Kebijakan Keamanan Informasi

DIREKTORAT PUSAT TEKNOLOGI INFORMASI
TELKOM UNIVERSITY

JANUARI 2021

Kebijakan Keamanan Informasi
(*Information Security Policy*)

PENGESAHAN

Disusun oleh :			Disahkan oleh :
			
Maya Setyawati KaBag RIYANTI	Widi Tri Yuwono. KaBag ISTI	Alfian Akbar Gozali KaBag DEVTI	Dadang Setiawan Direktur PUTI

Riwayat Revisi (*Revision History*)

Revisi (*Revision*)	Tanggal (*Date*)	Ringkasan Perubahan (*Summary of Changes*)	Pembuat (*Author*)
00	17 Oktober 2016	Terbitan pertama	Manajer Direktorat Sistem Informasi
01	06 Januari 2020	- Penambahan Penomoran Dokumen - Perubahan SOTK & Dasar Penerapan	Manajemen Mutu TI
02	29 Januari 2021	- Penambahan landasan rencana SMKI - Perubahan cakupan SMKI - Penambahan poin Dokumen Terkait - Penambahan klasifikasi informasi pada poin 7. Pengelolaan Aset - Penambahan penerapan poin 8. Pengendalian Akses - Penambahan poin 18. *Clear Desk Clear Screen*	Manajemen Mutu TI

DAFTAR ISI

1. Kebijakan dan Cakupan Sistem Manajemen Keamanan Informasi

1.1 Tujuan

Untuk memberikan arahan kepada manajemen dan memberikan dukungan untuk keamanan informasi sesuai dengan kebutuhan bisnis serta hukum dan peraturan yang relevan.

1.2 Penerapan

1.2.1 Telkom University menyadari bahwa informasi merupakan aset universitas yang harus dijaga. Oleh sebab itu, Telkom University berkomitmen mengimplementasikan Sistem Manajemen Kemananan Informasi (SMKI) yang bertujuan untuk memberikan perlindungan terhadap keamanan informasi sehingga terjamin kerahasiaan, keutuhan serta ketersediaannya yang berstandar internasional. Untuk mencapai hal di atas, Manajemen Puncak Telkom University harus menetapkan Rencana Sistem Manajemen Keamanan Informasi di Lingkungan Telkom University yang didasarkan atas hal-hal berikut ini:

- Peraturan UU No. 11 Th. 2008 tentang Informasi dan Transaksi Elektronik (UU ITE).
- Peraturan Menteri Kominfo No.4/2016 tentang Sistem Manajemen Pengamanan Informasi.
- Peraturan Pemerintah No. 71/2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
- Peraturan Menteri Pendidikan dan Kebudayaan Republik Indonesia Nomor 25 Tahun 2018 tentang Perizinan Berusaha Terintegrasi Secara Elektronik Sektor Pendidikan dan Kebudayaan.
- Keputusan Dewan Pengurus YPT No:KEP.1367/00/DTSP/HK00/YPT/2018 tentang Kebijakan *Cybersecurity*
- Keputusan Dewan Pengurus YPT Nomor: KEP.1267/00/DGS/HK0A/YPT/2019 tentang Peraturan Dasar Kepegawaian

- Standar Internasional ISO/IEC 27001.
- Hasil Kajian Risiko Keamanan Informasi.
- Kebutuhan internal terhadap pengamanan informasi dengan sudut pandang bahwa informasi adalah aset yang harus dilindungi.

1.2.2 Untuk mendukung suksesnya implementasi SMKI di Telkom University, Manajemen Telkom University menetapkan hal-hal berikut:

- Manajemen harus menetapkan sasaran keamanan informasi tahunan, yang merupakan bagian yang tidak terpisahkan dari Sistem Manajemen Kinerja Telkom University.
- Memastikan dipatuhinya segala peraturan dan perundangan yang berlaku terkait dengan keamanan informasi.
- Memastikan dilakukannya asesmen risiko keamanan informasi secara berkala.
- Memastikan bahwa tersedianya dokumentasi pendukung yang diperlukan untuk mengimplementasikan bab-bab ketentuan keamanan informasi yang tertulis dalam dokumen ini.
- Menyediakan sumber daya yang diperlukan agar implementasi SMKI dapat berlangsung secara efektif.
- Melakukan pemantauan terhadap pencapaian sasaran keamanan informasi.
- Memastikan terselenggaranya audit internal SMKI yang dilaksanakan sesuai dengan ketentuan perusahaan.
- Memastikan dilaksanakannya tinjauan manajemen SMKI, setidaknya satu kali dalam setiap tahun.
- Memastikan bahwa peningkatan berkelanjutan terhadap implementasi SMKI akan selalu dilaksanakan.

1.2.3 Ruang lingkup dari implementasi SMKI ini mencakup :

- Organisasi : Unit Infrastruktur TI, Direktorat Pusat TI
- Lokasi : Telkom University, Gedung Panambulai, Jl. Telekomunikasi No 1, Terusan Buah Batu, Kabupaten Bandung

- Proses bisnis / Layanan : Layanan Internet Akses
- Aset :

1. Data / Informasi :

   Dokumen pengadaan dan kontrak *vendor* perangkat infrastruktur, *data user internet*, dokumen teknis & konfigurasi jaringan, hasil *penetration test*, prosedur operasional, rekaman operasional penggunaan TI, BCP dan hasil audit, dsb.

2. Software :

   Aplikasi *monitoring, syslog*, aplikasi *user management , captive portal*, aplikasi dns *filter* dan *resolver*, windows server 2012, MSSQL server, aplikasi *remote* perangkat.

3. Hardware :

   Server monitoring, server syslog, server user management, server captive portal, server DNS filter dan *resolver*, laptop, media penyimpanan data.

4. Perangkat Jaringan Telekomunikasi :

   Router BGP, *firewall data center, firewall user, switch publik, router core, switch core, switch distribution*.

5. Sumber Daya Manusia :

   Staf Unit Infrastruktur TI.

6. Fasilitas Pendukung :

   Rak *network center,* rak *network distribution,* ruang NOC, UPS, PAC, CCTV, *access door, fire extinguisher.*

2. Standar Penerapan Sistem Manajemen Keamanan Informasi

2.1 Tujuan

Standar ini bertujuan memberikan panduan dalam melakukan implementasi Sistem Manajemen Keamanan Informasi (SMKI) di lingkungan Telkom University dengan menggunakan proses siklus P-D-C-A *(Plan-Do-Check-Act)* berbasis ISO/IEC

27001:2013, sehingga aset informasi Telkom University dapat terlindungi dari aspek kerahasiaan *(confidentiality)*, keutuhan *(integrity)*, dan ketersediaan *(availability)*.

2.2 Penerapan

2.2.1 Proses perencanaan *(Plan),* meliputi kegiatan:

- Menentukan isu internal dan eksternal yang dapat mempengaruhi proses implementasi SMKI;
- Menentukan pihak-pihak terkait proses implementasi SMKI serta mengidentifikasi persyaratan dan kebutuhan keamanan informasinya;
- Menentukan ruang lingkup penerapan SMKI;
- Menetapkan suatu komitmen manajemen terhadap penerapan SMKI;
- Mengkomunikasikan dan mensosialisasikan pedoman keamanan informasi.
- Melakukan asesmen risiko keamanan informasi;
- Menyusun Rencana Mitigasi Risiko Keamanan Informasi;
- Menentukan sasaran penerapan SMKI; dan
- Menentukan sumber daya yang diperlukan untuk penerapan SMKI.

2.2.2 Proses Pelaksanaan *(Do),* meliputi kegiatan:

- Pendokumentasian proses pelaksanaan SMKI;
- Menilai risiko keamanan informasi ketika ada penambahan risiko baru atau terdapat perubahan signifikan yang dapat mempengaruhi keamanan informasi;
- Melaksanakan *awareness* dan pelatihan SMKI;
- Melakukan pengadaan dan pengelolaan sumber daya untuk mendukung pelaksanaan penerapan SMKI; dan
- Menjalankan penerapan SMKI sesuai sasaran yang telah ditetapkan pada proses perencanaan (*plan*)

2.2.3 Proses Evaluasi *(Check),* meliputi kegiatan:

- Menilai keefektifan implementasi pengendalian keamanan informasi sekurang-kurangnya dilakukan satu kali dalam satu tahun.

- Memantau dan melaporkan pencapaian sasaran SMKI sekurang-kurangnya dilakukan satu kali dalam satu tahun.
- Mereviu hasil asesmen risiko minimal setiap enam bulan sekali.
- Melakukan audit internal penerapan SMKI yang dilakukan minimal satu kali dalam satu tahun.
- Melakukan Tinjauan Manajemen terhadap penerapan SMKI yang dilakukan sekurang-kurangnya satu kali dalam satu tahun.

2.2.4 Proses Tindak Lanjut *(Act),* meliputi kegiatan:

- Memantau penerapan rencana tindakan perbaikan hasil audit internal.
- Melakukan peningkatan berkelanjutan terhadap penerapan Sistem Manajemen Keamanan Informasi (SMKI) setiap tahunnya dengan melakukan perencanaan (*plan*) kembali.

2.3 Dokumen Terkait

- Dokumen Rencana Strategis Direktorat Pusat Teknologi Informasi 2019-2023
- Dokumen Integrated Management System Plan
- Dokumen Laporan Audit Internal dan / atau Eksternal

3. Manajemen Risiko Keamanan Informasi

3.1 Tujuan

Untuk memberikan panduan dalam melakukan penilaian risiko dan mengevaluasi kecukupan risiko keamanan informasi berdasarkan kriteria yang ditentukan yaitu kerahasiaan, keabsahan dan ketersediaan (CIA: *Confidentiality, Integrity, and Availability*).

3.2 Penerapan

3.2.1 Penilaian risiko keamanan informasi secara berkala perlu dilakukan untuk menghadapi prioritas-prioritas bisnis yang berubah dan ancaman-ancaman baru terhadap keamanan informasi.

3.2.2 Penilaian risiko keamanan informasi membantu mengidentifikasi risiko-risiko terkait keamanan informasi dan memungkinkan untuk melakukan mitigasi

terhadap risiko tersebut dengan menggunakan pengendalian yang sesuai. Dari hasil penilaian risiko keamanan informasi tersebut dapat ditentukan prioritas serta tindakan yang tepat dalam menerapkan pengendalian keamanan informasi berdasarkan suatu tingkat risiko yang dapat diterima (ARL, *acceptable risk level*) oleh perusahaan. Manajemen SMKI mengevaluasi kecukupan risiko keamanan informasi berdasarkan kriteria sebagai berikut:

- Kendala-kendala keuangan dan sumber daya pada saat ini,
- Rekomendasi dari pihak yang terkait,
- Hasil-hasil audit SMKI serta audit sistem informasi dan
- Kecenderungan insiden keamanan yang terjadi di masa lalu

3.2.3 Tingkat risiko keamanan informasi yang dapat diterima (ARL, *acceptable risk level*) harus dikaji ulang setiap tahun dan digunakan sebagai bagian dari masukan untuk manajemen risiko perusahaan. Maksud untuk penyelarasan dengan manajemen risiko strategis adalah untuk mengkoordinasikan keputusan risiko jangka panjang dengan unit-unit bisnis dan untuk meningkatkan kesadaran terhadap persoalan-persoalan yang sedang dihadapi.

3.3 Dokumen Terkait

- Dokumen Pedoman Pengelolaan Resiko
- Dokumen Risk Register

4. Struktur Tata Kelola Dokumentasi SMKI

4.1 Tujuan

4.1.1 Untuk menjabarkan struktur dokumentasi yang diterapkan oleh Telkom University.

4.1.2 Mengidentifikasi aset TI yang digunakan dalam penyelenggaraan layanan TI di Universitas Telkom.

4.2 Penerapan

Dengan menggunakan peta dokumentasi ISMS, pedoman-pedoman khusus, standar-standar khusus dan prosedur-prosedur khusus diidentifikasi. Penerapan dokumentasi ini adalah khusus untuk lingkungan yang telah ditetapkan.

4.3 Dokumen Terkait

- Prosedur Pengendalian Informasi Terdokumentasi

Jenis Dokumen	Definisi
Kebijakan	Dokumen kebijakan teknologi informasi di Telkom University.
Pedoman	Dokumen yang memberikan pedoman dalam implementasi keamanan informasi
Standar	Dokumen yang berisi persyaratan minimum dan ditetapkan berdasarkan konsensus para pemangku kepentingan dalam implementasi keamanan informasi
Prosedur	Dokumen yang berisi tata cara untuk menjalankan proses implementasi keamanan informasi
Formulir	Dokumen untuk merekam semua kegiatan implementasi keamanan informasi agar hasilnya dapat didokumentasikan

5. Organisasi Keamanan Informasi

5.1 Tujuan

5.1.1 Untuk mendirikan sebuah *framework* manajemen untuk memulai dan mengendalikan proses implementasi dan operasional dari keamanan informasi dalam perusahaan.

5.2 Penerapan

5.2.1 Semua tanggung jawab keamanan informasi harus ditetapkan dan dialokasikan.

5.2.2 Tugas yang bertentangan dan area tanggung jawab harus dipisahkan untuk mengurangi peluang bagi modifikasi yang tidak sah atau tidak disengaja atau penyalahgunaan aset perusahaan.

5.2.3 Mengidentifikasi dan menjalin kerjasama dengan pihak berwenang serta komunitas keamanan informasi diluar perusahaan.

5.2.4 Pengendalian terhadap keamanan informasi harus diterapkan dalam pengelolaan proyek dan harus diaplikasikan pada seluruh fase dalam metodologi pengelolaan proyek.

5.3 Dokumen Terkait

- Dokumen SOTK dan *Job Description*
- Eviden kerjasama dengan pihak berwenang dan/atau keikutsertaan dalam komunitas keamanan informasi
- Dokumen proses pengelolaan proyek (Prosedur, Instruksi Kerja, Standar, Aturan)

6. Keamanan Sumber Daya Manusia

6.1 Tujuan

6.1.1 Untuk memastikan bahwa para karyawan dan pekerja kontrak mengerti akan peran dan tanggung jawab dari pekerjaan mereka dan sesuai terhadap peran dan tanggung jawab yang mereka ambil.

6.1.2 Untuk memastikan bahwa para karyawan dan pekerja kontrak mengetahui dan melaksanakan peran dan tanggung jawab terhadap keamanan informasi.

6.1.3 Untuk melindungi kepentingan universitas sebagai bagian dari proses penerimaan, perubahan/mutasi dan pemutusan tenaga kerja.

6.2 Penerapan

6.2.1 Pemeriksaan latar belakang pada semua calon karyawan dan pekerja kontrak harus dilakukan sesuai dengan hukum, peraturan dan etika yang berlaku.

6.2.2 Perjanjian kontrak dengan karyawan dan pekerja kontrak harus menyatakan peran dan tanggung jawab mereka terhadap keamanan informasi.

6.2.3 Manajemen harus mensyaratkan seluruh karyawan dan pekerja kontrak untuk menerapkan keamanan informasi sesuai dengan kebijakan dan prosedur yang berlaku di institusi.

6.2.4 Seluruh karyawan dan pekerja kontrak di Telkom University perlu diberikan pendidikan, sosialiasi dan pelatihan terkait keamanan informasi sesuai dengan fungsi pekerjaan mereka.

6.2.5 Harus ada proses pemberian sanksi yang formal dan dikomunikasikan untuk mengambil tindakan terhadap karyawan yang melakukan pelanggaran keamanan informasi, sesuai dengan kebijakan dan prosedur yang berlaku di institusi.

6.2.6 Perlu dipastikan bahwa peran dan tanggung jawab keamanan informasi tetap diterapkan apabila terjadi perubahan atau terminasi terhadap karyawan.

6.3 Dokumen Terkait

- Surat Keterangan Catatan Kepolisian
- Dokumen NDA Pegawai dan Pihak Ketiga
- Dokumen Laporan Training Pegawai
- Awareness Keamanan Informasi
- Aplikasi Penilaian Kinerja

7. Pengelolaan Aset

7.1 Tujuan

7.1.1 Untuk mengidentifikasi aset-aset milik Telkom University dan menetapkan tanggung jawab terhadap perlindungan yang tepat dari asset-aset tersebut.

7.1.2 Untuk memastikan keamanan informasi tepat sesuai dengan tingkat kepentingan informasi

7.1.3 Untuk mencegah kebocoran, modifikasi, penghapusan, dan penghancuran informasi yang disimpan oleh pihak yang tidak berwenang.

7.2 Penerapan

7.2.1 Aset terkait dengan informasi dan fasilitas pengolahan informasi harus diidentifikasi dan diinventarisasi. Inventarisasi aset ini harus dibuat dan dipelihara secara berkala, serta ditetapkan penanggung jawab masing-masing aset tersebut.

7.2.2 Pemilik aset TI bertanggung jawab menetapkan dan menerapkan kontrol-kontrol pengamanan atas aset TI yang dikelolanya untuk melindungi aset TI

tersebut dari ancaman kerahasiaan, keutuhan dan ketersediaan selama siklus masa berlakunya.

7.2.3 Menerapkan aturan terhadap penggunaan informasi dan aset pada perusahaan.

7.2.4 Semua karyawan dan pengguna pihak eksternal harus mengembalikan seluruh aset milik Telkom University yang mereka gunakan ketika terjadi pemutusan hubungan kerja, kontrak atau perjanjian.

7.2.5 Aset informasi diklasifikasikan sesuai tingkat kerahasiaan, nilai, tingkat kritikalitas, serta aspek hukumnya.

Klasifikasi	Definisi
Rahasia	Informasi yang membutuhkan pengamanan tinggi/ketat dan hanya boleh diketahui oleh pimpinan dan /atau personil tertentu yang ditetapkan. Pembocoran informasi ini secara tidak berwenang dapat menimbulkan risiko yang TINGGI/BESAR bagi Universitas Telkom, seperti antara lain: ▪ kehilangan reputasi; ▪ ketidakpatuhan terhadap regulasi; ▪ kerugian finansial yang besar; atau ▪ terganggunya layanan TI dalam jangka lama. <u>Jenis informasi yang termasuk klasifikasi ini antara lain</u>: Topologi jaringan dengan IP Address, hasil *penetration test*, hasil penilaian kinerja karyawan, *log system administrator*, dan informasi rahasia lainnya.
Terbatas	Informasi yang telah terdistribusi di lingkungan internal Universitas Telkom yang penyebarannya secara internal tidak memerlukan persetujuan dari pemilik informasi. Risiko kebocoran informasi secara tak berwenang ke pihak luar berkategori SEDANG/MENENGAH, tidak sebesar risiko informasi berklasifikasi "Rahasia" <u>Jenis informasi yang termasuk klasifikasi ini antara lain</u>: Kebijakan dan prosedur, laporan audit (internal/eksternal), hasil kajian risiko, risalah rapat internal dan laporan operasional layanan TI yang

	tidak bersifat “Rahasia”, dokumen kontrak, dan informasi lain yang diklasifikasi "Terbatas".
Biasa	Informasi yang tidak memerlukan pengamanan dari aspek kerahasiaan atau informasi yang secara sengaja disediakan bagi publik. Jenis informasi yang termasuk klasifikasi ini antara lain: Brosur layanan dan website dengan domain telkomuniversity.ac.id, dan informasi lainnya yang disediakan bagi publik.

7.2.6 Pemberian label klasifikasi aset informasi harus dilakukan secara konsisten terhadap seluruh aset informasi.

7.2.7 Aset informasi harus ditangani sesuai dengan skema klasifikasi informasi yang diadopsi.

7.2.8 Menetapkan aturan untuk pengelolaan *removable media* sesuai dengan skema klasifikasi yang diadopsi.

7.2.9 Media penyimpanan yang memuat informasi harus dibuang/dihancurkan dengan metode yang aman ketika tidak lagi diperlukan.

7.2.10 Pengiriman media penyimpanan yang memuat informasi harus dilindungi terhadap akses yang tidak sah serta penyalahgunaan selama proses pengiriman.

7.3 Dokumen Terkait

- Pengelolaan Aset dan Klasifikasi Informasi
- Aplikasi Aset Management
- Instruksi Kerja Gangguan dan Perbaikan Perangkat

8. Pengendalian Akses

8.1 Tujuan

8.1.1 Untuk membatasi akses terhadap informasi dan perangkat pemrosesan informasi.

8.1.2 Untuk memastikan hanya pengguna yang berwenang yang dapat mengakses informasi dan untuk mencegah pihak yang tidak berwenang masuk ke dalam sistem dan layanan.

8.1.3 Untuk memastikan pengguna bertanggung jawab dalam menjaga otentikasi terhadap informasi.

8.1.4 Memastikan dan mencegah adanya akses secara tidak berwenang terhadap informasi dan fasilitas sistem informasi baik aplikasi, sistem operasi, internet dan akses ruang server (*data center* dan *network center*).

8.2 Penerapan

8.2.1 Sebuah aturan terkait pengendalian akses harus ditetapkan, didokumentasikan dan ditinjau berdasarkan persyaratan keamanan bisnis dan informasi.

8.2.2 Pengguna hanya boleh disediakan akses ke layanan jaringan dan jaringan yang telah secara khusus diizinkan bagi mereka untuk digunakan.

8.2.3 Proses pendaftaran dan penghapusan akses pengguna harus diterapkan.

8.2.4 Proses penyediaan akses pengguna terhadap sumber informasi harus diterapkan untuk semua jenis pengguna pada semua sistem dan layanan.

8.2.5 Alokasi dan penggunaan hak akses khusus harus dibatasi dan dikontrol.

8.2.6 Alokasi terhadap informasi otentikasi rahasia (seperti kata sandi) harus dikendalikan melalui proses pengelolaan secara formal.

8.2.7 Pemilik aset harus meninjau hak akses pengguna secara berkala.

8.2.8 Hak akses dari seluruh karyawan dan pengguna pihak eksternal terhadap informasi dan fasilitas pengolahan informasi harus dihapus setelah pemutusan hubungan kerja mereka, pemutusan kontrak atau perjanjian.

8.2.9 Pengguna wajib mematuhi peraturan penggunaan informasi otentikasi rahasia (seperti kata sandi).

8.2.10 Akses terhadap sistem informasi dan aplikasi harus dibatasi sesuai dengan peraturan pengendalian akses yang berlaku.

8.2.11 Akses ke sistem dan aplikasi harus dikendalikan dengan menggunakan metodologi *log-on* yang aman.

8.2.12 Mekanisme pengelolaan kata sandi harus interaktif dan harus memastikan kata sandi yang berkualitas.

8.2.13 Penggunaan program utilitas/alat bantu yang mungkin mampu meng-override sistem dan aplikasi harus dibatasi dan dikendalikan dengan ketat.

8.2.14 Akses ke kode sumber *(source code)* program harus dibatasi.

8.2.15 Hak akses, baik lojik maupun fisik (data center, network center dan seluruh ruangan karyawan di Direktorat Pusat TI) diberikan secara terbatas sesuai tugas pokok dan kewenangan pengguna. Pemberian hak akses tentunya harus disetujui minimum oleh Kepala Bagian yang berwenang.

8.2.16 Akses yang tingkatnya tinggi seperti administrator, hanya digunakan untuk kegiatan yang memerlukan pengguna administrator saja. Akses administrator tidak digunakan untuk melakukan pekerjaan operasional biasa. Untuk itu karyawan yang mendapatkan akses administrator bersifat terbatas.

8.3 Dokumen Terkait

- Matriks Hak Akses
- Kebijakan Keamanan Infrastruktur

9. Penggunaan Kriptografi

9.1 Tujuan

Tujuannya adalah untuk memastikan penggunaan yang tepat dan efektif terhadap kriptografi untuk melindungi kerahasiaan, keabsahan, dan integritas dari informasi.

9.2 Penerapan

9.2.1 Sebuah standar tentang penggunaan pengendalian kriptografi untuk perlindungan informasi harus dikembangkan dan diterapkan.

9.2.2 Menetapkan dan menerapkan standar untuk penggunaan dan perlindungan terhadap kunci kriptografi.

9.3 Dokumen Terkait

- *Evidence* enskripsi pada aplikasi / trafik data

10. Pengelolaan Keamanan Fisik dan Lingkungan

10.1 Tujuan

10.1.1 Untuk mencegah akses, kerusakan, dan campur tangan terhadap informasi dan perangkat pemrosesan informasi di Telkom University oleh pihak yang tidak berwenang.

10.1.2 Untuk mencegah terjadinya kerugian, kerusakan, pencurian atau hal-hal yang dapat membahayakan *asset* serta interupsi terhadap operasional di Telkom University.

10.2 Penerapan

10.2.1 Parameter keamanan harus ditetapkan dan digunakan untuk melindungi daerah-daerah yang berisi informasi dan fasilitas pengolahan informasi yang sensitif atau kritis.

10.2.2 Area aman harus dilindungi oleh pengendalian masuk yang tepat untuk menjamin bahwa hanya personil berwenang yang diperbolehkan untuk mengakses.

10.2.3 Keamanan fisik untuk kantor, ruangan dan fasilitas harus dirancang dan diterapkan.

10.2.4 Perlindungan fisik terhadap bencana alam, serangan berbahaya atau kecelakaan harus dirancang dan diterapkan.

10.2.5 Aturan untuk bekerja di area aman harus dirancang dan diterapkan.

10.2.6 Jalur akses seperti area pengiriman dan area bongkar muat di mana orang yang tidak berwenang bisa memasuki tempat tersebut harus dikendalikan dan, jika mungkin, diisolasi dari fasilitas pengolahan informasi untuk menghindari akses yang tidak sah.

10.2.7 Peralatan harus diletakkan dan dilindungi untuk mengurangi risiko dari ancaman lingkungan dan bahaya, dan kesempatan terhadap akses oleh yang tidak berwenang.

10.2.8 Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam fasilitas pendukung.

10.2.9 Kabel daya dan kabel telekomunikasi yang dilalui data harus dilindungi dari intersepsi, gangguan atau kerusakan.

10.2.10 Peralatan harus dipelihara dengan benar untuk memastikan aspek ketersediaan dan integritas.

10.2.11 Peralatan, informasi atau perangkat lunak tidak boleh dibawa keluar lokasi tanpa izin sebelumnya.

10.2.12 Keamanan harus diterapkan untuk aset yang berada diluar lokasi dengan memperhitungkan risiko yang berbeda dari bekerja di luar tempat perusahaan.

10.2.13 Semua peralatan yang mengandung media penyimpanan harus diverifikasi untuk memastikan bahwa setiap data sensitif dan perangkat lunak berlisensi telah dihapus atau ditimpa secara aman sebelum dibuang atau digunakan kembali.

10.2.14 Pengguna harus memastikan bahwa perangkat pengolah informasi yang ditinggal tanpa pengawasan memiliki perlindungan dari akses yang tidak berwenang.

10.2.15 Menetapkan aturan mengenai kebersihan area kerja dari dokumen kertas dan media penyimpanan *removable* dan fasilitas pengolahan informasi.

10.3 Dokumen Terkait

- Peta *Physical Security Area*
- Buku *Access Log* ruang NOC dan *Data Center*
- Ketentuan Ruang Kerja

11.Keamanan Operasional

11.1 Tujuan

11.1.1 Untuk memastikan proses yang benar dan aman terhadap operasional perangkat pemrosesan informasi.

11.1.2 Untuk memastikan bahwa informasi serta perangkat pemrosesan informasi terlindungi dari ancaman malware (virus, trojan, dsb).

11.1.3 Untuk melindungi dari kehilangan data.

11.1.4 Untuk mencatat kejadian (*event*) pada perangkat pengolah informasi.

11.1.5 Untuk memastikan integritas dari sistem informasi.

11.1.6 Untuk mencegah eksploitasi terhadap kerentanan teknis (*Technical Vulnerabilities*).

11.1.7 Untuk meminimalisir dampak dari aktifitas audit terhadap sistem operasional.

11.1.8 Untuk memastikan keamanan terhadap penggunaan *Teleworking* (berkerja jarah jauh) dan penggunaan *Mobile Device*.

11.2 Penerapan

11.2.1 Prosedur operasional harus didokumentasikan dan tersedia untuk semua pengguna yang membutuhkannya.

11.2.2 Perubahan terhadap perusahaan, proses bisnis, fasilitas pengolahan informasi dan sistem yang mempengaruhi keamanan informasi harus dikendalikan.

11.2.3 Penggunaan sumber daya harus dimonitor, dievaluasi dan diproyeksikan dari kebutuhan kapasitas di masa depan untuk memastikan kinerja sistem yang diperlukan.

11.2.4 Pengembangan, pengujian, dan operasional lingkungan harus dipisahkan untuk mengurangi risiko akses yang tidak sah atau perubahan lingkungan operasional.

11.2.5 Pendeteksian, pencegahan dan pemulihan kontrol untuk perlindungan terhadap malware harus diterapkan.

11.2.6 Salinan *back-up* dari informasi, perangkat lunak dan hasil *image* dari sistem harus disimpan dan diuji secara teratur sesuai dengan aturan *back-up* yang telah disepakati.

11.2.7 Log kejadian yang berfungsi untuk merekam kegiatan pengguna dan kejadian keamanan informasi pada perangkat TI harus diterapkan, disimpan dan di kaji secara berkala.

11.2.8 Fasilitas *Logging* dan informasi log harus dilindungi terhadap gangguan dan akses yang tidak sah.

11.2.9 Kegiatan dari operator dan administrator sistem harus tercatat (*logged*) dan catatan (*log*) tersebut harus dilindungi dan dikaji secara berkala.

11.2.10 Jam (waktu) dari semua sistem pengolahan informasi yang relevan harus disinkronisasikan sesuai referensi sumber waktu tunggal.

11.2.11 Peraturan harus ditetapkan untuk mengendalikan instalasi perangkat lunak pada sistem operasional dan instalasi yang dilakukan oleh pengguna.

11.2.12 Informasi tentang kerentanan teknis terhadap sistem informasi yang digunakan harus diperoleh secara tepat waktu, paparan untuk kerentanan tersebut perlu dievaluasi dan langkah yang tepat harus diambil untuk mengatasi risiko yang terkait.

11.2.13 Audit yang dilakukan terhadap system informasi harus direncanakan dengan hati-hati dan disetujui untuk meminimalkan gangguan terhadap proses bisnis.

11.2.14 Sebuah aturan harus ditetapkan untuk mengelola risiko yang diperkenalkan oleh penggunaan *mobile device*.

11.2.15 Sebuah aturan harus ditetapkan untuk melindungi informasi yang diakses, diproses atau disimpan pada perangkat *teleworking*.

11.3 Dokumen Terkait

- Aplikasi *Configuration Management Database*
- Laporan Performasi Triwulan
- *Capacity Plan*
- Laporan pengujian *backup* dan *restore*
- Peraturan *mobile device* dan *teleworking*

12. Keamanan Komunikasi

12.1 Tujuan

12.1.1 Untuk memastikan adanya perlindungan terhadap informasi di dalam jaringan dan dukungan terhadap perangkat pemprosesan informasi pada jaringan.

12.1.2 Untuk menjaga keamanan terhadap informasi yang dipertukarkan di lingkungan Telkom University maupun yang dipertukarkan di luar lingkungan Telkom University.

12.2 Penerapan

12.2.1 Jaringan harus dikelola dan dikendalikan untuk melindungi informasi yang berada dalam sistem dan aplikasi.

12.2.2 Mekanisme keamanan, tingkat layanan dan persyaratan manajemen dari seluruh layanan jaringan harus diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan, terlepas apakah layanan ini disediakan sendiri atau menggunakan jasa pihak ketiga.

12.2.3 Grup dari layanan informasi, pengguna dan sistem informasi di dalam jaringan harus dipisahkan.

12.2.4 Aturan terkait pengalihan informasi harus ditetapkan untuk melindungi pengalihan informasi melalui penggunaan semua jenis fasilitas komunikasi.

12.2.5 Perjanjian harus membahas tentang pengalihan yang aman terhadap informasi bisnis antara Telkom University dan pihak luar.

12.2.6 Informasi yang terlibat dalam pesan elektronik harus dilindungi secara tepat.

12.2.7 Persyaratan untuk kerahasiaan atau perjanjian kerahasiaan (*non-disclosure agreement*) yang mencerminkan kebutuhan internal Telkom Univeristy untuk perlindungan informasi harus diidentifikasi, dikaji secara berkala dan didokumentasikan.

12.3 Dokumen Terkait

- Topologi Jaringan
- SLA
- NDA dengan Pihak Ketiga

13. Akuisisi, Pengembangan dan Pemeliharaan Sistem

13.1 Tujuan

13.1.1 Untuk memastikan bahwa keamanan informasi adalah bagian yang tidak terpisahkan dari siklus hidup sistem informasi. Hal ini juga mencakup kebutuhan sistem informasi yang menyediakan layanan melalui jaringan publik.

13.1.2 Untuk memastikan bahwa keamanan informasi dibuat dan diterapkan dalam siklus pengembangan sistem informasi.

13.1.3 Untuk memastikan perlindungan terhadap data yang digunakan untuk pengujian (*testing*).

13.2 Penerapan

13.2.1 Kebutuhan terkait keamanan informasi harus dimasukkan dalam persyaratan untuk perancangan sistem informasi yang baru atau ditambahkan pada sistem informasi yang sedang berjalan.

13.2.2 Informasi yang terlibat dalam layanan aplikasi yang melewati jaringan publik harus dilindungi dari kegiatan kecurangan, pengungkapan yang tidak sah serta kegiatan modifikasi.

13.2.3 Informasi yang terlibat dalam transaksi layanan aplikasi harus dilindungi untuk mencegah transmisi data yang tidak lengkap, mis-routing, perubahan pesan yang tidak sah, pengungkapan yang tidak sah, duplikasi pesan yang tidak sah.

13.2.4 Peraturan untuk pengembangan sistem dan perangkat lunak harus ditetapkan dan diterapkan untuk proses pengembangan di dalam institusi.

13.2.5 Perubahan terhadap sistem dalam siklus pengembangan harus dikendalikan dengan menggunakan prosedur pengendalian perubahan yang formal.

13.2.6 Ketika terjadi perubahan platform/sistem operasi, aplikasi bisnis yang penting harus ditinjau dan diuji untuk memastikan bahwa tidak ada dampak buruk dari perubahan tersebut terhadap keamanan informasi.

13.2.7 Melakukan modifikasi terhadap paket perangkat lunak (*software package*) harus diminimalkan, hanya terbatas pada perubahan yang diperlukan dan semua perubahan harus dikendalikan secara ketat.

13.2.8 Prinsip untuk rekayasa sistem yang aman harus ditetapkan, didokumentasikan, dipelihara dan diterapkan untuk setiap upaya implementasi sistem informasi.

13.2.9 Direktorat Pusat TI harus menetapkan dan melindungi lingkungan pengembangan yang aman untuk proses pengembangan dan integrasi sistem yang menjangkau seluruh siklus hidup pengembangan sistem.

13.2.10 Direktorat Pusat TI harus mengawasi dan memantau aktivitas pengembangan sistem yang dialihdayakan (*outsourced*).

13.2.11 Pengujian fungsi keamanan harus dilakukan selama proses pengembangan.

13.2.12 Program pengujian penerimaan (*acceptance testing*) dan kriteria terkait harus ditetapkan untuk sistem informasi yang baru, yang di-*upgrade* dan menggunakan versi baru.

13.2.13 Data Pengujian harus dipilih dengan hati-hati, dilindungi dan dikendalikan.

13.3 Dokumen Terkait

- -

14. Pengendalian Pihak Ketiga (Vendor/Pemasok)

14.1 Tujuan

14.1.1 Untuk memastikan terlindungnya aset-aset milik Telkom University yang dapat diakses oleh pihak ketiga.

14.1.2 Untuk mempertahankan tingkat keamanan informasi dan pelayanan yang telah disepakati dengan pihak ketiga.

14.2 Penerapan

14.2.1 Melakukan kesepakatan dengan pemasok terhadap persyaratan keamanan Informasi untuk mengurangi risiko yang terkait dengan akses pemasok ke dalam aset perusahaan.

14.2.2 Semua persyaratan keamanan informasi yang relevan harus ditetapkan dan disetujui oleh setiap pemasok yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur TI untuk informasi perusahaan.

14.2.3 Perjanjian dengan pemasok harus meliputi persyaratan untuk mengatasi risiko keamanan informasi yang terkait dengan teknologi informasi dan komunikasi layanan serta rantai suplai produk.

14.2.4 Telkom University harus secara teratur memonitor, mereviu dan melakukan audit terhadap pelayanan dari pemasok.

14.2.5 Perubahan terhadap penyediaan layanan oleh pemasok harus dikelola, dengan mempertimbangkan kritikalitas dari informasi bisnis, sistem dan proses yang terlibat serta kajian risiko.

14.3 Dokumen Terkait

- NDA dengan Pihak Ketiga
- Penilaian Layanan Pihak Ketiga

15. Pengelolaan Insiden Keamanan Informasi

15.1 Tujuan

15.1.1 Untuk memastikan sebuah pendekatan yang efektif dan konsisten terhadap pengelolaan insiden keamanan informasi dan mencakup komunikasi pada kejadian *(event)* dan kelemahan *(weakness)* terkait keamanan Informasi.

15.1.2 Untuk memastikan agar peristiwa dan kelemahan keamanan informasi yang berhubungan dengan sistem informasi di komunikasikan secepat mungkin agar dapat di ambil tindakan perbaikan yang tepat.

15.2 Penerapan

15.2.1 Tanggung jawab dan prosedur pengelolaan insiden harus ditetapkan untuk memastikan respon yang cepat, efektif dan teratur terhadap insiden keamanan informasi.

15.2.2 Kejadian *(event)* keamanan informasi harus dilaporkan secepat mungkin sesuai mekanisme yang berlaku.

15.2.3 Karyawan dan pekerja kontrak yang menggunakan sistem dan layanan informasi harus mencatat dan melaporkan setiap kelemahan keamanan informasi yang diamati atau dicurigai dalam suatu sistem atau layanan.

15.2.4 Peristiwa keamanan informasi harus dinilai dan harus diputuskan apakah akan diklasifikasikan sebagai insiden keamanan informasi.

15.2.5 Insiden keamanan informasi harus ditanggapi sesuai dengan prosedur yang terdokumentasi.

15.2.6 Pengetahuan yang diperoleh dari proses analisa dan penyelesaian masalah insiden keamanan informasi harus digunakan untuk mengurangi kemungkinan atau dampak dari insiden di masa depan.

15.2.7 Telkom University harus menentukan dan menerapkan mekanisme untuk melakukan identifikasi, pengumpulan, akuisisi dan pelestarian informasi, yang dapat berfungsi sebagai bukti.

15.3 Dokumen Terkait

- Manajemen Insiden dan Permintaan

16. Pengendalian Aspek Keamanan Informasi dalam Pengelolaan Kesinambungan Bisnis

16.1 Tujuan

16.1.1 Kesinambungan keamanan informasi harus tertanam dalam BCMS *(Business Continuity Management Systems)* pada perusahaan.

16.1.2 Untuk memastikan ketersediaan terhadap perangkat pengolahan informasi.

16.2 Penerapan

16.2.1 Universitas harus menetapkan persyaratan untuk keamanan informasi dan kesinambungan terhadap pengelolaan keamanan informasi dalam situasi yang merugikan, misalnya selama krisis atau bencana.

16.2.2 Universitas harus menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol untuk memastikan tingkatan yang diperlukan oleh kesinambungan terhadap keamanan informasi selama situasi yang merugikan.

16.2.3 Universitas harus memverifikasi pelaksanaan dan menetapkan pengendalian terhadap kesinambungan keamanan informasi secara berkala untuk memastikan bahwa proses tersebut valid dan efektif dalam situasi yang merugikan.

16.2.4 Fasilitas pengolahan informasi harus diimplementasikan dengan redundansi yang cukup untuk memenuhi persyaratan ketersediaan.

16.3 Dokumen Terkait

- *Integrated Management System Plan* (IMS *Plan*)
- Laporan uji *coba backup* dan *restore*

17.Kepatuhan

17.1 Tujuan

17.1.1 Untuk menghindari pelanggaran terhadap kewajiban hukum, undang-undang, peraturan atau kontrak yang terkait dengan keamanan informasi dan persyaratan keamanan.

17.1.2 Untuk memastikan bahwa keamanan informasi diimplementasikan dan dijalankan sesuai dengan peraturan perusahaan.

17.2 Penerapan

17.2.1 Seluruh undang-undang, peraturan, persyaratan kontrak dan pendekatan legislatif yang terkait serta pendekatan universitas untuk memenuhi persyaratan tersebut harus secara eksplisit diidentifikasi, didokumentasikan dan selalu *up-to-date* untuk setiap sistem informasi dan perusahaan.

17.2.2 Peraturan harus diterapkan untuk memastikan kepatuhan dengan persyaratan legislatif, peraturan dan kontrak yang terkait dengan hak kekayaan intelektual dan penggunaan kepemilikan produk perangkat lunak.

17.2.3 Rekaman harus dilindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah dan rilis yang tidak sah, sesuai dengan legislasi, peraturan, persyaratan kontrak dan bisnis.

17.2.4 Perlindungan terhadap privasi dan informasi pribadi harus sesuai dengan undang-undang dan peraturan yang berlaku.

17.2.5 Pengendalian terhadap kriptografi harus digunakan sesuai dengan semua perjanjian, undang-undang dan peraturan yang berlaku.

17.2.6 Pendekatan universitas dalam mengelola keamanan informasi serta pelaksanaannya (misalnya sasaran pengendalian, kebijakan, proses dan prosedur untuk keamanan informasi) harus dikaji secara independen pada interval yang direncanakan atau ketika terjadi perubahan yang signifikan.

17.2.7 Manajer harus secara teratur meninjau kepatuhan terhadap proses pengolahan informasi dan prosedur dalam area tanggung jawab mereka, sesuai dengan kebijakan keamanan, standar dan persyaratan keamanan yang berlaku pada perusahaan.

17.2.8 Sistem informasi harus dikaji secara berkala untuk kepatuhan terhadap kebijakan dan standar keamanan informasi yang berlaku pada perusahaan.

17.3 Dokumen Terkait

- Daftar Peraturan perundang-undangan yang terkait keamanan informasi
- Laporan peninjauan kepatuhan terhadap keamanan informasi

18. *Clear Desk Clear Screen*

18.1 Tujuan

18.1.1 Melindungi informasi dan sistem informasi dari kesalahan penggunaan atau penyebaran secara tidak berwenang pada perangkat kerja

18.1.2 Memandu tata cara pengamanan informasi dan sistem informasi di Telkom University terutama di area kerja

18.1.3 Mencegah dan mengendalikan risiko yang timbul karena kesalahan pegawai dalam menggunakan perangkat pengolahan informasi.

18.2 Penerapan

18.2.1 Semua perangkat komputasi maupun pengolahan data harus dalam keadaan *log off* atau dilindungi dengan *screensaver* yang aktif pada batas waktu tertentu (contohnya 5 menit) atau mekanisme penguncian akses jika tidak sedang digunakan. Pengamanan perangkat dapat menggunakan salah satu atau lebih mekanisme yaitu menggunakan password, PIN, *fingerprint*, *pattern* atau *face lock*. Hal ini termasuk pada perangkat komputer, laptop, tablet dan *smartphone* yang digunakan untuk menunjang pekerjaan

18.2.2 Saat menampilkan informasi rahasia pada layar, pegawai harus memperhatikan keadaan sekitar dan memastikan tidak ada pihak yang tidak berkepentingan yang dapat melihat informasi yang ditampilkan

18.2.3 Setiap informasi rahasia atau kritikal yang menyangkut keberlangsungan bisnis, contohnya yang terdapat di kertas maupun perangkat penyimpanan harus diamankan, terutama saat staf tidak berada di tempat kerja

18.2.4 Kertas yang menyantumkan informasi rahasia atau kritikal harus segera diambil dari perangkat cetak

18.2.5 Setiap informasi rahasia maupun kritikal yang terdapat di media kertas maupun media penyimpanan elektronik harus segera dihancurkan jika sudah tidak terpakai, atau disimpan di tempat yang aman sampai dengan informasi tersebut bisa dihancurkan ata dihapus

18.3 Dokumen Terkait

18.3.1 -