

4.1.8 Dilarang untuk membawa pulang seluruh peralatan perangkat keras dengan alasan apapun.

4.1.9 Pemeliharaan secara berkala wajib dijalankan 1 kali dalam 6 bulan dan tidak boleh menunda penjadwalan pemeliharaan yang sudah ditentukan.

4.1.10 Segala bentuk kerusakan dan pemeliharaan wajib ditangani oleh pihak yang ahli dalam perangkat keras yang ada di perusahaan.

4.1.11 Kadiv GA wajib melakukan kontrol atas proses penggunaan, perbaikan, dan pemeliharaan perangkat keras.

4.1.12 Teknisi TI yang telah ditunjuk wajib bertanggung jawab atas pemeliharaan dan perbaikan yang dilakukan, serta melakukan konfirmasi dan pencatatan pada setiap proses yang dilakukan.

4.1.13 Segala bentuk pengadaan barang wajib dikonfirmasi dan atas persetujuan *Owner* dan Kadiv GA.

4.1.14 Seluruh kegiatan pengelolaan, pemeliharaan, perbaikan, dan penggunaan perangkat keras harus sesuai dengan prosedur keamanan peralatan TI dan mengikuti kebijakan keamanan yang berlaku.

4.1.15 Peralatan TI yang ada diperusahaan hanya boleh digunakan dan dioperasikan oleh seluruh karyawan (kecuali OB) yang merupakan bagian dari perusahaan.

4.1.16 Penggunaan perangkat TI hanya boleh dilakukan pada jam kerja, apabila diluar itu harus melakukan konfirmasi izin kepada Kadiv GA.

4.1.17 Semua perangkat TI kritis dan sangat penting wajib diberikan perlindungan asuransi.

4.1.18 Seluruh perangkat TI wajib dimatikan jika sudah selesai digunakan, kecuali apabila ada kebutuhan mendesak yang mengharuskan PC tetap menyala seperti proses render desain. Namun harus melakukan konfirmasi kepada Kadiv GA

4.1.19 Dalam PC, laptop, dan server wajib dipasang sistem *log in* yang mengharuskan pengguna memasukan ID dan *password*.

4.1.20 Setiap karyawan dan Kadiv GA wajib melakukan kontrol ketersediaan sarana pendukung seperti UPS untuk memastikan proses bisnis terus berjalan.

4.1.21 Setiap perangkat TI harus memiliki perlindungan altemative, seperti adanya silikon pelindung *keyboard*, pelindung layer, dsb.

4.1.22 Apabila kerusakan dan gangguan terjadi maka seluruh karyawan wajib menerapkan kebijakan RDP dalam waktu maksimal 2 jam setelah kerusakan terjadi.

4.2 Pengelolaan keamanan lingkungan perangkat keras

4.2.1 Seluruh perangkat TI harus ditempatkan pada ruangan khusus, aman, dan layak sesuai dengan prosedur yang sudah ditentukan perusahaan.

4.2.2 Seluruh ruangan perangkat TI harus diberikan CCTV yang selalu menyala dan kunci ruangan yang dilakukan setelah jam operasional perusahaan selesai.

4.2.3 Seluruh ruangan yang berisikan aset TI harus diberikan diberikan pendingin ruangan dan sirkulasi udara yang baik untuk mencegah *overheating*.

4.2.4 Dilarang untuk memindahkan seluruh perangkat TI selain pihak yang bertanggung jawab.

4.2.5 Dilarang membawa minuman atau makanan yang bersifat cair kedalam ruangan perangkat TI.

4.2.6 Dilarang merokok dalam ruangan perangkat TI.

4.2.7 Selain staff dan karyawan GeTs Architects dilarang memasuki ruangan perangkat TI, terkecuali atas izin dari Kadiv GA.

4.2.8 Dilarang membawa peliharaan kedalam ruangan perangkat TI.

4.2.9 Ruangan perangkat TI harus selalu dirawat dan dibersihkan untuk menhindari debu dan hewan seperti tikus.

4.2.10 Ruangan perangkat TI harus mendapatkan matahari yang cukup untuk menhindari kelembapan ruangan.

4.3 Pengelolaan keamanan jaringan

4.3.1 Setiap kabel yang ada pada ruangan perangkat TI wajib diberikan pelabelan nama dan fungsi untuk memudahkan konfigurasi dan *maintenance*.

4.3.2 Setiap kabel pada ruang perangkat TI harus dilakukan pembedaan warna untuk memundahkan konfigurasi dan *maintenance*.

4.3.3 Setiap kabel yang ada pada perusahaan harus ditempatkan pada tata letak yang aman tidak terinjak-injak serta wajib diberikan perlindungan pelapisan kabel menggunakan pipa atau karet pelindung kabel.

4.3.4 Setiap kabel yang ada pada ruang perangkat TI tidak boleh terlilit dan harus tersusun dengan rapih untuk mencegah arus pendek.

4.3.5 Pihak Kadiv GA dan teknisi TI wajib melakukan kontrol jaringan dan kabel dalam waktu 1 kali dalam 6 bulan.

4.3.6 Jika ada kerusakan atau gangguan jaringan maka wajib memberikan konfirmasi kepada Kadiv GA.

4.3.7 Setiap proses pemeliharaan dan perbaikan harus dilakukan pencatatan.

4.3.8 Proses pemeliharaan dan *maintenance* wajib dilakukan oleh teknisi TI yang ahli dalam jaringan.

4.3.9 Dilarang menumpuk steker pada terminal listrik untuk mencegah terjadinya konsleting.

4.3.10 Penempatan kabel jaringan dan kabel listrik harus diletakan ditempat terpisah.

PT. GUBAH ESTETIKA TATA SINERGI	NOMOR SOP	SOP - 05	TGL. PEMBUATAN	/ /
	PENANGGUNG JAWAB		TGL. REVISI	/ /
	NOMOR REVISI		TGL. TERBIT	/ /
	NAMA SOP	***Backup* data perusahaan dan pemusnahan media**		
	RUANG LINGKUP	Semua data perusahaan		

DESKRIPSI SOP	KUALIFIKASI PELAKSANA
Prosedur *backup* dan *restore* data perusahaan merupakan prosedur yang memastikan perusahaan memiliki pedoman dalam melakukan pengelolaan *backup* dan *restore* data dan menerapkannya secara baik	Pelaksana merupakan pihak yang bertanggung jawab atas hak akses server serta yang mengakses dan mengelola semua data dan informasi pada perusahaan
TUJUAN SOP	**PERLENGKAPAN DAN PERALATAN**
Tujuan dari SOP ini yaitu membantu manajemen dalam mengatur dan mengelola keamanan dalam proses *backup* dan *restore* data serta pemusnahan media secara benar, sehingga meminimalisir risiko pada aset data	
REFRENSI	**PIHAK PELAKSANA**
ISO 27002:2013 - 12.3.1 *Information Backup* - 8.3.1 *Management of removable media*	Kadiv GA, admin, dan karyawan
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan sebagaimana harusnya maka akan mengakibatkan risiko pada keamanan aset data, risiko pada ketersediaan informasi, dan proses bisnis terhambat	

KETERANGAN	DIBUAT OLEH	DISETUJUI OLEH	DISAHKAN OLEH
Nama			
Tanggal			
Tanda Tangan	(.....)	(.....)	(.....)

No.	Aktivitas	Pelaksana			Dokumen Pendukung
		Admin	Karyawan	Kadiv GA	
I.	**Proses persiapan melakukan *backup* data**				
1.	Mengelompokan data- data perusahaan berdasarkan kebutuhan dan katagori.				
2.	Melakukan tingkat kritikalitas data dan data yang masih digunakan untuk jangan panjang				
3.	Membuat draf atas data yang sudah dikelompokan dan ditentukan tingkat kritikalitasnya				
4.	Menentukan metode dan media yang digunakan untuk melakukan *backup*				
5.	Menentukan penjadwalan untuk melakukan *backup*				
6.	Melakukan konfirmasi kepada semua karyawan atas pencatatan data yang akan di*backup*, tanggal *backup*, metode, dan media *backup*				

No.	Aktivitas	Pelaksana			Dokumen Pendukung
		Admin	Karyawan	Kadiv GA	
II.	**Proses melakukan *backup* secara berkala**				
1.	Memberikan konfirmasi dan intruksi kepada admin untuk melakukan *backup* data				
2.	Melakukan proses *backup*				
3.	Melakukan kontrol terhadap data yang di*backup* apakah sesuai pencatatan dan semua data tidak *corrupt*				
A	**Jika gagal**, maka akan melakukan pencatatan data yang rusak dan melakukan proses *backup* ulang.				
4.	Melakukan pencatatan pada formular laporan *backup* data				**FORM/SOP/05**
5.	Melakukan kontrol bahwa admin menjalankan tugas secara baik dan sesuai kebijakan keamanan informasi				

No.	Aktivitas	Pelaksana			Dokumen Pendukung
		Admin	Karyawan	Kadiv GA	
III.	**Melakukan evaluasi proses *backup* data**				
1.	Melakukan uji *backup* data dalam waktu 3 bulan sekali				
2.	Melakukan persiapan uji coba *backup* data				
2.	Melakukan kontrol media yang digunakan, apakah aman dan sesuai				
3	Melakukan kontrol log *backup* data, apakah berhasil atau gagal				
A	**Jika Gagal**, melakukan proses evaluasi dan persiapan uji coba *backup* ulang				
B	**Jika berhasil**, aman, dan sesuai melakukan pencatatan pada laporan form *backup* data				

No.	Aktivitas	Pelaksana			Dokumen Pendukung
		Admin	Karyawan	Kadiv GA	
IV.	**Proses pemusnahan media**				
1.	Melakukan klasifikasi media informasi atau data yang akan dimusnahkan				
2.	Melakukan konfirmasi atas list media atau data yang akan dimusnahkan				
3.	Melakukan pengecekan pada list apakah sudah sesuai atau belum				
4.	Menentukan metode dan waktu pemusnahan media				
5.	Melaporkan form berita acara pemusnahan media				**FORM/SOP/06**
6.	Melakukan konfirmasi jika pemusnahan sudah sesuai dan disetujui				
7.	Melakukan proses pemusnahan media				

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. FORM	FORM/SOP/05	**TGL. REVISI**	/ /
	NOMOR REVISI	00	**TGL. TERBIT**	/ /
	NAMA FORMULIR	**Formulir *backup* data**		
	PENANGGUNG JAWAB			
	WAKTU PELAKSANAAN	Bulan :	Tahun :	

No.	Tanggal *Backup*	Waktu *Backup*	Nama Media *Backup*	Jumlah Media	Metode *Backup*	Isi media *backup*	Status	Keterangan

Petugas *Backup*

(Nama Lengkap)

Mengetahui,
Kepala Divisi General Affairs

(Nama Lengkap)

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. FORM	FORM/SOP/06	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA FORMULIR	Formulir berita acara pemusnahan media		

BERITA ACARA PEMUSNAHAN MEDIA

Pada hari ini, …. tanggal ….. bulan ….. tahun …….. bertempat di PT. Gubah Estetika Tata Sinergi. Kami yang bertanda tangan dibawah ini atas persetujuan manajemen yang bertanggung jawab atas media informasi, dengan ini memusnahkan media informasi yang terdiri sebagai berikut :

No.	Jenis Media	Nama media	Ket. Spesifikasi media	Metode Pemusnahan

Disiapkan Oleh,
Petugas Pemusnahan Media

_____
(Nama Lengkap)

Diperiksa oleh,
Kepala Divisi General Affairs

_____
(Nama Lengkap)

Disetujui oleh,
Pemimpin GeTs Architects

_____
(Nama Lengkap)

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. SURAT	KEB/SOP/04	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA KEBIJAKAN	Kebijakan keamanan data dan informasi		
	PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan untuk memastikan terjaminnya keamanan seluruh data dan informasi perusahaan

II. RUANG LINGKUP

Cakupan kebijakan ini yaitu berlaku bagi seluruh pihak yang mengelola dan mengakses seluruh data dan informasi perusahaan. Data dan informasi tersebut yaitu :

- Data Keuangan
- Data Karyawan
- Data Klien
- Data Aset Perusahaan
- Data Supplier
- Data Desain Bangunan
- *Database*

III. REFRENSI

Dalam penyusunan kebijakan ini tentu menggunakan refrensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan refrensi yaitu :

- 12.4.3 *Administrator & Operation logs*
- 12.4.1 *Event logging*
- 12.3.1 *Information Backup*
- 8.3.1 *Management of removable media*

IV. KEBIJAKAN

4.1 Pengelolaan keamanan data

4.1.1 Seluruh pegawai wajib melakukan klasifikasi dan *backup* data secara berkala minimal 1 kali dalam 3 bulan sesuai jadwal yang telah direncanakan.

4.1.2 Admin wajib memeriksa data yang di *backup* sudah sesuai dan tidak rusak atau *corrupt*.

4.1.3 Admin wajib memastikan data selalu tersedia dan akurat.

4.1.4 Jika diperlukan, semua data didokumentasikan kebentuk *hardcopy* dan diarsipkan di tempat yang aman dari gangguan dan akses yang tidak sah.

4.1.5 Dilarang memalsukan data dan informasi perusahaan.

4.1.6 Dilarang melakukan pemusnahan data dengan alasan apapun jika tidak ada izin berita acara pemusnahan media.

4.1.7 Dilarang memperjual belikan data dan informasi kepada pihak lain dengan alasan atau keadaan apapun.

4.1.8 Dilarang menyalin atau memperbanyak data tanpa seizin dari admin dan Kadiv GA.

4.1.9 Dilarang mencampur data pribadi dengan data perusahaan.

4.1.10 Admin dan Kadiv GA wajib melakukan kontrol keamanan data dan informasi minimal 1 kali dalam 3 bulan.

4.1.11 Apabila kerusakan dan gangguan terjadi maka seluruh karyawan wajib menerapkan kebijakan RDP dalam waktu maksimal 2 jam setelah kerusakan terjadi.

4.2 Pengelolaan keamanan pemusnahan media

4.2.1 Seluruh karyawan wajib melakukan klasifikasi data serta mencatat dalam list data dan informasi yang akan di musnahkan.

4.2.2 Kadiv GA wajib melakukan pencatatan pada daftar list media yang sudah rusak dan tidak digunakan sebelum dimusnahkan.

4.2.3 Seluruh list data dan media yang akan dimusnahkan harus disiapkan 2 minggu sebelum dilakukannya pemusnahan.

4.2.4 Kadiv GA wajib melakukan pelaporan list kepada pemimpin perusahaan dan melakukan pengecekkan minimal 1 minggu sebelum dilakukan pemusnahan.

4.2.5 Pemimpin wajib memastikan bahwa data atau media yang dimusnahkan benar-benar sudah sesuai.

4.2.6 Kadiv GA Bersama admin wajib menentukan metode pemusnahan dan memastikan bahwa semua data dan media yang dimusnahkan benar-benar aman dan sesuai dengan kebijakan perusahaan.

4.2.7 Untuk media yang menyimpan dan mengelola data kritis seperti PC atau server wajib dimusnahkan atau dihancurkan. Dilarang dijual kembali atau dibuang.

4.2.8 Untuk data kritis harus dihapus dan dipastikan tidak dapat diakses kembali, untuk data kritis yang sudah didokumentasikan wajib dimusnahkan dengan dibakar.

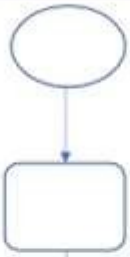
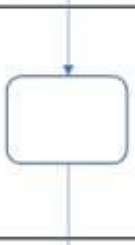
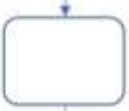
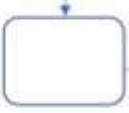
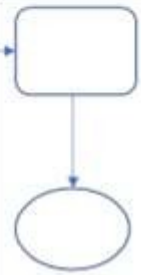
4.2.9 Admin dan Kadiv GA wajib melakukan pencatatan pada berita acara pemusnahan media, serta membuat laporan mengenai data dan media yang dimusnahkan sebagai bukti dan catatan audit.

4.2.10 Berita acara wajib ditandatangani oleh pemimpin perusahaan, Kadiv GA, dan petugas pemusnahan.

PT. GUBAH ESTETIKA TATA SINERGI	NOMOR SOP	SOP - 06	TGL. PEMBUATAN	/ /
	PENANGGUNG JAWAB		TGL. REVISI	/ /
	NOMOR REVISI		TGL. TERBIT	/ /
	NAMA SOP	**Manajemen keamanan terhadap *malware***		
	RUANG LINGKUP	Seluruh perangkat lunak		

DESKRIPSI SOP	KUALIFIKASI PELAKSANA
Prosedur manajemen keamanan terhadap *malware* merupakan prosedur yang memastikan setiap aset informasi memiliki pengelolaan keamanan terhadap virus dan kerentanan yang dapat menyerang keamanan aset informasi	Pelaksana harus memiliki pengetahuan dan kemampuan akan mengelola serta menggunakan perangkat lunak yang ada pada perusahaan.
TUJUAN SOP	**PERLENGKAPAN DAN PERALATAN**
Tujuan dari SOP ini yaitu membantu manajemen dalam melakukan pengelolaan keamanan aset informasi, membantu melakukan kontrol pada *firewall* semua aset informasi, serta meminimalisir adanya virus atau serangan *hacker*	
REFRENSI	**PIHAK PELAKSANA**
ISO 27002:2013 - 12.2.1 *Control against malware*	Kadiv GA, Teknisi TI (pihak ketiga), dan karyawan
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan sebagaimana harusnya maka akan mengakibatkan kerentanan pada perangkat lunak yang berisiko adanya virus dan *hacker* yang dapat menghambat proses bisnis	

KETERANGAN	DIBUAT OLEH	DISETUJUI OLEH	DISAHKAN OLEH
Nama			
Tanggal			
Tanda Tangan	(.....)	(.....)	(.....)

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Teknisi TI	Karyawan	Kadiv GA	
I.	**Proses perlindungan atas *malware***				
1.	Memasang perangkat untuk pencegahan *malware* seperti anti virus, *spam filtering*, anti *spyware*, dll sesuai dengan kebutuhan				
2.	Melakukan update atau isntalasi ulang untuk sistem atau aplikasi yang bermasalah atau dibutuhkan				
3.	Melakukan kontrol semua perangkat sudah terpasang anti *malware* dan dapat digunakan				
4.	Melakukan update anti *malware* pada setiap perangkat				
5.	Melakukan kontrol semua PC tidak terdapat file, aplikasi, sistem, dll yang menimbulkan virus				
6.	Memastikan bahwa tidak membuka sistus web atau file apapun yang memicu virus				

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Teknisi TI	Karyawan	Kadiv GA	
II.	**Proses perbaikan atas gangguan *malware***				
1.	Memberitahukan informasi indikasi umum jika terdapat gangguan *malware*				
2.	Melaporkan kepada kadiv GA jika terdapat gangguan keamanan informasi				
3.	Melaporkan gangguan atau insiden kepada teknisi TI				
4.	Melakukan pencatatan pada form kegagalan sistem informasi				**FORM/SOP/07**
5.	Melakukan *backup* data maksimal 1 jam setelah konfirmasi kepada kadiv GA				
7.	Melakukan perbaikan dan penanganan gangguan *malware*				
9.	Melakukan kontrol selama 1 bulan untuk memastikan apakah penanganan berhasil atau tidak				
10.	Melakukan pencatatan mengenai status penanganan pada form gangguan sistem informasi				

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. FORM	FORM/SOP/07	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA FORMULIR	Formulir laporan kegagalan sistem informasi		
	PENANGGUNG JAWAB			
	WAKTU PELAKSANAAN	Bulan :	Tahun :	

Total Kegagalan Sistem Informasi	☐ *Hacker*	..... Kejadian	☐ Sistem *Crush*	..... Kejadian
	☐ Virus	..... Kejadian	☐ *Bugs*	..... Kejadian
	☐ Sabotase	..... Kejadian	☐ *Spyware*	..... Kejadian
	☐ *Human Error*	..... Kejadian	☐ Lain-lain	..... Kejadian
Uraian Kegagalan Sistem Informasi				

Tindakan Penanganan	Tindakan Pencegahan	Tanggal Penanganan		Status	Keterangan
		Mulai	Selesai		

Dibuat Oleh, Staff Divisi TI	Mengetahui, Kepala Divisi General Affairs
_____ (Nama Lengkap)	_____ (Nama Lengkap)

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. SURAT	KEB/SOP/05	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA KEBIJAKAN	Kebijakan pengelolaan keamanan perangkat lunak		
	PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan untuk memastikan terjaminnya keamanan perangkat lunak dari gangguan, kerusakan, virus, dan *hacker* yang dapat mengganggu serta menghambat proses bisnis.

II. RUANG LINGKUP

Cakupan kebijakan ini yaitu berlaku bagi seluruh pihak yang mengelola, memelihara, dan memperbaiki perakat lunak yang ada pada perusahaan. Perangkat lunak yang dimaksud terdiri dari sebagai berikut :

- Sistem operasi
- Auto CAD Architecture
- SketchUp
- Lumion 3D Rendering
- Adobe Photoshop
- Adobe Premiere

III. REFRENSI

Dalam penyusunan kebijakan ini tentu menggunakan refrensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan refrensi yaitu :

- 12.2.1 *Control against malware*
- 12.5.1 *Installation of software on operational systems*
- 12.6.2 *Restriction on software installation*

IV. KEBIJAKAN

4.1 Pengelolaan keamanan perangkat lunak

4.1.1 Seluruh kerusakan atau gangguan perangkat lunak harus dilaporkan kepada Kadiv GA minimal 1 x 24 jam.

4.1.2 Segala perbaikan dan pemeliharaan perangkat lunak wajib dilakukan oleh teknisi TI dalam waktu 1 kali dalam 6 bulan.

4.1.3 Seluruh kerusakan dan pemeliharaan oleh Kadiv GA serta teknisi TI harus dicatat untuk dijadikan evaluasi.

4.1.4 Dilarang untuk mengotak-atik ataupun menambahkan perangkat lunak apapun selain pihak teknisi TI atas permintaan perusahaan.

4.1.5 Apabila kerusakan dan gangguan terjadi maka seluruh karyawan wajib menerapkan kebijakan DRP dalam waktu maksimal 2 jam setelah kerusakan terjadi.

4.2 Pengelolaan keamanan instalasi perangkat lunak

4.2.1 Proses instalasi perangkat lunak harus dijalankan sesuai prosedur keamanan oleh teknisi TI.

4.2.2 Dilarang melakukan instalasi perangkat lunak apapun yang bersifat illegal atau palsu.

4.2.3 Instalasi perangkat lunak harus dilakukan sesuai kebutuhan perusahaan.

4.2.4 Karyawan dilarang melakukan instalasi perangkat lunak yang berbahaya atau tidak aman untuk mencegah kerusakan dan ancaman virus.

4.2.5 Perangkat lunak wajib dilakukan *update* sesuai dengan kebutuhan masing-masing aplikasi atau sistem.

4.2.6 Perusahaan wajib melakukan uji coba dan kontrol minimal selama 1 bulan setelah dilakukannya konfigurasi perangkat lunak untuk memantau jika terdapat gangguan atau kerusakan.

4.2.7 Hasil instalasi dan konfigurasi perangkat lunak harus dicatat dan dikonfirmasi kepada Kadiv GA.

4.3 Pengelolaan keamanan terhadap *malware*

4.3.1 Seluruh perangkat lunak harus terpasang anti virus dan dilakukan oleh teknisi TI.

4.3.2 Pemeliharaan dan pembaharuan *firewall* harus dilakukan minimal 1 kali dalam 3 bulan untuk mencegah ancaman *hacker* ataupun virus.

4.3.3 Perangkat lunak harus terdapat peringatan akan ancaman virus.

4.3.4 Karyawan dilarang membuka situs berbahaya atau terlarang serta mengunduh file yang bersifat membahayakan untuk mencegah masuknya virus pada perangkat lunak.

PT. GUBAH ESTETIKA TATA SINERGI	NOMOR SOP	SOP - 07	TGL. PEMBUATAN	/ /
	PENANGGUNG JAWAB		TGL. REVISI	/ /
	NOMOR REVISI		TGL. TERBIT	/ /
	NAMA SOP	**Konfigurasi dan instalasi perangkat lunak**		
	RUANG LINGKUP	Sistem operasi dan aplikasi		

DESKRIPSI SOP	KUALIFIKASI PELAKSANA
Prosedur konfigurasi dan instalasi perangkat lunak merupakan prosedur yang memastikan perusahaan memiliki pedoman dalam konfigurasi dan pemakaian perangkat lunak sesuai dengan kebijakan dan aturan yang ada	Pelaksana harus merupakan ahli dibagian TI serta memiliki pengetahuan akan mengelola dan menggunakan perangkat lunak yang ada pada perusahaan
TUJUAN SOP	**PERLENGKAPAN DAN PERALATAN**
Tujuan dari SOP ini yaitu membantu manajemen dalam melakukan kontrol instalasi serta konfigurasi perangkat lunak sudah sesuai dengan aturan, kebijakan, dan kebutuhan perusahaan	
REFRENSI	**PIHAK PELAKSANA**
ISO 27002:2013 - 12.5.1 *Installation of software on operational systems* - 12.6.2 *Restriction on software isntallation*	Kadiv GA, karyawan, dan teknisi TI (pihak ketiga)
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan sebagaimana harusnya maka akan mengakibatkan risiko penurunan kinerja karyawan, kerusakan perangkat lunak dan sanksi hukum bagi perusahaan	

KETERANGAN	DIBUAT OLEH	DISETUJUI OLEH	DISAHKAN OLEH
Nama			
Tanggal			
Tanda Tangan	(.....)	(.....)	(.....)

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Teknisi TI	*Owner*	Kadiv GA	
I.	Proses persiapan instalasi dan konfigurasi				
1.	Mengidentifikasi kebutuhan perangkat lunak yang digunakan dalam proses bisnis				
2.	Memberikan konfirmasi kebutuhan perangkat lunak kepada teknisi TI				
3.	Mengidentifikasi informasi jenis sistem atau aplikasi yang sesuai dengan kebutuhan				
4.	Memberikan konfirmasi jenis perangkat lunak yang sesuai				
5.	Melakukan konfirmasi, apakah sudah sesuai atau tidak				
7.	Melakukan perhitungan biaya yang akan dikeluarkan				
8.	Memberikan konfirmasi untuk dilakukan instalasi				
9.	Memberikan konfirmasi mengenai durasi pengerjaan				

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Teknisi TI	*Owner*	Kadiv GA	
II.	**Proses instalasi dan konfigurasi**				
1.	Melakukan persiapan kebutuhan yang akan digunakan dalam proses instalasi				
2.	Melakukan instalasi dan konfigurasi perangkat lunak				
3.	Melakukan kontrol terhadap proses instalasi				
4.	Memastikan status instalasi apakah berhasil tanpa gangguan atau gagal				
A	**Jika gagal**, melakukan konfirmasi untuk dilakukan perbaikan				
5.	Melakukan pencatatan pada form konfigurasi dan instalasi perangkat lunak				FORM/SOP/08
6.	Memastikan konfigurasi dan instalasi sudah sesuai dengan kebijakan keamanan perangkat lunak				

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Teknisi TI	*Owner*	Kadiv GA	
III.	**Proses pemeliharaan perangkat lunak**				
1.	Melakukan pemeliharaan sistem dan aplikasi 1 kali dalam 6 bulan				
2.	Melakukan pencatatan pada form pemeliharaan perangkat lunak				**FORM/SOP/09**
3.	Melakukan identifikasi apakah diemukan kelemahan atau tidak				
A	**Jika ada**, melakukan konfirmasi kepada kadiv GA dan proses perbaikan.				
4.	Melakukan konfirmasi hasil pemeliharaan perangkat lunak kepada Kadiv GA				
5.	Menentukan penjadwalan pemeliharaan berikutnya				

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. FORM	FORM/SOP/07/01	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA FORMULIR	Formulir pemeliharaan sistem dan aplikasi		
	PENANGGUNG JAWAB			
	WAKTU PELAKSANAAN	Tanggal :	Waktu :	

KETERANGAN PERANGKAT LUNAK	
JENIS PERANGKAT LUNAK	
NAMA SISTEM/APLIKASI	

KETERANGAN PEMELIHARAAN	
URAIAN PEMELIHARAAN	

KONDISI PERANGKAT LUNAK	
URAIAN KONDISI	
SARAN	

Petugas Perbaikan

(Nama Lengkap)

Mengetahui,
Kepala Divisi General Affairs

(Nama Lengkap)

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. FORM	FORM/SOP/08	**TGL. REVISI**	/ /
	NOMOR REVISI	00	**TGL. TERBIT**	/ /
	NAMA FORMULIR	**Formulir instalasi dan konfigurasi perangkat lunak**		
	PENANGGUNG JAWAB			
	WAKTU PELAKSANAAN	Bulan :	Tahun :	

No.	Deskripsi kebutuhan	Jenis perangkat lunak	Jumlah	Uraian pelaksanaan	Tanggal Pelaksana		Staff pelaksana	Status
					Mulai	Selesai		

Dibuat Oleh, Staff Divisi TI	Mengetahui, Kepala Divisi General Affairs
_____ (Nama Lengkap)	_____ (Nama Lengkap)

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. SURAT	KEB/SOP/05	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA KEBIJAKAN	Kebijakan pengelolaan keamanan perangkat lunak		
	PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan untuk memastikan terjaminnya keamanan perangkat lunak dari gangguan, kerusakan, virus, dan *hacker* yang dapat mengganggu serta menghambat proses bisnis.

II. RUANG LINGKUP

Cakupan kebijakan ini yaitu berlaku bagi seluruh pihak yang mengelola, memelihara, dan memperbaiki perakat lunak yang ada pada perusahaan. Perangkat lunak yang dimaksud terdiri dari sebagai berikut :

- Sistem operasi
- Auto CAD Architecture
- SketchUp
- Lumion 3D Rendering
- Adobe Photoshop
- Adobe Premiere

III. REFRENSI

Dalam penyusunan kebijakan ini tentu menggunakan refrensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan refrensi yaitu :

- 12.2.1 *Control against malware*
- 12.5.1 *Installation of software on operational systems*
- 12.6.2 *Restriction on software installation*

IV. KEBIJAKAN

4.1 Pengelolaan keamanan perangkat lunak

4.1.1 Seluruh kerusakan atau gangguan perangkat lunak harus dilaporkan kepada Kadiv GA minimal 1 x 24 jam.

4.1.2 Segala perbaikan dan pemeliharaan perangkat lunak wajib dilakukan oleh teknisi TI dalam waktu 1 kali dalam 6 bulan.

4.1.3 Seluruh kerusakan dan pemeliharaan oleh Kadiv GA serta teknisi TI harus dicatat untuk dijadikan evaluasi.

4.1.4 Dilarang untuk mengotak-atik ataupun menambahkan perangkat lunak apapun selain pihak teknisi TI atas permintaan perusahaan.

4.1.5 Apabila kerusakan dan gangguan terjadi maka seluruh karyawan wajib menerapkan kebijakan DRP dalam waktu maksimal 2 jam setelah kerusakan terjadi.

4.2 Pengelolaan keamanan instalasi perangkat lunak

4.2.1 Proses instalasi perangkat lunak harus dijalankan sesuai prosedur keamanan oleh teknisi TI.

4.2.2 Dilarang melakukan instalasi perangkat lunak apapun yang bersifat illegal atau palsu.

4.2.3 Instalasi perangkat lunak harus dilakukan sesuai kebutuhan perusahaan.

4.2.4 Karyawan dilarang melakukan instalasi perangkat lunak yang berbahaya atau tidak aman untuk mencegah kerusakan dan ancaman virus.

4.2.5 Perangkat lunak wajib dilakukan *update* sesuai dengan kebutuhan masing-masing aplikasi atau sistem.

4.2.6 Perusahaan wajib melakukan uji coba dan kontrol minimal selama 1 bulan setelah dilakukannya konfigurasi perangkat lunak untuk memantau jika terdapat gangguan atau kerusakan.

4.2.7 Hasil instalasi dan konfigurasi perangkat lunak harus dicatat dan dikonfirmasi kepada Kadiv GA.

4.3 Pengelolaan keamanan terhadap *malware*

4.3.1 Seluruh perangkat lunak harus terpasang anti virus dan dilakukan oleh teknisi TI.

4.3.2 Pemeliharaan dan pembaharuan *firewall* harus dilakukan minimal 1 kali dalam 3 bulan untuk mencegah ancaman *hacker* ataupun virus.

4.3.3 Perangkat lunak harus terdapat peringatan akan ancaman virus.

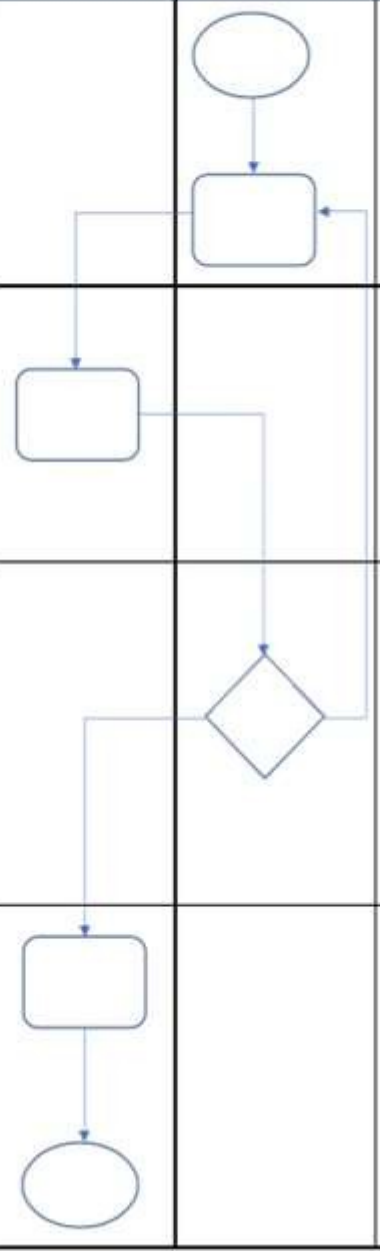
4.3.4 Karyawan dilarang membuka situs berbahaya atau terlarang serta mengunduh file yang bersifat membahayakan untuk mencegah masuknya virus pada perangkat lunak.

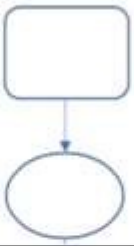
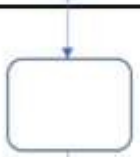
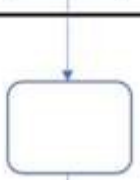
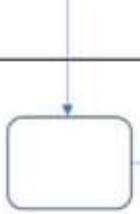
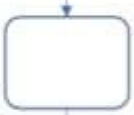
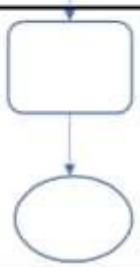
PT. GUBAH ESTETIKA TATA SINERGI	NOMOR SOP	SOP - 08	TGL. PEMBUATAN	/ /
	PENANGGUNG JAWAB		TGL. REVISI	/ /
	NOMOR REVISI		TGL. TERBIT	/ /
	NAMA SOP	**Perawatan dan pengelolaan keamanan jaringan**		
	RUANG LINGKUP	Kabel jaringan		

DESKRIPSI SOP	KUALIFIKASI PELAKSANA
Prosedur perawatan dan pengelolaan keamanan jaringan merupakan prosedur yang memastikan perusahaan memiliki pedoman dalam kontrol keamanan jaringan dan perlakuan yang tepat	Pihak pelaksana merupakan orang yang ahli dalam perawatan dan pengelolaan jaringan
TUJUAN SOP	**PERLENGKAPAN DAN PERALATAN**
Tujuan dari SOP ini yaitu membantu manajemen dalam melakukan kontrol pada keamanan aset yang mendukung jaringan dengan perlaukan yang tepat dan sesuai dengan kebutuhan perusahaan	
REFRENSI	**PIHAK PELAKSANA**
ISO 27002:2013 - 11.2.1 *Equipment siting and protection* - 11.2.3 *Cabling security*	Kadiv GA dan vendor (pihak ketiga)
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan sebagaimana harusnya maka akan mengakibatkan risiko rusaknya peralatan pada jaringan sehingga proses bisnis menjadi terhenti	

KETERANGAN	DIBUAT OLEH	DISETUJUI OLEH	DISAHKAN OLEH
Nama			
Tanggal			
Tanda Tangan	(.....)	(.....)	(.....)

No	Aktivitas	Pelaksana		Dokumen Pendukung
		Vendor	Kadiv GA	
I.	**Proses penempatan kabel jaringan**			
1.	Menentukan penempatan kabel jaringan yang yang tepat dan sesuai dengan kebijakan keamanan informasi			
2.	Melakukan proses penempatan kabel sesuai dengan kebijakan keamanan informasi dan kebutuhan perusahaan			
3.	Melakukan kontrol apakah penempatan kabel jaringan sudah sesuai dan aman			
4.	Melakukan pemeliharaan kabel untuk menjaga kabel agar terhindar dari kerusakan dan gangguan			



No	Aktivitas	Pelaksana		Dokumen Pendukung
		Vendor	Kadiv GA	
II.	**Proses pemeliharaan kabel jaringan**			
1.	Melakukan pelabelan pada setiap kabel jaringan			
2.	Melakukan pembedaan warna kabel untuk memudahkan proses *maintenance*			
3.	Melakukan perlindungan alternatif untuk menjaga keamanan kabel seperti pemasangan pipa untuk melindungi kabel			
4.	Melakukan pemeliharaan kabel 1 kali dalam 6 bulan untuk memastikan tidak ada kabel yang rusak atau terkelupas			
5.	Melakukan pencatatan pada form kegagalan peralatan TI jika ditemukan kerusakan atau gangguan			**FORM/SOP/03**
6.	Melakukan kontrol untuk memastikan pemeliharaan kabel dijalankan dengan baik dan sesuai dengan kebijakan perusahaan			

No	Aktivitas	Pelaksana		Dokumen Pendukung
		Vendor	Kadiv GA	
III.	**Proses perbaikan kabel jaringan**			
1.	Melaporkan kerusakan atau keluhan yang terjadi			
2.	Menentukan jadwal perbaikan kabel			
3.	Melakukan perbaikan pada kabel dan memastikan kerusakan benar-benar tertangani			
4.	Melakukan uji coba dan kontrol selama 1 bulan apakah masih ada kerusakan atau tidak			
5.	Jika perbaikan berhasil maka melakukan pemeliharaan kabel sesuai kebijakan yang ditentukan			

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. FORM	FORM/SOP/03	**TGL. REVISI**	/ /
	NOMOR REVISI	00	**TGL. TERBIT**	/ /
	NAMA FORMULIR	**Formulir laporan kegagalan perangkat TI**		
	PENANGGUNG JAWAB			
	WAKTU PELAKSANAAN	Bulan :	Tahun :	

No.	Deskripsi kegagalan	Jumlah kegagalan	Tanggal Kegagalan	Tindakan Penanganan	Tanggal Penanganan		Staff Penanganan	Status
					Mulai	Selesai		

Dibuat Oleh, Staff Divisi TI	Mengetahui, Kepala Divisi General Affairs
_____ (Nama Lengkap)	_____ (Nama Lengkap)

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. SURAT	KEB/SOP/01	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA KEBIJAKAN	Pengelolaan keamanan perangkat keras dan jaringan		
	PENANGGUNG JAWAB			

V. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan menjamin keamanan aset perangkat keras dan jaringan yang ada pada perusahaan agar dapat digunakan selama berjalannya proses bisnis tanpa adanya gangguan.

VI. RUANG LINGKUP

Cakupan kebijakan ini yaitu berlaku bagi para pihak yang terkait dalam penggunaan, pengelolaan, pemeliharaan, dan pengamanan seluruh aset perangkat keras dan jaringan yang ada pada perusahaan. Adapun aset perangkat keras dan jaringan yang dimaksud terdiri dari :

- PC
- Server
- Printer
- Laptop
- *Mouse*
- *Speaker*
- *Keyboard*
- CPU
- UPS
- Proyektor

VII. REFRENSI

Dalam penyusunan kebijakan ini tentu menggunakan refrensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan refrensi yaitu :

- 11.2.2 *Supporting utilities*
- 11.2.4 *Equipment maintenance*
- 11.2.1 *Equipment siting and protection*
- 11.2.3 *Cabling security*

VIII. KEBIJAKAN

8.1 Pengelolaan keamanan perangkat keras

8.1.1 Segala bentuk kerusakan dan gangguan yang terjadi pada perangkat keras wajib untuk di laporkan kepada pihak yang bertanggung jawab.

8.1.2 Seluruh laporan kerusakan atau gangguan harus segera di proses dan ditangani dalam kurun waktu 2 x 24 jam oleh pihak teknisi TI.

8.1.3 Segala proses perbaikan atau pengadaan peralatan perangkat keras wajib dilakukan pencatatan dan dikonfirmasi paling lambat 1 x 24 jam oleh pihak teknisi TI.

8.1.4 Seluruh perangkat keras yang sudah rusak atau tidak digunakan kembali wajib ditempatkan di ruangan gudang penyimpanan yang sudah disediakan perusahaan.

8.1.5 Seluruh perangkat keras yang sudah rusak atau tidak digunakan kembali tidak boleh dibuang atau diperjual belikan tanpa keputusan pemusnahan media oleh perusahaan.

8.1.6 Dilarang merusak atau mengotak-atik peralatan TI secara sengaja atau tidak jika tidak diberikan izin atau arahan dari pihak teknisi TI yang bertanggung jawab.

8.1.7 Dilarang melakukan pengadaan perangkat keras tambahan jika tidak adanya izin atau perintah dari Kadiv GA.

8.1.8 Dilarang untuk membawa pulang seluruh peralatan perangkat keras dengan alasan apapun.

8.1.9 Pemeliharaan secara berkala wajib dijalankan 1 kali dalam 6 bulan dan tidak boleh menunda penjadwalan pemeliharaan yang sudah ditentukan.

8.1.10 Segala bentuk kerusakan dan pemeliharaan wajib ditangani oleh pihak yang ahli dalam perangkat keras yang ada di perusahaan.

8.1.11 Kadiv GA wajib melakukan kontrol atas proses penggunaan, perbaikan, dan pemeliharaan perangkat keras.

8.1.12 Teknisi TI yang telah ditunjuk wajib bertanggung jawab atas pemeliharaan dan perbaikan yang dilakukan, serta melakukan konfirmasi dan pencatatan pada setiap proses yang dilakukan.

8.1.13 Segala bentuk pengadaan barang wajib dikonfirmasi dan atas persetujuan *Owner* dan Kadiv GA.

8.1.14 Seluruh kegiatan pengelolaan, pemeliharaan, perbaikan, dan penggunaan perangkat keras harus sesuai dengan prosedur keamanan peralatan TI dan mengikuti kebijakan keamanan yang berlaku.

8.1.15 Peralatan TI yang ada diperusahaan hanya boleh digunakan dan dioperasikan oleh seluruh karyawan (kecuali OB) yang merupakan bagian dari perusahaan.

8.1.16 Penggunaan perangkat TI hanya boleh dilakukan pada jam kerja, apabila diluar itu harus melakukan konfirmasi izin kepada Kadiv GA.

8.1.17 Semua perangkat TI kritis dan sangat penting wajib diberikan perlindungan asuransi.

8.1.18 Seluruh perangkat TI wajib dimatikan jika sudah selesai digunakan, kecuali apabila ada kebutuhan mendesak yang mengharuskan PC tetap menyala seperti proses render desain. Namun harus melakukan konfirmasi kepada Kadiv GA

8.1.19 Dalam PC, laptop, dan server wajib dipasang sistem *log in* yang mengharuskan pengguna memasukan ID dan *password*.

8.1.20 Setiap karyawan dan Kadiv GA wajib melakukan kontrol ketersediaan sarana pendukung seperti UPS untuk memastikan proses bisnis terus berjalan.

8.1.21 Setiap perangkat TI harus memiliki perlindungan alternative, seperti adanya silikon pelindung *keyboard*, pelindung layer, dsb.

8.1.22 Apabila kerusakan dan gangguan terjadi maka seluruh karyawan wajib menerapkan kebijakan RDP dalam waktu maksimal 2 jam setelah kerusakan terjadi.

8.2 Pengelolaan keamanan lingkungan perangkat keras

8.2.1 Seluruh perangkat TI harus ditempatkan pada ruangan khusus, aman, dan layak sesuai dengan prosedur yang sudah ditentukan perusahaan.

8.2.2 Seluruh ruangan perangkat TI harus diberikan CCTV yang selalu menyala dan kunci ruangan yang dilakukan setelah jam operasional perusahaan selesai.

8.2.3 Seluruh ruangan yang berisikan aset TI harus diberikan diberikan pendingin ruangan dan sirkulasi udara yang baik untuk mencegah *overheating*.

8.2.4 Dilarang untuk memindahkan seluruh perangkat TI selain pihak yang bertanggung jawab.

8.2.5 Dilarang membawa minuman atau makanan yang bersifat cair kedalam ruangan perangkat TI.

8.2.6 Dilarang merokok dalam ruangan perangkat TI.

8.2.7 Selain staff dan karyawan GeTs Architects dilarang memasuki ruangan perangkat TI, terkecuali atas izin dari Kadiv GA.

8.2.8 Dilarang membawa peliharaan kedalam ruangan perangkat TI.

8.2.9 Ruangan perangkat TI harus selalu dirawat dan dibersihkan untuk menhindari debu dan hewan seperti tikus.

8.2.10 Ruangan perangkat TI harus mendapatkan matahari yang cukup untuk menhindari kelembapan ruangan.

8.3 Pengelolaan keamanan jaringan

8.3.1 Setiap kabel yang ada pada ruangan perangkat TI wajib diberikan pelabelan nama dan fungsi untuk memudahkan konfigurasi dan *maintenance*.

8.3.2 Setiap kabel pada ruang perangkat TI harus dilakukan pembedaan warna untuk memundahkan konfigurasi dan *maintenance*.

8.3.3 Setiap kabel yang ada pada perusahaan harus ditempatkan pada tata letak yang aman tidak terinjak-injak serta wajib diberikan perlindungan pelapisan kabel menggunakan pipa atau karet pelindung kabel.

8.3.4 Setiap kabel yang ada pada ruang perangkat TI tidak boleh terlilit dan harus tersusun dengan rapih untuk mencegah arus pendek.

8.3.5 Pihak Kadiv GA dan teknisi TI wajib melakukan kontrol jaringan dan kabel dalam waktu 1 kali dalam 6 bulan.

8.3.6 Jika ada kerusakan atau gangguan jaringan maka wajib memberikan konfirmasi kepada Kadiv GA.

8.3.7 Setiap proses pemeliharaan dan perbaikan harus dilakukan pencatatan.

8.3.8 Proses pemeliharaan dan *maintenance* wajib dilakukan oleh teknisi TI yang ahli dalam jaringan.

8.3.9 Dilarang menumpuk steker pada terminal listrik untuk mencegah terjadinya konsleting.

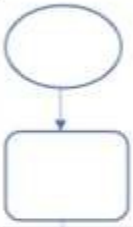
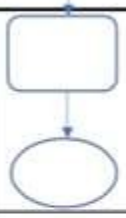
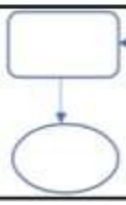
8.3.10 Penempatan kabel jaringan dan kabel listrik harus diletakan ditempat terpisah.

PT. GUBAH ESTETIKA TATA SINERGI	NOMOR SOP	SOP - 09	TGL. PEMBUATAN	/ /
	PENANGGUNG JAWAB		TGL. REVISI	/ /
	NOMOR REVISI		TGL. TERBIT	/ /
	NAMA SOP	**Pengelolaan keamanan hak akses server**		
	RUANG LINGKUP	Server dan SDM		

DESKRIPSI SOP	KUALIFIKASI PELAKSANA
Prosedur pengelolaan keamanan hak akses server merupakan prosedur yang memastikan perusahaan memiliki pedoman proses dalam melakukan kontrol terhadap keamanan hak akses server perusahaan	Pelaksana merupakan pihak yang memiliki tanggung jawab atas hak akses server serta pihak yang mengakases data perusahaan
TUJUAN SOP	**PERLENGKAPAN DAN PERALATAN**
Tujuan dari SOP ini yaitu membantu manajemen melakukan kontrol terhadap tanggung jawab keamanan SDM dalam aktivitas akses server	
REFRENSI	**PIHAK PELAKSANA**
ISO 27002:2013 - 12.4.3 *Administrator & Operation logs* - 7.2.1 *Management responsibilities* - 7.1.2 *Terms and conditions of employment* - 12.4.1 *Event logging*	Kadiv GA, admin, dan karyawan
PERINGATAN	**PENCATATAN DAN PENDATAAN**
Jika SOP ini tidak dijalankan sebagaimana harusnya maka mengakibatkan risiko terhadap kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) data	

KETERANGAN	DIBUAT OLEH	DISETUJUI OLEH	DISAHKAN OLEH
Nama			
Tanggal			
Tanda Tangan	(.....)	(.....)	(.....)

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Admin	Karyawan	Kadiv GA	
I.	**Proses pemberian hak akses server**				
1.	Melakukan permintaan hak akses sever serta konfirmasi atas tujuan dan data yang akan diakses				
2.	Melakukan pelaporan jika informasi dan data yang diakses sangat rahasia dan terbatas				
3.	Melakukan konfirmasi persetujuan atau penolakan perihal permintaan hak akses server				
A	**Jika ditolak**, maka pemohon tidak sesuai dengan ketentuan penerima hak akses				
4.	Melakukan pencatatan pada form pengelolaan akses				
5.	Melakukan konfirmasi kepada pihak pemohon hak akses				
6.	Melakukan tanda tangan pada kontrak hak akses server				FORM/SOP/10
7.	Memberikan akses server kepada pihak yang melakukan permintaan				
8.	Melakukan kontrol bahwa hak akses yang diberikan tidak melanggar prosedur keamanan hak akses				
9.	Memastikan admin menjalankan prosedur pemeberian hak akses dengan baik				

No	Aktivitas	Pelaksana			Dokumen Pendukung
		Admin	Karyawan	Kadiv GA	
II.	**Proses blokir hak akses server**				
1.	Melakukan permintaan dan konfirmasi terkait pengajuan pemblokiran hak akses beserta alasan				
2.	Melakukan pelaporan atas permintaan pemblokiran hak akses				
4.	Melakukan pemeriksaan apakah pemohon melanggar prosedur hak akses dan kontrak atau tidak				
A	**Jika melanggar**, maka sanksi akan diberlakukan				
6.	Melakukan persetujuan untuk pemblokiran hak akses				
7.	Melakukan proses pemblokiran hak akses				

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. FORM	FORM/SOP/10	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA FORMULIR	Formulir kontrak hak akses		

SURAT PERJANJIAN KOMITMEN ATAS KEAMANAN HAK AKSES SERVER

Pada hari ini, ... tanggal ..... bulan ..... tahun ..... bertempat di PT. Gubah Estetika Tata Sinergi. Pihak yang bertanda tangan dibawah ini :

I. **Nama** :
Jabatan :

Dalam hal ini, pihak yang bertanda tangan diatas merupakan pihak pertama yang merupakan penanggung jawab dalam aktivitas pemberian hak akses server

II. **Nama** :
Jabatan :

Dalam hal ini, pihak yang bertanda tangan diatas merupakan pihak kedua yang bertanggung jawab atas aktivitas hak akses server yang sudah diberikan.

Pihak pertama dan pihak kedua merupakan para pihak yang sepakat untuk menandatangani dan menjalani perjanjian komitmen atas keamanan hak akses server, dengan ketentuan dan syarat sebagai berikut :

PASAL 1
PERAN DAN TANGGUNG JAWAB

1.1 Pihak pertama merupakan pihak dengan kedudukan yang tinggi atau setara manajer
- **1.1.1** Pihak pertama merupakan pihak yang bertanggung jawab atas penyerahan aktivitas hak akses kepada pihak kedua
- **1.1.2** Pihak pertama wajib berperan dalam melakukan kontrol atas hak akses server yang telah diberikan
- **1.1.3** Pihak pertama ikut berperan dalam mencegah pelanggaran keamanan hak akses server
- **1.1.4** Apabila terjadi pelanggaran berat atas keamanan hak akses server, maka pihak pertama akan bertanggung jawab sesuai dengan sanksi yang akan diberikan perusahaan

1.2 Pihak kedua merupakan pihak dengan kedudukan dibawah manajer atau disebut karyawan
- **1.2.1** Pihak kedua merupakan pihak yang bertanggung jawab atas aktivitas hak akses server yang telah diberikan oleh pihak kedua
- **1.2.2** Pihak kedua sepenuhnya bertanggung jawab apabila terjadi pelanggaran keamanan hak akses server dan akan menjalani sanksi yang diberikan perusahaan

PASAL 2

KERAHASIAAN INFORMASI

2.1 Segala informasi mengenai atau yang berhubungan dengan perusahaan baik informasi eksternal maupun internal yang disampaikan secara lisan maupun tertulis melewati media langsung maupun tidak langsung merupakan informasi yang bersifat rahasia.

2.2 Segala informasi mengenai atau yang berhubungan dengan transaksi baik informasi eksternal maupun internal yang disampaikan secara lisan maupun tertulis melewati media langsung maupun tidak langsung merupakan informasi yang bersifat rahasia.

2.3 Segala komunikasi mengenai atau yang berhubungan dengan perusahaan baik informasi eksternal maupun internal yang disampaikan secara lisan maupun tertulis melewati media langsung maupun tidak langsung merupakan informasi yang bersifat rahasia.

PASAL 3

INFORMASI TIDAK DILINDUNGI

3.1 Informasi tidak dilindungi merupakan segala informasi yang tersedia untuk umum disampaikan secara lisan maupun tertulis melewati media langsung maupun tidak langsung.

3.2 Informasi tidak dilindungi merupakan segala informasi yang dimana penyampaiannya sudah berada pada pihak penerima yang berhak dan tidak berasal dari sumber lain yang memiliki kewajiban untuk menyampaikan

PASAL 4

KEADAAN MEMAKSA

4.1 Keadaan memaksa merupakan keadaan diluar kendali pihak pertama maupun pihak kedua seperti bencana alam, kebakaran, pembobolan server oleh *hacker*, dan lain-lain.

4.2 Apabila terjadinya pelanggaran keamanan hak akses server dalam keadaan memaksa, maka sanksi yang akan diberikan ke kedua belah pihak akan dipertimbangangkan sesuai dengan kebijakan perusahaan

PASAL 5

PENUTUP

5.1 Kedua belah pihak menyanggupi untuk menjalankan aktivitas dalam menjaga keamanan hak akses server.

5.2 Sanggup untuk setiap saat menjaga kerahasiaan informasi kepada pihak manapun.

5.3 Menyanggupi dalam menghindari penyalahgunaan penggunaan informasi rahasia dengan alasan dan kepentingan apapun.

Surat perjanjian ini dinyatakan sah dan mengikat setelah ditandatangani oleh kedua belah pihak. Surat perjanjian ini dibuat 2 (dua) rangkap dan masing-masing bermatrai mempunyai kedudukan hukum yang sama.

Pihak Pertama	Pihak Kedua
_____	_____
(Nama Lengkap)	(Nama Lengkap)

	PT. GUBAH ESTETIKA TATA SINERGI Divisi General Affairs			
	NO. SURAT	KEB/SOP/03/01	TGL. REVISI	/ /
	NOMOR REVISI	00	TGL. TERBIT	/ /
	NAMA KEBIJAKAN	Kebijakan pengelolaan SDM		
	PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan untuk mengatur dan memastikan SDM ikut berperan aktif dalam menerapkan aktivitas prosedur keamanan informasi pada perusahaan.

II. RUANG LINGKUP

Cakupan kebijakan ini yaitu berlaku bagi seluruh pihak yang menggunakan seluruh aset TI dan aset informasi perusahaan baik pihak internal perusahaan dan pihak ketiga. Pihak yang dimaksud tersebut yaitu :

- Seluruh pegawai GeTs Architects
- Pihak ketiga / vendor
- Pegawai magang / bantuan kerja

III. REFRENSI

Dalam penyusunan kebijakan ini tentu menggunakan refrensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan refrensi yaitu :

- 7.2.1 *Management responsibilities*
- 7.1.2 *Terms and conditions of employment*
- 12.4.3 *Administrator & Operation logs*
- 7.2.2 *Information security, awareness, education, and training*

IV. KEBIJAKAN

4.1 Keamanan SDM dalam penggunaan aset TI dan aset informasi

4.1.1 Seluruh pegawai dan staff GeTs Architects wajib menandatangani kontrak komitmen dalam menerapkan dan menjaga keamanan aset informasi perusahaan.

4.1.2 Seluruh pegawai dan staff wajib diberikan pelatihan dan pengetahuan mengenai aktivitas keamanan informasi minimal 6 bulan 1 kali, sehingga pegawai dan staff memiliki kesadaran dan pengertian akan pentingnya menerapkan keamanan informasi pada perusahaan.

4.1.3 Seluruh pihak ketiga wajib melakukan tanda tangan komitmen kerahasiaan informasi dan penerapan aktivitas keamanan aset informasi pada perusahaan.

4.1.4 Seluruh pegawai magang atau bantuan kerja harus melakukan tanda tangan perjanjian untuk komitmen menerapkan aktivitas keamanan informasi serta menjaga kerahasiaan informasi.

4.1.5 Seluruh pegawai magang atau bantuan kerja wajib diberikan pelatihan dan pengetahuan mengenai aturan dan aktivitas keamanan informasi sebelum menggunakan seluruh aset TI dan aset informasi.

4.1.6 Kadiv GA wajib melakukan kontrol dan evaluasi atas kinerja karyawan dan staff dalam menerapkan aktivitas keamanan informasi minimal 3 bulan 1 kali.

4.1.7 Kadiv GA wajib memberikan sanksi atau peringatan bagi pihak yang melanggar kontrak dan aktivitas keamanan informasi

4.1.8 Seluruh pihak yang ada pada perusahaan wajib menjaga seluruh aset TI dan aset informasi.

4.1.9 Kadiv GA berhak dalam melakukan rotasi posisi apabila hasil evaluasi dan kontrol menunjukan karyawan dan staff tersebut tidak mampu atau tidak berkompenten dalam menjalankan aktivitas keamanan informasi.

4.1.10 Karyawan dilarang melakukan transaksi apapun mengatasnamakan data atau kepentingan perusahaan.

4.2 Keamanan SDM dalam hak akses

4.2.1 Seluruh karyawan yang diberikan hak akses tidak boleh melakukan penyalinan data atau memperbanyak data yang ada pada server tanpa seizin Kadiv GA dan admin dengan alasan apapun.

4.2.2 Seluruh karyawan wajib menjaga ID dan *password* akses server yang telah diberikan, apabila tersebarluaskan maka Kadiv GA berhak memberikan sanksi sesuai keputusan perusahaan.

4.2.3 Melakukan hak akses server hanya boleh dilakukan dalam lingkup perusahaan.

4.2.4 Pegawai magang atau bantuan kerja serta pihak ketiga tidak boleh memiliki hak akses server, apabila ingin melakukan akses harus didampingi oleh admin.

4.2.5 Seluruh data yang dan informasi yang ada pada server tidak boleh difoto, direkam, atau di *screenshoot* dengan alasan apapun.

4.2.6 Admin wajib bertanggung jawab atas kerahasiaan data, keaslian data, dan ketersediaan data.

4.2.7 Admin dan Kadiv GA bertanggung jawab dalam pemberian hak akses server serta pemblokiran hak akses server.

LAMPIRAN

Surat Keterangan Penelitian

SURAT KETERANGAN PENELITIAN

Yang bertanda tangan dibawah ini,

Nama	: Lusiana Tambunan
Jabatan	: Kepala Divisi GA & Finance
Perusahaan	: GeTs Architects
Alamat	: Jl. Bungur I No 4 RT 02/01, Kebayoran Lama Selatan, Kebayoran Lama, Jakarta Selatan, DKI Jakarta, 12240.

Dengan ini menerangkan bahwa,

Nama	: Nadia Magdalena Margaretha Sihombing
NPM	: 171709492
Fakultas/Prodi	: Fakultas Teknologi Industri / Sistem Informasi
Universitas	: Universitas Atma Jaya Yogyakarta

Adalah benar telah melakukan penelitian untuk memenuhi tugas akhir dengan judul **Perancangan SOP (Standar Operasional Prosedur) Manajemen Keamanan Aset Informasi berdasarkan Kontrol Kerangka Kerja ISO27002:2013** dan telah memberikan hasil tugas akhir kepada perusahaan dengan judul dokumen **SOP Keamanan Aset Informasi GeTs Architetcts** pada tanggal 21 Desember 2020.

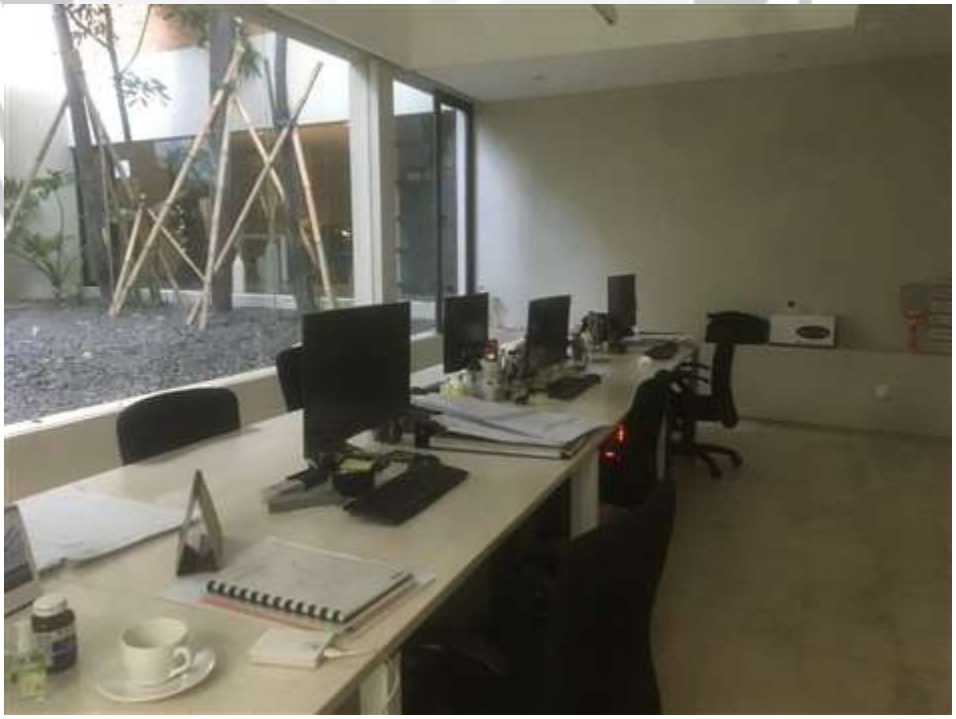
Demikian surat ini dibuat untuk kepentingan pemenuhan persyaratan dalam menyelesaikan tugas akhir.

Jakarta, 21 Desember 2020
Kepala Divisi GA & Finance

Lusiana Tambunan

LAMPIRAN

Foto Observasi di GeTs Architects




KEEP OUR PROMISES
TELL THE TRUTH
LOVE ONE ANOTHER
HAVE FUN

LAMPIRAN

Tabel Revisi

No	Tugas Revisi	Hasil Revisi
1.	Font tulisan tidak konsisten	Font yang digunakan sebelumnya tidak Times New Romans secara keseluruhan maka hasil revisi yaitu semua font sudah diganti menjadi Times New Romans
2.	Rapikan daftar isi	Daftar isi sudah dirapihkan dengan menambahkan *space* dan diatur rata kanan dan kiri
3.	Bab 1 seharusnya belum diberikan penjelasan metode yang digunakan, hanya berisikan ulasan saja	Pada latar belakang, penjelasan metode yang digunakan pada penelitian diganti dan hanya memasukkan penjelasan mengenai penelitian sebelumnya dan kerangka kerja yang digunakan sebagai acuan dalam manajemen keamanan informasi (Hal : 3 dan 4)
4.	*Typo* atau kesalahan penulisan	Sudah diperbaiki dan diganti untuk kata-kata yang salah dalam penulisan.
5.	Perbaikan pada penomoran dan pemanggilan gambar dan tabel	Pada halaman 207 dan 208 sebelumnya gambar mengalami kesalahan dalam penomoran tidak sesuai dengan penomoran sub judul sehingga kini sudah diperbaiki sesuai dengan penomoran sub judul dan nama gambar diubah
6.	Tabel pada bab 2 belum sesuai tamplate	Pada halaman 8 dan 9 sebelumnya tabel yang menjelaskan studi sebelumnya ditulis dalam tabel terpisah dengan dengan tamplate yang berbeda, sehingga diubah menjadi 1 tabel yang

No	Tugas Revisi	Hasil Revisi
		terdiri dari studi sebelumnya yang digunakan dalam penelitian dengan lebih spesifik.
7.	Penulisan rumusan masalah belum tepat	Pada halaman 4 di sub judul perumusan masalah, penjabaran rumusan masalah belum sesuai dan menggabarkan latar belakang masalah secara detail, sehingga diganti menjadi penjabaran latar belakang masalah yang ada pada poin poin latar belakang.
8.	Pertimbangan dalam menggunakan metode yang dipilih	Pada tahapan yang dituliskan di halaman 28 dan 29 sebelumnya belum ada penjelasan mengenai pertimbangan dalam menggunakan metode OCTAVE dan FMEA, sehingga pada sub judul tahapan identifikasi risiko dan analisis risiko sudah dituliskan dasar pada penggunaan metode tersebut yaitu berisikan kegunaan dari masing-masing metode dan kelebihan pada setiap metode yang dijadikan dasar dalam pertimbangan menggunakan metode tersebut.
9.	Kurangnya detail mengenai pihak yang bertanggung jawab pada perancangan SOP di perusahaan	Pada halaman 34 di sub judul identifikasi proses bisnis sebelumnya belum dituliskan mengenai divisi yang bertanggung jawab pada perancangan suatu kebijakan atau SOP pada perusahaan, sehingga dalam halaman 34 juga kini ditambahkan detail masing-masing tanggung jawab dan peran setiap divisi.
10.	Belum ada detail berapa lama proses penyusunan SOP serta pihak yang membantu untuk konsultasi SOP	Pada halaman 178 sub judul perancangan dokumen SOP sudah dituliskan detail waktu perancangan sop dan pihak yang membantu

No	Tugas Revisi	Hasil Revisi
11.	Penulisan judul dengan studi kasus belum tepat	Sebelumnya penulisan judul merupakan perancangan sop keamanan aset informasi berdasarkan kontrol kerangka kerja ISO 27002:2013 (Studi kasus : GeTs Architects) kini diganti menjadi **Perancangan Standar Operasional Prosedur (SOP) Manajemen Keamanan Aset Informasi pada PT. Gubah Estetika Tata Sinergi (GeTs Architects) berdasarkan Kontrol Kerangka Kerja ISO27002:2013**
12.	Detail alasan dalam melakukan analisis risiko untuk dijadikan bahan dalam perancangan SOP	Pada halaman 31 sub judul tahapan penyusunan SOP sudah dituliskan detail pertimbangan dalam melakukan analisis risiko dalam tahapan perancangan SOP
13.	Metode yang digunakan diberi tanda pada setiap tahapan	Sebelumnya penggunaan OCTAVE, FMEA dan ISO27002:2013 sudah dituliskan dalam tahapan identifikasi, analisis risiko, serta justifikasi kebutuhan di halaman 28, 29, dan 31. Sehingga ditambahkan detailnya Kembali pada bab 4 yaitu pada halaman 60, 68, dan 88.