PEDOMAN
PENGELOLAAN KEAMANAN INFORMASI

INSTITUT TEKNOLOGI TELKOM PURWOKERTO

No. : ITTel3603/IS-000/REK-00/VI/2022 Rev. : 01 Tgl Efektif : 01 Juni 2022	DISUSUN OLEH: Yudha Saintika, MTI **Bagian IT Support**	DIAJUKAN OLEH: Tata Sambada, MBA **Management Representative**	DISETUJUI OLEH: Arfianto Fahmi, ST., MT., IPM **Rektor**

BAB 1 PENDAHULUAN

1.1 Daftar Isi

NO. COPY	JABATAN	NAMA	DOC. TYPE

1	*KABAG IT SUPPOT*	Yudha Saintika	*Softfile*
2			

1.2 Status Revisi dan Riwayat Perubahan

REVISI	NO BAB	DETIL PERUBAHAN	TANGGAL EFEKTIF
00	1 sd 3	Inisiasi Dokumen	15 Oktober 2021
	4 sd 7	Penambahan kebijakan	10 November 2021
	7	Penambahan kebijakan	7 Desember 2021
	1-7	Merapikan sistematika	1 Juni 2022

1.3 Pendahuluan

Pengelolaan Mutu dalam suatu aktifitas bisnis Institusi merupakan suatu hal yang sudah umum dan wajib diterapkan dalam suatu Institusi atau organisasi untuk mencapai unjuk kerja yang memuaskan semua *stakeholder* yang terkait dengan Institusi atau organisasi. Pengelolaan mutu jika dibarengi dengan pengelolaan informasi yang baik akan lebih meningkatkan nilai dari suatu Institusi/organisasi.

Selain aspek Mutu, Informasi merupakan aset yang sangat penting bagi organisasi, dimana dalam operasionalnya, pertukaran informasi adalah hal yang sangat dibutuhkan bagi kelangsungan bisnis organisasi. Bentuk dari informasi tersebut dapat berupa informasi tertulis pada kertas, tertulis dan tersimpan secara elektronik, ditransmisikan secara manual dan elektronik, suara, video, dan lainnya.

Sebagai salah satu alat penunjang proses bisnis organisasi, sistem pengolah informasi (sistem komputer – termasuk didalamnya adalah *hardware, software*, dan jaringan) harus dipastikan penggunaannya secara efektif dan produktif karena tidak seluruh informasi dapat dikonsumsi oleh seluruh pengguna. Jika tidak digunakan sebagaimana mestinya, maka penggunaan sistem komputer dapat memberikan dampak yang sangat buruk bagi organisasi (misalnya penurunan citra organisasi).

Untuk memastikan sistem komputer digunakan sebagaimana mestinya, adalah hal yang penting bahwa pemilik, operator, dan pengguna dari sistem yang dimaksud memiliki standar panduan penggunaan sistem beserta pengetahuan atas pentingnya menjaga data/informasi yang diolah maupun dihasilkan oleh sistem tersebut. Hal-hal tersebut tertuang dalam dokumen Pedoman Keamanan Informasi.

1.4 Tujuan

Pengelolaan Mutu bertujuan untuk menjamin semua proses bisnis dalam suatu Institusi agar sesuai dengan standar manajemen yang sudah diakui sehingga diharapkan agar bisa mencapai kepuasan pelangan dan harapan semua stakeholder terkait, sedangkan Keamanan informasi bertujuan untuk melindungi informasi terhadap berbagai macam ancaman (fisik maupun teknologi, seperti penipuan menggunakan komputer, spionase, sabotase, perusakan, kebakaran, banjir, virus, *hacker*, *denial of service*, dan lain-lain) guna menjaga kelangsungan bisnis, meminimalisasi risiko bisnis, dan memaksimalkan keuntungan dan kesempatan bisnis.

Dengan memiliki dokumen yang mengatur mengenai tata kelola mutu dan keamanan informasi berarti penanganan mutu dan informasi sudah sesuai dengan standar baku dan ekspektasi dari pelanggan, juga informasi di organisasi akan terjaga kerahasiaannya (*confidentiality*), integritasnya (*integrity*), dan keberadaannya (*availability*) sehingga informasi tidak ter-ekspose dan tidak termodifikasi oleh orang yang tidak berkepentingan, dan selalu tersedia bila dibutuhkan.

Dan seperti yang telah diuraikan pada butir sebelumnya, informasi memiliki berbagai bentuk dan setiap bentuk informasi harus diberikan pengendalian (kontrol) sesuai tingkatannya guna memenuhi tujuan dari keamanan informasi tersebut.

BAB 2 – MATRIKS ISO 9001:2015 & ISO 27001:2013

2.1 Matriks Sistem Manajemen Mutu ISO 9001:2015

Persyaratan ISO 9001:2015		Bagian Manual Mutu
4	*Sistem Manajemen Mutu*	*Umum*
4.1	Persyaratan Umum	4.1, 4.2, 4.3
4.2	Persyaratan Dokumentasi	4.1
4.2.1	Umum	Umum
4.2.2	Manual Mutu	Umum
4.2.3	Pengendalian Dokumen	9.2, 10.2, 11.2, 12.2, 13.2, 14.2, 15.2, 16.2, 17.2, 18.2, 19.2, 20.2, 21.2
4.2.4	Pengendalian Catatan Mutu	8.2, 9.2, 10.2, 11.2, 12.2, 13.2, 14.2, 15.2, 16.2, 17.2, 18.2, 19.2, 20.2, 21.2
5	*Tanggung Jawab Manajemen*	*Umum*
5.1	Komitmen Manajemen	Umum
5.2	Fokus Kepada Pelanggan	4.4, 8.2, 9.2, 11.2, 12.2
5.3	Kebijakan Mutu	5.1
5.4	Perencanaan	Umum
5.4.1	Sasaran Mutu	5.2
5.4.2	Perencanaan Sistem Manajemen Mutu	5.3
5.5	Tanggung Jawab, Wewenang dan Komunikasi	Umum
5.5.1	Tanggung Jawab dan Wewenang	6.1, 6.2
5.5.2	Wakil Manajemen	6.3
5.5.3	Komunikasi Internal	4.5
5.6	Tinjauan Manajemen	21.2
5.6.1	Umum	Umum
5.6.2	Masukan Tinjauan Manajemen	21.2
5.6.3	Hasil Tinjauan Manajemen	21.2
6	*Manajemen Sumber Daya*	*Umum*
6.1	Penyediaan Sumber Daya	11.2, 13.2, 14.2, 15.2, 16.2, 17.2, 18.2, 19.2, 20.2
6.2	Sumber Daya Manusia	19.2
6.2.1	Umum	Umum
6.2.2	Kompetensi, Kepedulian dan Pelatihan	19.2
6.3	Infrastruktur	12.2, 17.2, 19.2, 20.2
6.4	Lingkungan Kerja	17.2, 18.2, 20.2
7	*Realisasi Produk*	*Umum*
7.1	Perencanaan dan Merealisasikan Produk	11.2
7.2	Proses Yang Berhubungan dengan Pelanggan	8.2, 9.2, 11.2, 12.2, 13.2, 14.2
7.2.1	Penentuan Syarat yang Berhubungan dengan Produk	9.2, 11.2, 12.2, 13.2, 14.2
7.2.2	Tinjauan Terhadap Syarat Yang Berhubungan dengan Produk	9.2, 11.2, 12.2, 13.2, 14.2
7.2.3	Komunikasi dengan Pelanggan	8.2, 11.2, 12.2, 14.2,
7.3	Disain dan Pengembangan	Umum
7.3.1	Perencanaan Disain dan Pengembangan	11.2, 12.2
7.3.2	Masukan Disain dan Pengembangan	11.2, 12.2
7.3.3	Hasil Disain dan Pengembangan	11.2, 12.2
7.3.4	Tinjauan Disain dan Pengembangan	11.2, 12.2
7.3.5	Verifikasi Disain dan Pengembangan	11.2, 12.2
7.3.6	Validasi Disain dan Pengembangan	11.2, 12.2
7.3.7	Pengendalian Perubahan Disain dan Pengembangan	11.2, 12.2
7.4	Pembelian	Umum
7.4.1	Proses Pembelian	8.2, 17.2

7.4.2	Informasi Pembelian	10.2,.12.2, 14.2, 17.2, 20.2
7.4.3	Verifikasi Produk yang Dibeli	10.2, 11.2, 12.2
7.5	Produksi dan Penyediaan Jasa	Umum
7.5.1	Pengendalian Produksi dan Penyediaan Jasa	10.2, 11.2, 12.2, 18.2
7.5.2	Validasi Proses-proses Produksi dan Penyediaan Jasa	11.2, 12.2
7.5.3	Identifikasi dan Kemampuuan Telusur	10.2, 11.2, 12.2, 17.2
7.5.4	Hak Milik Pelanggan	11.2, 12.2
7.5.5	Pengawetan/pemeliharaan Produk	10.2, 11.2, 12.2,17.2
7.6	Pengendalian Alat Ukur dan Alat Monitor	12.2
8	*Pengukuran, Analisa dan Penyempurnaan*	*Umum*
8.1	Umum	Umum
8.2	Pemantauan dan Pengukuran	Umum
8.2.1	Kepuasan Pelanggan	8.2, 12.2
8.2.2	Internal Audit	21.2
8.2.3	Pemantauan dan Pengukuran Proses	11.2, 12.2, 21.2
8.2.4	Pemantauan dan Pengukuran Produk	10.2, 11.2, 12.2, 21.2
8.3	Pengendalian Ketidaksesuaian Produk	10.2, 11.2, 12.2, 21.2
8.4	Analisa Data	8.2, 11.2, 12.2, 14.2, 15.2
8.5	Penyempurnaan/peningkatan	Umum
8.5.1	Perbaikan Berkesinambungan	11.2, 12.2, 21.2
8.5.2	Tindakan Perbaikan	11.2, 12.2, 17.2, 21.2
8.5.3	Tindakan Pencegahan	11.2, 12.2, 17.2, 21.2

BAB 3 - PROFIL INSTITUSI

3.1 *Vision*/Visi

Menjadi perguruan tinggi yang unggul di tingkat internasional dalam pengembangan ilmu pengetahuan berbasis teknologi informasi dengan keunggulan pada bidang Healthcare, Agro-industry, Tourism, dan Small-Medium Enterprise.

3.2 *Mission*/Misi

Menyelenggarakan dan mengembangkan pendidikan berstandar internasional berbasis teknologi informasi yang fokus pada bidang Healthcare, Agro-Industry, Tourism, dan Small-Medium Enterprise.

1. Menyelenggarakan dan mengembangkan pendidikan berstandar internasional berbasis teknologi informasi yang fokus pada bidang Healthcare, Agro-Industry, Tourism, dan Small-Medium Enterprise.
2. Menyelenggarakan penelitian dan menyebarluaskan hasilnya untuk pengembangan ilmu pengetahuan dan teknologi.
3. Menerapkan dan memanfaatkan ilmu pengetahuan dan teknologi bagi kemaslahatan masyarakat.
4. Menerapkan Good University Governance dan menjalin kerjasama nasional maupun internasional.

3.3 *Scope of Works*

Aplikasi registrasi mata kuliah (KRS) iGracias.

3.4 *Offering*

Efisien, kualitas tinggi dan desain sistem TI yang tepat, penyebaran/pengembangan, Operasi dan Pemeliharaan.

Note: Profil institusi juga bisa dilihat di website: http://www.ittelkom-pwt.ac.id

BAB 4 - SISTEM MANAJEMEN MUTU & KEAMANAN INFORMASI

4.1 Struktur Dokumentasi

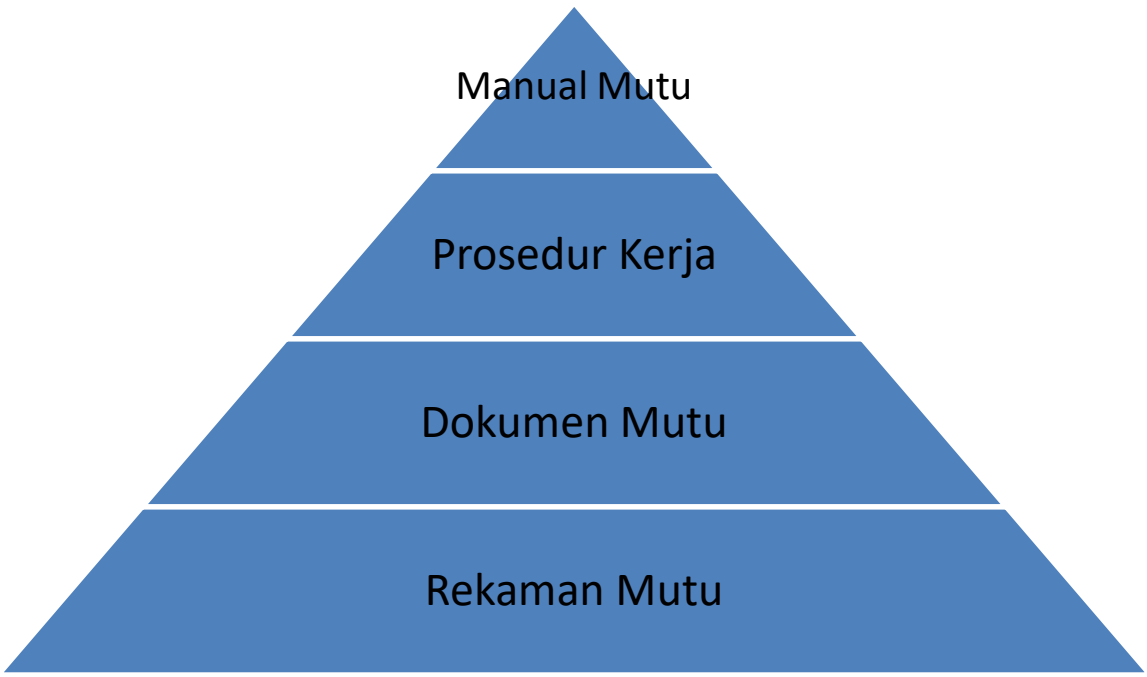
Secara umum struktur dokumentasi sistem manajemen mutu dan keamanan informasi adalah:

- Manual Mutu dan Pedoman Sistem Keamanan Informasi:
  Suatu dokumen level pertama yang berisi pernyataan-pernyataan kebijakan Institusi dalam rangka memenuhi persyaratan ISO 9001: 2015 dan ISO 27001:2013, termasuk didalamnya adalah cakupan dari sistem manajemen mutu dan sistem manajemen informasi, prosedur-prosedur terdokumentasi dan interaksi antar proses dalam sistem manajemen mutu.

- Prosedur Kerja/Standar Operasional Prosedur (SOP):
  Suatu dokumen level kedua yang berisi langkah-langkah yang telah ditetapkan untuk melakukan suatu aktifitas. Di dalam setiap prosedur kerja terdapat referensi terhadap syarat-syarat ISO 9001:2015 dan ISO 27001:2013.

- Dokumen Pendukung:
  Suatu dokumen level ketiga yang berisi langkah-langkah lebih detil bagaimana menjalankan satu tugas. Dokumen pendukung ini terdiri dari instruksi kerja, formulir, spesifikasi dan lain-lain.

- Rekaman Mutu:
  Suatu dokumen level keempat yang menyatakan bukti dari pelaksanaan suatu aktifitas yang telah dijalankan.



Metode pengendalian dokumen:

Untuk dokumen yang berupa *hardcopy* akan dilakukan pengendalian sebagai berikut :

a. *Master* dokumen akan disimpan di lokasi/lemari milik Satuan Penjaminan Mutu Institusi.
b. Dokumen terkendali diberi stempel '*Controlled Document'.*
c. Dokumen tidak terkendali diberi stempel *'Uncontrolled Document'.*
d. Dokumen *Master* yang tidak berlaku diberi stempel *'Obsolete'.*

Untuk dokumen yang berupa *soft copy* khusus untuk dokumen level 2 prosedur kerja dan Level 3 (Instruksi Kerja dan Standar) akan dilakukan pengendalian sebagai berikut :

a. Dokumen akan diletakkan pada komputer *server*/*Public Folder* sebagai *'Controlled Document'* sedangkan Master dokumennya berupa *hardcopy.*
b. Persetujuan dari dokumen yang terdapat dalam *server*/*Public Folder* ini dilakukan dari masing-masing pemilik proses yang dilampirkan dalam tiap dokumen.
c. Dokumen ini akan didistribusikan melalui web/intranet dan pengumuman/pemberitahuannya kepada seluruh karyawan/pihak terkait dilakukan melalui media e-mail dan/atau intranet. Dokumen dalam *server* ini tidak dapat diedit oleh pemilik proses maupun karyawan lainnya dan jika dokumen di-*print out* dianggap sebagai dokumen yang tidak sah, kecuali diberi stempel *'Controlled Document'* oleh *Document Controller (*Satuan Penjaminan Mutu Institusi.*)* .
d. Jika terjadi perubahan terhadap dokumen maka dokumen yang tidak berlaku yang terdapat di server/*Public Folder* akan dihapus dan digantikan dengan dokumen versi yang terbaru oleh *Document Controller* (Satuan Penjaminan Mutu Institusi).
   Detil tata cara Pengendalian Dokumen dan Pengendalian Catatan masing-masing dijelaskan secara lengkap didalam SOP-xxx Pengendalian Dokumen dan SOP-xxx Pengendalian Catatan.
   (Elemen ISO 9001:2015, Klausul: 4.1, 4.2 dan Elemen ISO 27001:2013 Klausul: 4.3.2)

4.2 Aliran Bisnis Proses Institusi

Aliran *Business Process* Institusi terdapat pada Lampiran A-1**.**
(Elemen ISO 9001:2015, Klausul: 4.1)

4.3 Cakupan Sistem Manajemen Mutu dan Keamanan Informasi

Cakupan sistem manajemen dan manajemen keamanan informasi adalah hanya meliputi operasional dan pelayanan Aplikasi Registrasi Mata Kuliah pada aplikasi iGracias IT Telkom Purwokerto, Jalan DI Panjaitan 128, Purwokerto Selatan 53147.
(Elemen ISO 9001:2015, Klausul: 4.1 dan Elemen ISO 27001:2013 Klausul 4.1).

4.4 Fokus Kepada Pelanggan

Fokus kepada pelanggan dilakukan oleh IT Telkom Purwokerto dengan cara memahami dan menentukan keinginan, persyaratan pelanggan dan memberikan solusi, layanan dan produk yang berkualitas tinggi guna meningkatkan kepuasan pelanggan. IT Telkom Purwokerto melakukan survei pengukuran kepuasan pelanggan yang dilakukan secara periodik setahun sekali dan melakukan pelayanan penanganan keluhan pelanggan. ***(Elemen ISO 9001:2015, Klausul: 5.2, 8.2.1)***

4.5 Komunikasi Internal

Untuk memastikan terjalinnya komunikasi internal yang efektif antar jenjang dan fungsi di IT Telkom Purwokerto, maka "*Intranet*" dipakai sebagai salah satu sarana untuk berkomunikasi

dalam mewujudkan keberhasilan Sistem Manajemen Mutu. Bentuk komunikasi yang lain adalah dalam bentuk tulisan dengan menggunakan memo internal, e-mail maupun verbal dalam pertemuan internal. ***(Elemen ISO 9001:2015, Klausul: 5.5.3 dan Elemen ISO 27001:2013 Klausul 5.1).***

4.6 Analisa Data

Untuk memastikan data hasil implementasi dapat dipergunakan untuk efektifitas pelaksanaan tindakan perbaikan, tindakan pencegahan dan perbaikan berkesinambungan, maka dilakukan analisa data oleh pemilik proses yang dilaporkan kepada manajemen secara berkala.

BAB 5 - KEBIJAKAN MUTU, LAYANAN TEKNOLOGI INFORMASI DAN KEAMANAN INFORMASI

5.1 Kebijakan Mutu, Layanan Teknologi Informasi dan Keamanan Informasi

Institut Teknologi Telkom Purwokerto secara konsisten bertekad untuk mengelola setiap aktivitas dengan selalu memperhatikan mutu, perlindungan lingkungan hidup, mengutamakan keselamatan & kesehatan kerja, prinsip-prinsip layanan teknologi informasi dan keamanan informasi serta melaksanakan setiap peraturan dan perundang-undangan yang relevan sebagaimana mestinya.

Untuk implementasi tersebut, IT Telkom Purwokerto akan**:**

1. Mengatur aktifitas yang dilakukan secara efisien dan dengan produktifitas yang tinggi untuk menjamin bahwa keinginan *customer* dapat dipenuhi.
2. Meminimalkan risiko terkait keselamatan dan kesehatan kerja, keamanan informasi, layanan teknologi informasi, lingkungan hidup, karyawan dan pihak-pihak lain yang mungkin terkena risiko terkait dengan kegiatan usaha Institusi, sesuai dengan kriteria penerimaan dan manajemen risiko Institusi.
3. Mencegah terjadinya penyakit dan kecelakaan akibat kerja, insiden teknologi informasi & keamanan informasi serta pencemaran lingkungan.
4. Memastikan bahwa karyawan IT Telkom Purwokerto mempunyai kompetensi yang dibutuhkan serta terus menerus mengembangkan kompetensi yang ada di setiap level guna mendukung semua solusi yang ditawarkan.
5. Meningkatkan terus menerus sistem manajemen mutu, keselamatan & kesehatan kerja, lingkungan hidup, keamanan informasi dan layanan teknologi informasi yang dijalankan dengan menerapkan dan mempertahankan ISO 9001, SMK3, ISO 27001 dan ISO 20000.

Kebijakan Mutu dan Keamanan Informasi IT Telkom Purwokerto ini akan menjadi kerangka kerja di dalam penyusunan dan peninjauan Sasaran Mutu, Layanan TI dan Keamanan Informasi.

Untuk menjamin Kebijakan Mutu, Layanan TI dan Keamanan Informasi tersebut diimplementasikan, semua karyawan dilibatkan dan melakukan kerja sesuai dengan dokumen sistem manajemen mutu dan keamanan informasi IT Telkom Purwokerto yang sesuai dengan persyaratan Standar Internasional ISO 9001 : 2015 dan ISO 27001:2013
(Elemen ISO 9001:2015, Klausul: 5.3 dan Elemen ISO 27001:2013 Klausul 5.1 & Annex A.5).

5.2 Sasaran Mutu, Layanan Teknologi Informasi & Keamanan Informasi

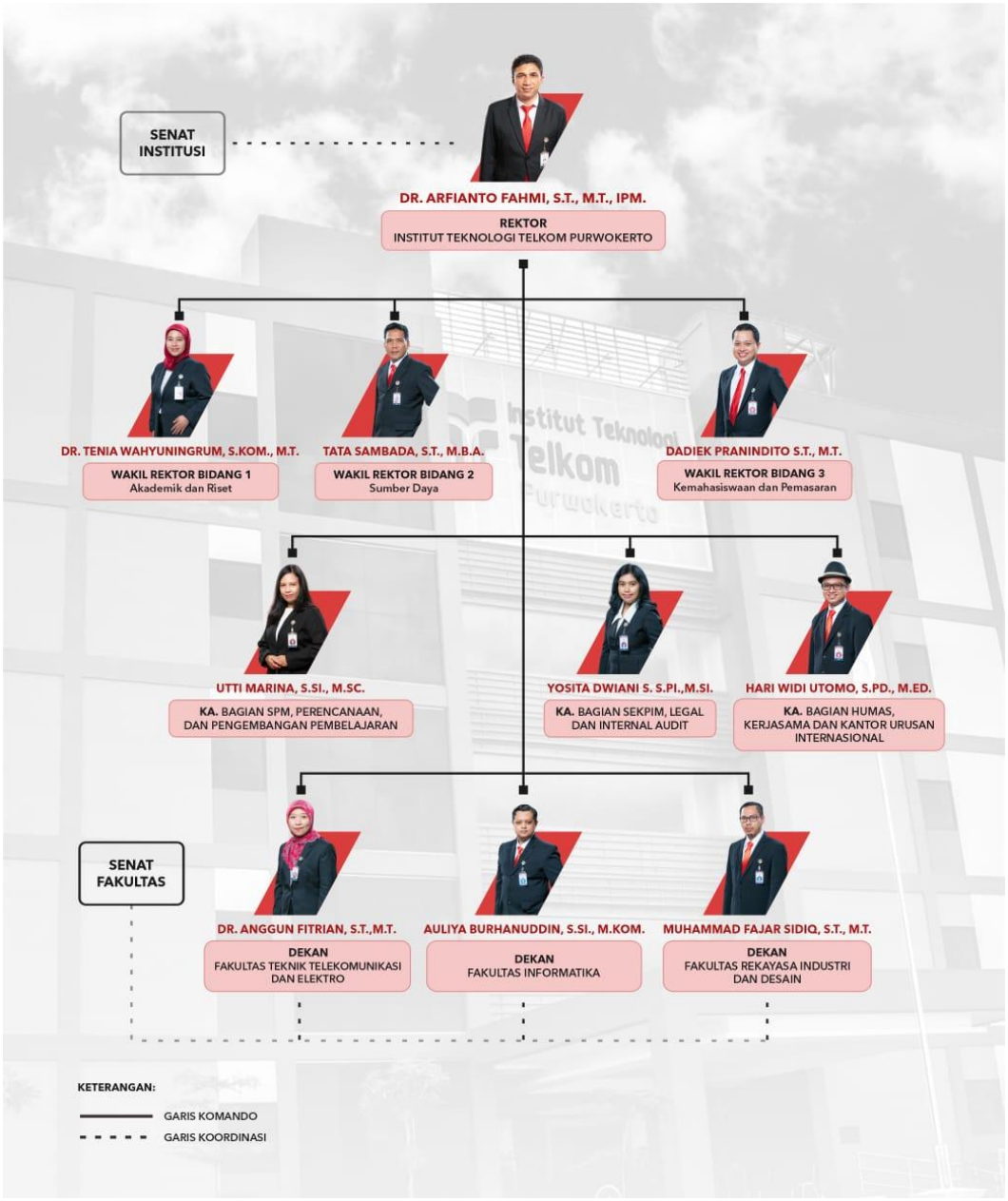
Manajemen IT Telkom Purwokerto menentukan Sasaran berdasarkan target Institusi yang ditentukan dalam Perencanaan Strategis yang disetujui oleh Rektor dan kebijakan Institusi. Untuk tercapainya sasaran mutu, layanan TI dan keamanan informasi Institusi, masing-masing pemilik proses wajib menentukan sasaran mutu dan keamanan informasi proses bisnisnya. Pemenuhan Sasaran Mutu dan Keamanan Informasi ini direview secara berkala terhadap pencapaiannya.

(Elemen ISO 9001:2015, Klausul: 5.4.1 dan Elemen ISO 27001:2013 Klausul 5.1).

BAB 6 - ORGANISASI INSTITUSI

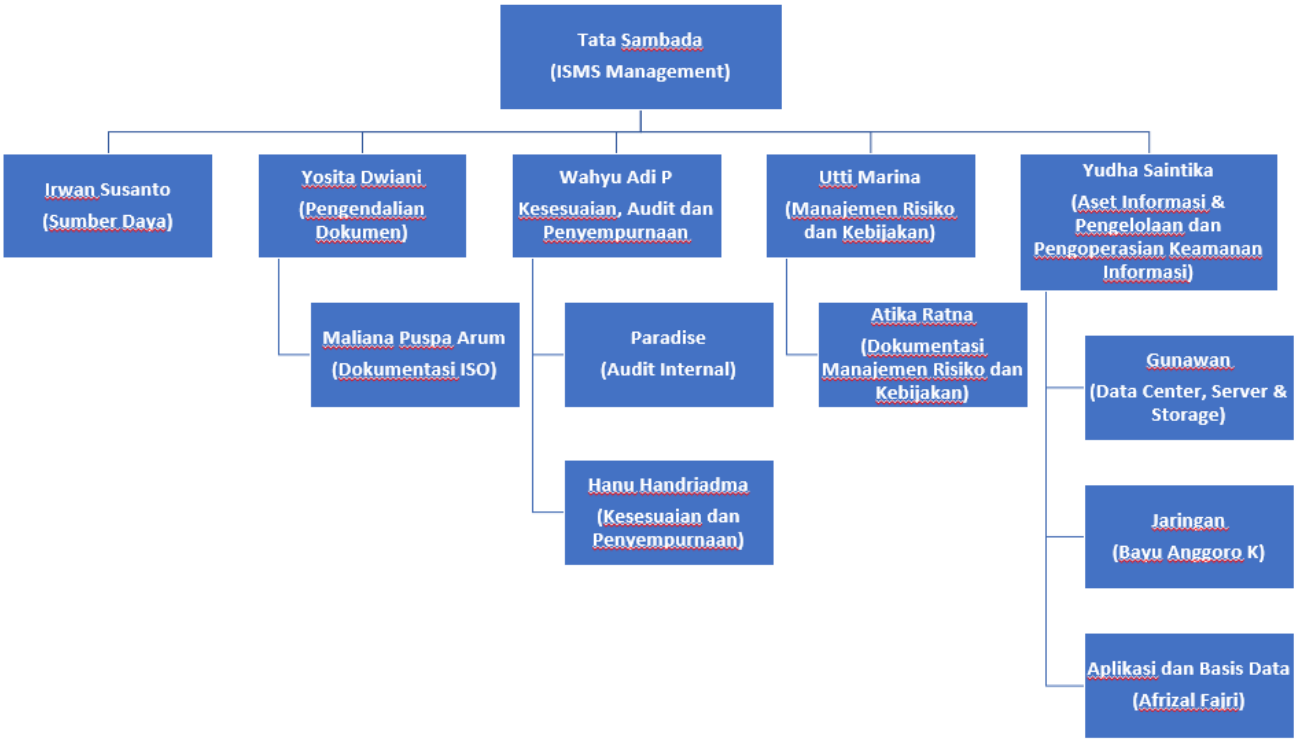
6.1 Organisasi Institut Teknologi Telkom Purwokerto

Sesuai dengan Struktur Organisasi Tata Kelola terbaru untuk période 2021-2025, Institut Teknologi Telkom Purwokerto memiliki struktur berikut ini :



Institut Teknologi Telkom Purwokerto memiliki 3 Bidang Utama yaitu Bidang I Akademik dan Riset yang di bawahnya meliputi Lembaga Penelitian dan Pengabdian Masyarakat (LPPM), Perpustakaan, Fakultas dan Layanan Akademik, Bidang II Sumber Daya yang meliputi logistik dan asset, IT Support, Keuangan, dan Sumber Daya Manusia (SDM), serta Bidang III Kemahasiswaan dan Pemasaran yang meliputi penerimaan mahasiswa baru dan pemasaran. Sedangkan unit di bawah rektorat terdapat Satuan Penjaminan Mutu, Satuan Audit Internal, Sekretaris Pimpinan, Legal, serta Bagian Hubungan masyarakat dan Kantor Urusan Internasional.

6.2 Organisasi Pengelolaan Ruang Lingkup ISO 27001



6.3 Tanggung Jawab dan Wewenang *Management Reperesentatives*

Wakil manajemen yang dalam Institusi ini disebut *Management Representatives* (MR) langsung melaporkan ke Rektor. Adapun tugas dan tanggung jawab MR sebagai berikut:

1. Mengkoordinir dan mengelola Sistem Manajemen Mutu & Keamanan Informasi yang efektif sesuai arahan Manajemen Puncak dan sesuai dengan Kebijakan Mutu & Keamanan Informasi dan Sasaran Mutu & Keamanan Informasi.

2. Memastikan proses–proses dan dokumentasi yang diperlukan dalam Sistem Manajemen Mutu dan Keamanan Informasi telah ditetapkan, dilaksanakan dan dipelihara dalam Institusi.

3. Melaporkan kepada Manajemen Puncak tentang Kinerja Sistem Manajemen Mutu & Keamanan Informasi dan kebutuhan–kebutuhan untuk melakukan penyempurnaan.

4. Meningkatkan kepedulian dan kesadaran karyawan tentang pentingnya memenuhi persyaratan pelanggan dan peraturan yang berlaku.

Membina hubungan dengan pihak pihak luar dalam kaitannya dengan Sistem Manajemen Mutu dan Keamanan Informasi. ***(Elemen ISO 9001:2015, Klausul: 5.5.2)***

6.4 Tanggung Jawab Keamanan Informasi

Seluruh personel yang mengakses dan memroses informasi memiliki kewajiban untuk menjaga keamanan informasi. Hal ini termasuk seluruh staf yang berada di Institut Teknologi Telkom Purwokerto, termasuk staf tidak tetap, staf kerja paruh waktu, rekanan, calon rekanan, dan pihak eksternal lainnya yang mengakses sistem informasi Institut Teknologi Telkom Purwokerto. Jika terjadi penyalahgunaan informasi, maka seluruh pihak berkewajiban untuk memberitahukan kepada manajemen organisasi.

BAB 7 – KEBIJAKAN KEAMANAN INFORMASI

7.1. Organisasi Keamanan Informasi

7.1.1. Persyaratan Keamanan Informasi di dalam Organisasi

Tujuan
Untuk mengatur keamanan informasi dan memastikan bahwa kebijakan yang berlaku telah diterapkan.

Risiko
Keamanan informasi yang tidak diatur secara efektif akan mengakibatkan kebutuhan dan tujuan bisnis tidak tercapai dan adanya risiko kebocoran informasi yang tinggi atau kegagalan fasilitas untuk memroses informasi.

7.1.1.1. KOMITMEN MANAJEMEN TERHADAP KEAMANAN INFORMASI

- Institut Teknologi Telkom Purwokerto menetapkan komitmen terhadap Sistem Manajemen Keamanan Informasi melalui "PERNYATAAN MANUAL MUTU DAN PEDOMAN PENGELOLAAN KEAMANAN INFORMASI" sebagai berikut:
  1. Bagian Sistem Penjaminan Mutu dan IT Support bertanggung jawab untuk menyusun kebijakan keamanan informasi.
  2. Kepala Unit Operasional bertanggung jawab untuk meninjau kebijakan keamanan informasi minimal sekali dalam waktu tiga tahun atau jika terjadi perubahan dalam organisasi Institut Teknologi Telkom Purwokerto yang berdampak pada implementasi Manajemen Keamanan Informasi serta memenuhi sasaran keamanan informasi yang merupakan indikator kinerja Sistem Manajemen Keamanan Informasi.
  3. Rektor bertanggung jawab untuk menyetujui kebijakan keamanan informasi.
  4. *Management Representatives* bertanggung jawab untuk meninjau efektivitas implementasi kebijakan keamanan informasi dan memastikan implementasi kontrol keamanan informasi telah dikoordinasikan ke seluruh bidang yang ada di Institut Teknologi Telkom Purwokerto.
  5. *Manajemen* Institut Teknologi Telkom Purwokerto bertanggung jawab untuk menyediakan sumber daya yang dibutuhkan untuk keamanan informasi dan menyetujui peran dan tanggung jawab keamanan informasi di Institut Teknologi Telkom Purwokerto.
  6. *Management Representatives* bertanggung jawab untuk melaksanakan asesmen risiko keamanan informasi serta mengevaluasinya secara rutin.
  7. *Management Representatives* bertanggung jawab untuk menyusun rencana dan program untuk memelihara kesadaran (*awareness*) terhadap keamanan informasi.
  8. *Management Representatives* bertanggung jawab untuk melaksanakan perbaikan yang berkesinambungan terhadap kinerja Sistem Manajemen Keamanan Informasi.
- Institut Teknologi Telkom Purwokerto, menerapkan Sistem Manajemen Keamanan Informasi (SMKI) yang mengacu kepada Standar Internasional ISO/IEC 270001:2013 berbasis *Plan-Do-Check-Action* (siklus PDCA), dengan kerangka kerja sebagai berikut:

1. Tahapan "*Plan*" dilakukan hal-hal berikut:
    a. Rektor Institut Teknologi Telkom Purwokerto menetapkan cakupan implementasi SMKI.
    b. Rektor Institut Teknologi Telkom Purwokerto menunjuk Wakil Manajemen SMKI yang bertugas memimpin pembangunan dan implementasi SMKI di Institut Teknologi Telkom Purwokerto.
    c. Rektor Institut Teknologi Telkom Purwokerto memastikan dilakukannya asesmen risiko keamanan informasi dalam rangka pelaksanaan pengamanan dan perlindungan aset informasi.
    d. Rektor Institut Teknologi Telkom Purwokerto menyetujui diimplementasikannya Rencana Mitigasi Risiko Keamanan Informasi (*Risk Treatment Plan)* yang disusun berdasarkan hasil asesmen risiko keamanan informasi.
    e. Rektor Institut Teknologi Telkom Purwokerto menyetujui Pernyataan Pemberlakuan SMKI (*Statement of Applicability)* terhadap elemen-elemen pengendalian yang ada pada Annex A Standar ISO/IEC 27001:2013.
    f. Rektor Institut Teknologi Telkom Purwokerto menetapkan sasaran dan Target SMKI yang merupakan indikator kinerja SMKI di Institut Teknologi Telkom Purwokerto.

2. Tahapan "*Do*" dilakukan hal-hal berikut:
    a. *Management Representatives* mengorganisasikan implementasi *Risk Treatment Plan* yang dapat berupa:
        - Melakukan penyadaran *awareness* dan pelatihan SMKI;
        - Penyusunan dan implementasi Prosedur dan Instruksi Kerja;
        - Pengadaan dan pengelolaan Sumber Daya, baik SDM maupun sumber daya teknis; dan
    b. *Management Representatives* menetapkan kriteria keefektifan implementasi pengendalian keamanan informasi.
3. Tahapan "*Check*" dilakukan hal-hal berikut:
    a. *Management Representatives* menilai keefektifan implementasi pengendalian keamanan informasi berdasarkan kriteria yang telah ditetapkan pada tahapan "*Do*," dilakukan setidaknya tiga kali dalam satu tahun.
    b. *Management Representatives* memantau pencapaian sasaran dan target SMKI dan melaporkannya kepada Rektor Institut Teknologi Telkom Purwokerto, dilakukan setidaknya tiga kali dalam satu tahun.
    c. Kepala Bagian Satuan penjaminan Mutu meninjau hasil asesmen risiko, paling sedikit satu kali dalam satu tahun.
    d. *Management Representatives* mengkoordinasikan dilakukannya audit internal SMKI, dilakukan setidaknya satu kali dalam satu tahun.

e. Rektor Institut Teknologi Telkom Purwokerto memimpin Rapat Tinjauan Manajemen untuk SMKI, yang dilakukan setidaknya satu kali dalam satu tahun.

4. Tahapan "*Action*" dilakukan hal-hal berikut:
   a. *Management Representatives* memastikan diimplementasikannya tindakan perbaikan dan/atau tindakan pencegahan sebagaimana yang teridentifikasi pada tahapan "*Check".*
   b. *Management Representatives* mengkoordinasikan pengukuran keefektifan tindakan perbaikan dan/atau tindakan pencegahan terkait dengan SMKI yang telah dilakukan.
   c. *Management Representatives* memastikan peningkatan berkelanjutan terhadap implementasi SMKI.

- *Management Representatives* mengendalikan seluruh dokumen yang menjadi acuan bagi implementasi SMKI.
- Seluruh bagian/unit yang ada di Institut Teknologi Telkom Purwokerto mengendalikan rekaman-rekaman hasil implementasi SMKI pada area yang relevan dengan divisi tersebut.

7.1.1.2. KOORDINASI KEAMANAN INFORMASI

Pelaksanaan aktifitas keamanan informasi harus dikoordinasikan oleh manajer keamanan informasi (*information security manager*) yakni Kepala Aset Informasi , Pengelolaan dan Pengoperasian Keamanan Informasi.

7.1.1.3. PROSES RENCANA KOMUNIKASI

1. Komunikasi Internal
   a. Komunikasi internal organisasi merupakan proses penyampaian informasi antara pegawai di lingkungan Institusi untuk memastikan setiap informasi yang berhubungan dengan pelaksanaan sistem manajemen layanan sampai kepada pihak yang tepat;
   b. Aktivitas yang dilakukan dalam komunikasi internal organisasi, antara lain:
      - Rapat berkala;
      - Sosialisasi;
      - Penyampaian laporan kepada atasan/*Top Management.*
   c. Media komunikasi yang dapat digunakan dalam komunikasi internal organisasi/institusi, antara lain:
      - Papan pengumuman;
      - Surat elektronik (*Email);*
      - *Website;* dan
      - Sistem informasi lainnya yang terdapat di Institusi.
   d. Hasil aktivitas komunikasi internal organisasi dicatat dalam bentuk notulen rapat, pengumuman, surat edaran, memo, ketetapan atau bentuk lainnya. Masing-masing personil Institusi menyimpan dan memelihara catatan aktivitas komunikasi internal.

2. Komunikasi Eksternal
   a. Komunikasi eksternal organisasi merupakan komunikasi antara Institusi dengan pihak di luar Institusi.
   b. Aktivitas komunikasi eksternal organisasi, antara lain:
      - Sosialisasi layanan yang diberikan oleh Institusi;
      - Pelaporan kinerja layanan yang diberikan oleh Institusi;
      - Penanganan laporan gangguan, permintaan layanan, dan keluhan terhadap layanan;
      - Survei kepuasan pelanggan;
      - Rapat berkala dengan perwakilan pelanggan; dan
      - Rapat berkala dengan penyedia layanan.
   c. Media komunikasi yang dapat digunakan dalam komunikasi eksternal, antara lain:
      - Telepon atau surat elektronik yang disampaikan kepada *Helpdesk* sebagai *Single point of contact;* dan
      - Surat antar unit pengelola dengan pengguna layanan.
   d. Hasil aktivitas komunikasi eksternal organisasi dicatat dalam bentuk notulen rapat, pengumuman, surat edaran, memo, ketetapan, atau bentuk lainnya. Masing-masing personil menyimpan dan memelihara catatan aktivitas komunikasi eksternal.

7.1.1.4. PROSES OTORISASI UNTUK FASILITAS PEMROSESAN INFORMASI

1. Terhadap suatu fasilitas pemrosesan informasi baru yang memroses informasi sensitif, maka Kepala Bagian IT Support akan menyusun Surat Penunjukan kepada staf (atau beberapa staf) *ICT/Engineer* lainnya yang terpilih sebagai administrator fasilitas pemrosesan informasi tersebut, yang dengan kriteria dan tugas sebagai berikut:

   - Administrator harus dari kalangan staf yang memiliki kompetensi yang cukup untuk mengadministrasikan fasilitas informasi tersebut.
   - Administrator terpilih harus melakukan pengaturan hak akses terhadap seluruh *user* yang akan mengakses fasilitas informasi tersebut, serta secara rutin melakukan pemeriksaan terhadap perangkat keras dan perangkat lunak untuk memastikan kesesuaian dengan komponen sistem yang lain dan memenuhi standar.

2. Pengendalian juga diterapkan untuk penggunaan fasilitas pribadi baru yang diberikan hak untuk memroses informasi bisnis (misalnya komputer jinjing, komputer, atau *handheld devices*). Pengendalian yang dilakukan sesuai dengan butir 7.2.1.3 mengenai Ketentuan Penggunaan Aset TI yang sesuai.

7.1.1.5. HUBUNGAN DENGAN PIHAK YANG BERWENANG

Jika terjadi insiden yang mengakibatkan kehilangan/kerusakan informasi atau tersebarnya suatu informasi rahasia ke pihak-pihak yang tidak berwenang, maka akan dilakukan hal-hal sebagai berikut:

1. Penanganan insiden sesuai dengan mekanisme penanganan insiden yang berlaku.
2. Jika terdapat potensi tindak pidana, maka akan dikoordinasikan untuk menghubungi pihak-pihak yang berwajib.

7.1.1.6. HUBUNGAN DENGAN PIHAK YANG MEMILIKI KEAHLIAN KHUSUS

Setiap Administrator Fasilitas Teknologi Informasi yang menyimpan, mengolah informasi sensitif diharuskan mendaftarkan diri kepada asosiasi/komunitas keahlian (*expert user-group*). Hal ini bertujuan agar mendapatkan *update* yang cukup terhadap perkembangan terbaru terkait aspek keamanan informasi terkait fasilitas teknologi informasi yang dikelolanya.

7.1.1.7. PERJANJIAN KERAHASIAAN MENGENAI TANGGUNG JAWAB KEAMANAN INFORMASI

1. Sebagai bagian dari perjanjian yang tertuang di dalam kontrak atau perjanjian terpisah, staf tidak tetap, staf kerja paruh waktu, rekanan, calon rekanan, dan pihak eksternal lainnya, diharuskan untuk menyetujui dan menandatangani perjanjian kerahasiaan yang menyebutkan tanggung jawab pihak eksternal dan Institut Teknologi Telkom Purwokerto terhadap keamanan informasi sebelum memberikan akses ke informasi dan aset yang berkaitan.
2. Perjanjian kerahasiaan dan *non-disclosure* harus ditinjau saat terjadinya perubahan pada peran dan tanggung jawab serta harus ditinjau secara berkala untuk memastikan kesesuaian dengan kebutuhan Institut Teknologi Telkom Purwokerto.

7.1.2. Persyaratan Keamanan Informasi untuk pihak eksternal

Tujuan

Untuk mengelola keamanan informasi Institut Teknologi Telkom Purwokerto dan fasilitas yang digunakan untuk memroses informasi yang diakses, diproses, dikomunikasikan atau dikelola oleh pihak-pihak eksternal.

Risiko

Pertukaran informasi antara pihak eksternal dan Institut Teknologi Telkom Purwokerto tanpa akuntabilitas dapat berakibat pada kebocoran keamanan informasi.

7.1.2.1. IDENTIFIKASI RISIKO ASET INFORMASI YANG TERKAIT DENGAN PIHAK EKSTERNAL

1. Risiko aset informasi di Institut Teknologi Telkom Purwokerto dan fasilitas yang digunakan untuk memroses informasi yang melibatkan pihak eksternal harus diidentifikasi dan dikontrol sebelum memberikan akses untuk meminimalkan risiko keamanan dengan pihak eksternal. Akses baru hanya dapat diberikan setelah kontrol diimplementasikan.

2. Tipe akses yang diberikan kepada pihak eksternal harus diidentifikasi, diklasifikasi dan alasan pemberian akses harus dijelaskan.
3. Penggunaan fasilitas informasi oleh pihak ketiga harus dipantau.
4. Administrator fasilitas informasi bertanggung jawab untuk mengidentifikasi, menetapkan, serta memantau kontrol-kontrol tersebut.

7.1.2.2. PERJANJIAN KEAMANAN INFORMASI DENGAN PIHAK KETIGA

1. Pihak ketiga harus membaca, menyetujui, dan menandatangani persyaratan dan ketentuan kontrak penugasan mereka yang menyebutkan tanggung jawab terkait dengan keamanan informasi Institut Teknologi Telkom Purwokerto.
2. Pengecekan kebenaran latar belakang (*background check*) untuk pihak ketiga yang berpotensi mengakses informasi sensitif atau mengakses fasilitas pemrosesan informasi. Pengecekan tersebut berdasarkan dengan hukum, peraturan, dan kode etik yang berlaku.
3. Tanggung jawab pada saat mengubah atau menghentikan pekerjaan pihak ketiga harus dijabarkan dengan jelas dan terdokumentasi. Hal ini termasuk:
   a. Semua aset Institut Teknologi Telkom Purwokerto yang berada di pihak ketiga akan dikembalikan kepada Institut Teknologi Telkom Purwokerto setelah periode pekerjaan atau kontrak berakhir.
   b. Hak akses dan fasilitas yang digunakan oleh pihak ketiga untuk memroses informasi harus dihapus setelah periode pekerjaan atau kontrak berakhir.

7.2. Pengelolaan Aset

7.2.1 Tanggung Jawab Terhadap Aset

Tujuan
Untuk memastikan bahwa kontrol keamanan informasi yang sesuai telah diterapkan untuk melindungi aset Institut Teknologi Telkom Purwokerto dalam mencapai dan mengelola kerahasiaan, integritas, dan ketersediaan, serta untuk memastikan bahwa semua aset Institut Teknologi Telkom Purwokerto memiliki pemilik (*asset owner*).

Risiko
Keamanan informasi yang tidak diimplementasikan dengan baik dapat berakibat pada kebutuhan bisnis yang tidak terpenuhi dan kebocoran informasi atau kegagalan fasilitas dalam memroses informasi.
Keamanan informasi harus diterapkan untuk melindungi aset informasi Institut Teknologi Telkom Purwokerto, aset yang ditinggalkan dalam keadaan tidak terlindungi dapat berakibat adanya potensi kerugian finansial pada Institut Teknologi Telkom Purwokerto.

7.2.1.1. PERSEDIAAN ASET (*INVENTORY OF ASSET*)

1. Institut Teknologi Telkom Purwokerto harus mendata dan mendokumentasikan semua aset yang memiliki kaitan terhadap informasi.

2. Hasil pendataan aset harus mencakup semua informasi yang dibutuhkan untuk mengidentifikasi risiko-risiko yang mungkin terjadi terhadap aset tersebut.

7.2.1.2. KEPEMILIKAN ASET

1. Kepemilikan harus ditentukan terhadap setiap aset yang telah didata.
2. Pemilik aset bertanggung jawab atas keamanan aset dan/atau informasi yang tersimpan dalam aset tersebut.

7.2.1.3. PENGGUNAAN ASET YANG SESUAI (*ACCEPTABLE USE OF ASSET*)

1. Aset terkait informasi harus digunakan secara sesuai agar informasi yang ada di dalamnya berada dalam keadaan yang aman.
2. Penggunaan aset yang benar mencakup hal-hal berikut:
   - Fasilitas pemrosesan informasi harus terlindungi secara fisik dan logis. Perlindungan secara fisik dapat dilakukan dengan penyimpanan pada tempat yang terlindungi, perlindungan secara logis dapat dilakukan menggunakan *password*, *screen lock*, enkripsi, dan sebagainya.
   - Fasilitas pemrosesan informasi harus ditentukan sesuai penggunaannya. Hal ini mencakup namun tidak terbatas pada ketentuan penggunaan alat pesan elektronis (*e-mail* organisasi, *instant messenger*, dan sebagainya), penggunaan akses internet organisasi, penggunaan aplikasi, dan penggunaan *file sharing*.
3. Seluruh personel Institut Teknologi Telkom Purwokerto, termasuk staf tidak tetap, staf kerja paruh waktu, rekanan, calon rekanan, dan pihak eksternal lainnya harus mengikuti ketentuan penggunaan aset yang sesuai.

7.2.2. Klasifikasi Informasi

Tujuan
Untuk memastikan bahwa informasi mendapatkan perlindungan yang sesuai.

Risiko
Keamanan informasi yang tidak dikontrol dan diklasifikasikan dengan tepat dapat mengakibatkan terjadinya akses yang tidak tepat.

7.2.2.1. PANDUAN KLASIFIKASI INFORMASI

Informasi diklasifikasikan untuk menentukan manfaat, sensitivitas, serta tingkat perlindungan yang sesuai terhadap informasi tersebut, dengan ketentuan sebagai berikut:

Klasifikasi Informasi	Definisi	Contoh
Strictly Confidential	Informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu operasional	• Surat maupun dokumen yang hanya boleh diketahui oleh Manajemen IT Telkom Purwokerto

	kegiatan perusahaan dan/atau menyebabkan kerugian secara finansial atau bahkan terhentinya operasional bisnis serta reputasi institusi	• Informasi Institusi tentang merger, akuisisi, kontrak, prakiraan keuangan, atau hasil sebelum pengungkapan internal/public • Informasi perencanaan strategis institusi sebelum pengungkapan internal/publik
Confidential	Informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu operasional kegiatan perusahaan dan/atau menyebabkan kerugian secara finansial serta reputasi institusi namun tidak menyebabkan terhentinya operasional bisnis institusi	• Topologi jaringan institusi • Laporan penilaian keamanan.audit internal dan eksternal • PII (*Personally Identifiable Information*) tentang pelanggan (misalkan nomor rekening, PIN, nomor jaminan sosial) atau karyawan (misalnya payroll/informasi gaji, data medis, dan lain-lain)
Internal Use Only	Informasi yang tidak untuk konsumsi publik, informasi ini boleh diketahui Bersama antar pegawai, dan biarpun informasi tersebut tersebar di public, tidak mengganggu operasional kegiatan perusahaan dan/atau menyebabkan kerugian secara finansial serta reputasi institusi.	• Komunikasi internal ditujukan hanya untuk pegawai, seperti berita divisi, surat/email berisi bulltin/berita, SOP, Instruksi kerja, standar, dan lain-lain • Publikasi internal
Publik	Penyebaran informasi tidak akan menyebabkan kerugian bagi perusahaan dan mitra jika secara bebas dibagi kepada masyarakat umum. Tidak ada pembatasan untuk informasi yang dianggap publik	• Siaran Pers • Pemasaran program dirilis ke masyarakat umum • Pidato

Setiap Kepala Bagian/Unit bertanggung jawab untuk mengkoordinasikan pengidentifikasian seluruh informasi yang ada pada bidangnya sesuai dengan klasifikasi di atas.

7.2.2.2. PENAMAAN DAN PENANGANAN INFORMASI (*INFORMATION LABELLING AND HANDLING*)

1. Ketentuan Pelabelan Informasi adalah sebagai berikut:

Klasifikasi Informasi	Ketentuan tentang Pelabelan
Strictly Confidential	Diberi label dengan stempel atau *footer "Strictly Confidential"* baik untuk *softcopy* maupun *hardcopy*. Label harus ada pada lemari penyimpanan, folder, map, dan bindernya (bila ada).
Confidential	Diberi label dengan stempel atau *footer "Confidential"* baik untuk *softcopy* maupun *hardcopy*. Label harus ada pada setiap halaman/*screen view*.
Internal Use Only	Diberi label dengan stempel atau *footer "Internal Use Only"* baik untuk *softcopy* maupun *hardcopy*. *L* abel harus ada pada setiap halaman/*screen view*.
Publik	Tidak perlu diberi label

2. Ketentuan tentang penanganan informasi sesuai dengan klasifikasinya adalah sebagai berikut:

Klasifikasi Informasi	Pertukaran	Ketentuan tentang Penyimpanan	Ketentuan tentang Pemusnahan
Publik	Lihat bagian 7.5.8 Pertukaran Informasi	Tidak ada ketentuan khusus mengenai penyimpanan.	Tidak ada ketentuan khusus mengenai pemusnahan.
Internal Use Only		Tidak ada ketentuan khusus mengenai penyimpanan.	Menghapus data-data atau melakukan format sehingga media dapat digunakan untuk keperluan lain.
Confidential dan *Strictly Confidential*		Disimpan dalam tempat yang terproteksi, sebagai berikut: Untuk informasi dalam bentuk *softcopy*: 1) Disimpan dalam folder non-portable. 2) Akses ke folder tempat penyimpanan informasi harus dikendalikan. 3) Untuk *softcopy* yang disimpan pada media *removable (flash disk, CDROM,* dan sebagainya) harus disimpan dalam lemari tertutup dan terkunci dengan kondisi aman, kunci lemari penyimpanan harus dikendalikan peredaran/penyimpanannya. Untuk informasi dalam bentuk *hardcopy*: 1) Disimpan dalam lemari tertutup dan terkunci dengan kondisi aman. 2) Kunci lemari penyimpanan harus dikendalikan peredaran/penyimpanannya.	Untuk informasi dalam bentuk *softcopy*: a. Harus mendapat persetujuan dari minimal direksi terkait. b. Penghapusan dilakukan dengan teknik *non-recoverable* dan bersifat total serta dituangkan dalam Berita Acara. c. Jika dalam prosesnya tidak dapat dimusnahkan secara total, maka dilakukan pemusnahan media penyimpanan secara fisik. d. Format media disaksikan oleh paling sedikit dua orang saksi di luar divisi yang sama dengan pihak yang melakukan *formatting*. Untuk informasi dalam bentuk *hardcopy:* a. Untuk klasifikasi informasi *Strictly Confidential* harus mendapat persetujuan minimal dari direksi. Sedangkan untuk informasi *Confidential*, minimal mendapat persetujuan dari *General Manager (GM)* terkait. b. Penghancuran dokumen menggunakan penghancur kertas. c. Penghancuran disaksikan oleh paling sedikit dua orang saksi di luar divisi yang sama dengan pihak yang melakukan penghancuran dokumen.

7.3. Kebijakan Keamanan Informasi untuk Sumber Daya Manusia

7.3.1. Sebelum Mempekerjakan Staf

Tujuan

Untuk memastikan bahwa seluruh personel Institut Teknologi Telkom Purwokerto, termasuk staf tetap, staf tidak tetap, staf kerja paruh waktu, rekanan, calon rekanan, dan pihak eksternal lainnya mengerti mengenai tanggung jawabnya, sesuai dengan peran

yang diberikan, serta dapat mengurangi risiko adanya *human error*, pencurian, kecurangan, dan penyalahgunaan fasilitas.

Risiko
Kurangnya pengaturan personel dapat membahayakan keamanan informasi.

7.3.1.1. PERAN DAN TANGGUNG JAWAB

Peran dan tanggung jawab terkait keamanan informasi harus dijelaskan dan dikomunikasikan dengan jelas dalam deskripsi pekerjaan (*job description*), persyaratan, dan ketentuan pekerjaan sebelum mempekerjakan staf tersebut.

7.3.1.2. *SCREENING*

Pemeriksaan kebenaran latar belakang (*background check*) pada semua kandidat staf INSTITUT TEKNOLOGI TELKOM PURWOKERTO, termasuk staf tidak tetap, staf kerja paruh waktu, rekanan, calon rekanan, dan pihak eksternal lainnya harus dilakukan terkait dengan hukum, peraturan dan etika, klasifikasi dari informasi yang bisa diakses, dan risiko yang dirasakan. Hal ini setidaknya meliputi:

a. Karakteritistik yang memuaskan;
b. Pemeriksaan (untuk kelengkapan dan keakuratan) terhadap riwayat hidup kandidat;
c. Konfirmasi terhadap kualifikasi akademis dan profesional;
d. Pemeriksaan identitas (KTP, paspor, atau dokumen sejenis); dan
e. Pemeriksaan lebih detil, seperti pemeriksaan jumlah kewajiban/kredit atau catatan kriminal, jika diperlukan.

Verifikasi latar belakang dapat dilakukan pada proses rekrutmen atau dilakukan secara tersendiri.

7.3.1.3. PERSYARATAN DAN KETENTUAN PENEMPATAN PERSONEL

Semua staf Institut Teknologi Telkom Purwokerto harus mempunyai tanggung jawab untuk meningkatkan kesadaran keamanan informasi mereka dengan mengikuti pelatihan yang berkaitan dengan peran, tanggung jawab, dan keahlian staf.

7.3.2. Selama Masa Kerja Staf

Tujuan
Untuk memastikan bahwa setiap personel Institut Teknologi Telkom Purwokerto termasuk staf tidak tetap, staf kerja paruh waktu, rekanan, calon rekanan, dan pihak eksternal lainnya sadar akan keamanan informasi dan peduli dengan tanggung jawab dan kewajiban mereka.

Risiko
Kurangnya pengaturan staf dapat membahayakan keamanan informasi.

7.3.2.1. TANGGUNG JAWAB MANAJEMEN

Manajemen Institut Teknologi Telkom Purwokerto harus memastikan bahwa semua personel Institut Teknologi Telkom Purwokerto sadar akan peran dan tanggung jawab keamanan informasi pada hari-hari kerja dalam mengakses informasi dan aset yang sensitif.

7.3.2.2. KESADARAN DAN PELATIHAN KEAMANAN INFORMASI

1. Manajemen harus memantau keahlian dan kualifikasi staf terkait dengan keamanan informasi yang cocok dengan deskripsi pekerjaan (*job description*) staf.
2. Semua staf Institut Teknologi Telkom Purwokerto harus mendapatkan pelatihan yang sesuai dan pembaruan terkait kebijakan, prosedur, dan tanggung jawab keamanan informasi yang berkaitan dengan fungsi pekerjaan mereka.
3. Pelatihan pengguna harus menjelaskan mengenai konsekuensi kedisiplinan staf terhadap tanggung jawab keamanan informasi untuk mencegah staf dalam melanggar kebijakan keamanan Institut Teknologi Telkom Purwokerto.

7.3.2.3. PROSES PENEGAKAN DISIPLIN

Penegakan disiplin terkait pelanggaran terhadap keamanan informasi harus memastikan perlakuan yang benar dan adil kepada semua staf Institut Teknologi Telkom Purwokerto yang diduga telah melakukan pelanggaran keamanan.

7.3.3. Pemberhentian atau Perubahan Staf

Tujuan
Untuk memastikan bahwa setiap orang, termasuk staf tidak tetap, staf kerja paruh waktu, rekanan, calon rekanan, dan pihak eksternal lainnya, berhenti atau berubah pekerjaan sesuai dengan tata cara yang telah ditetapkan.

Risiko
Tanpa adanya tata cara berhenti yang wajar, terdapat kemungkinan yang tinggi terjadinya akses yang tidak terotorisasi (*unauthorized access*), selain itu juga terdapat kemungkinan terjadinya kebocoran informasi.

7.3.3.1. TANGGUNG JAWAB PEMBERHENTIAN

Ketentuan tentang pemberhentian hubungan kerja sebagai konsekuensi pelanggaran keamanan informasi di Institut Teknologi Telkom Purwokerto harus secara jelas didefinisikan dan ditetapkan dalam Perjanjian Kerja Kepegawaian.

7.3.3.2. PENGEMBALIAN ASET

Semua staf Institut Teknologi Telkom Purwokerto harus mengembalikan semua aset Institut Teknologi Telkom Purwokerto setelah pemberhentian dari pekerjaan, kontrak, atau perjanjian.

7.3.3.3. PENGHAPUSAN HAK AKSES

Hak akses dari semua staf Institut Teknologi Telkom Purwokerto atas informasi dan fasilitas yang digunakan untuk memroses informasi harus dihapus setelah pemberhentian dari pekerjaan, kontrak atau perjanjian, atau disesuaikan setelah adanya perubahan pekerjaan.

7.4. Kebijakan Keamanan Informasi untuk Pengelolaan Lingkungan dan Fisik

7.4.1. Area yang Aman (*Secured Area*)

Tujuan
Untuk mencegah akses fisik yang tidak terotorisasi, kerusakan, dan campur tangan ke dalam informasi Institut Teknologi Telkom Purwokerto.

Risiko
Akses yang tidak terotorisasi dapat mengakibatkan kehilangan atau kerusakan informasi atau aset.

Pembagian wilayah (area) berdasarkan tingkat keamanan informasinya adalah sebagai berikut:

Klasifikasi Area	Definisi	Contoh
Area Level 1	Area yang dapat diakses oleh pegawai atau tamu tanpa pengaturan khusus	Lobby
Area Level 2	Area yang hanya dapat diakses oleh pegawai dan tamu yang terdaftar yang memperoleh akses sesuai ketentuan yang ada.	Ruang kerja, Ruang rapat, Ruang manajemen
Area Level 3	Area yang hanya dapat diakses oleh pegawai dan tamu yang sudah diotorisasi	Ruang Data Center, Server

7.4.1.1. BATAS KEAMANAN AKSES FISIK (*PHYSICAL SECURITY PERIMETER*)

Batas Keamanan Askes Fisik ditentukan sebagai berikut:

Klasifikasi Area	Perlindungan fisik yang diterapkan

Area Level 1	Tidak memerlukan proteksi fisik khsuus
Area Level 2	Terlindung dengan dinding dan pintu
Area Level 3	• Aktivitas dan perlengkapan tidak terlihan dari luar • Pintu, dinding, atap, dan laintai diperkuat sehingga tahan dari kebakaran

7.4.1.2 KONTROL AKSES FISIK

Kontrol Akses Masuk Fisik ditentukan sebagai berikut:

Klasifikasi Area	Pengendalian Akses	Otorisasi Akses
Area Level 1	Tidak ada	Petugas keamanan gedung
Area Level 2	Kartu Akses	Petugas keamanan Gedung, pegawai, kepala bagian dan/atau kepala bagian Humas
Area Level 3	Kartu akses	Petugas keamanan Gedung, pegawai, kepala bagian dan/atau kepala bagian Humas

7.4.1.3 PERLINDUNGAN TERHADAP ANCAMAN DARI LINGKUNGAN

Perlindungan terhadap ancaman lingkungan ditentukan sebagai berikut:

Klasifikasi Area	Persyaratan Lingkungan
Area Level 1	• Memenuhi persyaratan Kesehatan dan keselamatan kerja yang ditentukan pemerintah • Terpantau CCTV
Area Level 2	• Memenuhi persyaratan Kesehatan dan keselamatan kerja yang ditentukan pemerintah • Terpantau CCTV
Area Level 3	• Memenuhi persyaratan Kesehatan dan keselamatan kerja yang ditentukan pemerintah • Terpantau CCTV • Memenuhi semua persyaratan keamanan

	fisik/informasi/teknologi informasi • Memenuhi persyaratan lingkungan dari peralatan yang ada di dalamnya • Akses masuk personel terbatas

7.4.1.4. AKSES PUBLIK, AREA PENGIRIMAN, DAN PENGISIAN BARANG

1. Titik akses, seperti area pengiriman dan pengisian barang harus diisolasi, dikontrol, dan jika memungkinkan tidak diberikan akses sedemikian rupa sehingga setiap orang tidak terotorisasi tidak dapat menggunakan fasilitas pemrosesan informasi.
2. Barang yang masuk harus diperiksa dari kemungkinan adanya ancaman sebelum dipindahkan ke lokasi yang telah ditentukan.

Kiriman barang masuk dan keluar harus dipisahkan secara fisik jika memungkinkan.

7.5. Manajemen Operasi dan Komunikasi IT

7.5.1. Prosedur dan Tanggung Jawab Manajemen Keamanan Informasi

Tujuan
Untuk memastikan keakuratan dan keamanan operasi dari fasilitas pemrosesan informasi.

Risiko
Kebutuhan bisnis dapat tidak terpenuhi karena ketidakakuratan atau ketidakamanan proses operasional.

7.5.1.1. PENDOKUMENTASIAN SISTEM MANAJEMEN INFORMASI

Semua dokumentasi yang berkaitan dengan pengelolaan sistem informasi harus dipelihara dan tersedia untuk semua pengguna yang membutuhkannya.

1. Perubahan pada setiap dokumentasi membutuhkan persetujuan dari manajemen atau dari orang yang didelegasikan oleh manajemen.
2. Penduplikasian dokumen harus mendapatkan persetujuan dari pemilik dokumen.

7.5.1.2. MANAJEMEN PERUBAHAN DARI FASILITAS PEMROSESAN INFORMASI

1. Perubahan terhadap fasilitas dan sistem pemrosesan informasi harus dikelola dengan baik dan perubahan yang diusulkan memerlukan persetujuan manajemen dan orang yang terotorisasi melalui prosedur persetujuan yang telah diformalkan.
2. Perubahan pada sistem operasional harus direncanakan dan diuji.
3. Semua perubahan yang dilakukan terhadap sistem operasional harus disosialisasikan kepada semua pihak yang terkait.

4. Prosedur pengembalian ke pengaturan awal (*fallback*) harus dideskripsikan dengan jelas termasuk prosedur dan tanggung jawab untuk membatalkan dan memulihkan perubahan yang tidak berhasil.

7.5.1.3. PEMISAHAN TUGAS DAN TANGGUNG JAWAB

1. Pemisahan tugas dan juga tanggung jawab harus dilakukan untuk mengurangi potensi modifikasi sistem yang tidak terotorisasi dan tidak disengaja.
2. Kontrol harus diterapkan untuk menghindari risiko adanya staf yang tidak terotorisasi untuk mengakses, memodifikasi sistem, atau menggunakan aset tanpa otorisasi.
3. Aktifitas pemantauan, *audit trail*, dan manajemen pengendalian harus dipertimbangkan untuk mengurangi modifikasi yang tidak disengaja atau tidak terotorisasi terhadap aset.

7.5.1.4. PEMISAHAN ANTARA FASILITAS PENGEMBANGAN, PENGUJIAN, DAN OPERASIONAL/PRODUKSI

1. Lingkungan pengembangan, pengujian, dan operasional/produksi harus dipisahkan bila memungkinkan untuk mengurangi risiko akses dan perubahan yang tidak terotorisasi atas sistem.
2. Prosedur formal harus dikembangkan dalam proses transfer *software* dari lingkungan pengembangan ke lingkungan operasional/produksi.
3. Pengembang sistem dan pihak yang melakukan modifikasi atas sistem tidak boleh mengakses lingkungan operasional/produksi.
4. Prosedur *login* terpisah harus digunakan untuk lingkungan pengembangan dan operasional/produksi. Prosedur ini harus secara jelas mengidentifikasi lingkungan yang boleh dan tidak boleh diakses.
5. Lingkungan sistem pengembangan dan atau pengujian harus menyamai lingkungan sistem operasional/produksi semirip mungkin.
6. Data yang sensitif tidak boleh di-*copy* ke dalam lingkungan sistem pengujian.

7.5.2. Pengendalian Layanan Pihak ke Tiga

Tujuan
Untuk memastikan bahwa pihak ketiga yang memberikan layanan terhadap pemrosesan informasi melaksanakan ketentuan-ketentuan terkait keamanan informasi.

Risiko
Kehilangan/kebocoran informasi sensitif oleh pihak ketiga.

7.5.2.1. PEMANTAUAN KINERJA PIHAK KETIGA

1. Evaluasi kinerja keamanan informasi serta kepatuhan terhadap ketentuan keamanan informasi untuk setiap pihak ketiga yang memberikan layanan terkait dengan kegiatan/fasilitas pemrosesan harus dilakukan secara rutin,

sesuai dengan ketentuan yang berlaku di organisasi terkait pemantauan kinerja pihak ketiga.
2. Selain evaluasi kinerja, audit terhadap pihak ketiga yang memberikan layanan terkait dengan kegiatan/fasilitas pemrosesan harus pula dilakukan secara rutin.

7.5.2.2. PENGELOLAAN PERUBAHAN TERHADAP LAYANAN PIHAK KETIGA

Jika terdapat perubahan terkait layanan pihak ketiga, proses addendum perjanjian harus dilakukan, sesuai dengan mekanisme addendum perjanjian dan kontrak kerja yang berlaku di organisasi.

7.5.3. Perencanaan dan Penerimaan Sistem

Tujuan
Untuk memastikan bahwa fasilitas pemrosesan informasi beroperasi dengan benar dan aman, dan untuk meminimalisasi risiko kegagalan aset informasi.

Risiko
Kebutuhan bisnis dapat tidak terpenuhi karena aset informasi yang dibutuhkan tidak tersedia.

7.5.3.1. MANAJEMEN KAPASITAS UNTUK ASET INFORMASI DAN FASILITAS PEMROSESAN INFORMASI

1. Permintaan kapasitas harus dipantau, disesuaikan, dan dibuat perkiraan berdasarkan kebutuhan kapasitas yang akan datang untuk memastikan kinerja sistem yang dibutuhkan.
2. Pemilik aset informasi harus memantau sumber daya sistem yang utama seperti beban *processor*, penyimpanan disk, *memory*, printer, dan *output* lainnya dan mengidentifikasi tren pemakaian, khususnya dalam hubungannya dengan aplikasi bisnis/perdagangan atau alat sistem informasi manajemen untuk menghindari hambatan dan ketergantungan pada sumber daya sistem yang utama yang dapat mengancam keamanan sistem informasi atau layanan, sehingga dapat merencanakan langkah mitigasi yang sesuai.

7.5.3.2. PENERIMAAN SISTEM INFORMASI

1. Kriteria dan proses penerimaan (*acceptance criteria*) untuk implementasi sistem baru dan peningkatan sistem informasi harus ditetapkan, disetujui, didokumentasikan, dan diuji sesuai dengan karakteristik dan *best practice* sistem tersebut.
2. Pengujian dan penyesuaian terhadap kriteria penerimaan sistem informasi baru harus dilakukan sebelum sistem dapat diterima di lingkungan operasional/produksi.

7.5.4. Perlindungan Terhadap *Malicious Code* dan *Mobile Code*

Tujuan
Untuk melindungi integritas *software* dan informasi dengan mencegah dan mendeteksi *malicious code* dan juga *mobile code* yang tidak terotorisasi.

Risiko
Malicious code dan *mobile code* yang tidak terotorisasi dapat menimbulkan kehilangan atau kerusakan pada aset atau informasi.

7.5.4.1. KONTROL TERHADAP *MALICIOUS CODE*

1. Penggunaan *software* yang tidak diotorisasi tidak diperbolehkan.
2. *Software* anti-virus harus diinstal pada semua *personal computer* dan diperbaharui secara rutin.
3. Semua *file* harus dideteksi dengan *software* anti-virus sebelum digunakan.
4. Lampiran *email* harus dideteksi terhadap virus di *mail server* sebelum digunakan.
5. Rencana kesinambungan bisnis harus diterapkan untuk pemulihan terhadap serangan virus.
6. Prosedur harus diterapkan untuk proses verifikasi dan tindak lanjut pada saat terkena virus.
7. Program pengecekan virus harus secara berkesinambungan dilakukan pada semua *server* LAN (*Local Area Network*) dan *personal computer*.

7.5.4.2. KONTROL TERHADAP *MOBILE CODE*

1. Jika penggunaan *mobile code* diperbolehkan, harus ada konfigurasi yang dapat memastikan bahwa *mobile code* yang terotorasi beroperasi sesuai dengan kebijakan keamanan yang ditentukan, dan pengeksekusian *mobile code* yang tidak terotorisasi dapat dicegah.
2. Tindakan yang harus diterapkan untuk mencegah pengeksekusian *mobile code* yang tidak terotorisasi, antara lain:
   a. Memblokir seluruh penggunaan dan penerimaan *mobile code*
   b. Mengaktifkan parameter teknis pada sistem tertentu untuk memastikan *mobile code* telah dikendalikan
   c. Memantau sumber daya yang tersedia untuk akses *mobile code*
   d. Menggunakan kontrol kriptografi dalam mengotentikasi *mobile code*

7.5.5. *Backup*

Tujuan
Untuk memelihara integritas dan ketersediaan informasi dan aset yang terkait.

Risiko
Informasi yang tidak di-*backup* tidak bisa dipulihkan jika informasi hilang atau rusak. Risiko penting lainnya yang mungkin muncul adalah pemulihan tidak akan dapat dilakukan jika prosedur dan seperangkat *backup* tidak diuji secara rutin.

7.5.5.1. *BACKUP* INFORMASI

1. *Backup* harus dilakukan secara rutin terhadap informasi dan *software* yang telah ditetapkan sebagai aset.
2. Media *backup* dan dokumentasi hasil *backup* harus disimpan dan dikelola dengan baik.
3. Media *backup* serta hasil *backup* harus diuji secara rutin.
4. Prosedur *restore* harus diuji dan ditinjau secara rutin.
5. Frekuensi *backup* harus didefinisikan terkait dengan pertimbangan keamanan informasi.
6. Hasil *backup* harus disimpan pada tempat yang aman dan memiliki profil risiko yang berbeda.
7. Duplikasi utama tidak boleh digunakan untuk kegiatan bisnis normal (hanya boleh digunakan untuk kondisi darurat).

7.5.6. Manajemen Keamanan Jaringan

Tujuan
Untuk memastikan perlindungan informasi pada jaringan dan infrastruktur pendukung.

Risiko
Kerahasiaan dan integritas dari informasi pada jaringan dapat disalahgunakan atau aset informasi menjadi tidak tersedia.

7.5.6.1. KONTROL TERHADAP JARINGAN

1. Pihak yang bertanggung jawab atas jaringan harus membuat kontrol untuk memastikan keamanan data pada jaringan. Batasan yang tegas harus diberikan kepada kerahasiaan dan integritas dari data yang diberikan ke jaringan publik dan/atau jaringan nirkabel.
2. Tanggung jawab dan prosedur harus diterapkan untuk mengelola akses remote (*remote access*).
3. Kontrol harus diterapkan untuk memastikan ketersediaan layanan jaringan.
4. Pencatatan dan pemantauan harus diterapkan untuk mencegah pemakaian atas jaringan yang tidak terotorisasi.
5. Staf tidak boleh membuat sambungan terhadap *intranet server*, *local area network*, *modern connection* terhadap jaringan internal yang ada, atau sistem *multi-user* lainnya untuk melakukan komunikasi tanpa persetujuan dari pihak yang berwenang terkait keamanan informasi.

7.5.6.2. KEAMANAN ATAS LAYANAN JARINGAN

1. Keamanan layanan jaringan harus diidentifikasi dan dimasukkan di dalam seluruh perjanjian layanan jaringan, baik layanan yang disediakan secara *in-house* atau *outsource*.
2. Keamanan untuk layanan jaringan, termasuk:
   a. teknologi yang diterapkan untuk layanan jaringan keamanan;

b. parameter teknis yang dibutuhkan untuk koneksi yang aman dalam layanan jaringan; dan
c. Prosedur untuk membatasi pemakaian layanan jaringan, jika dibutuhkan.

7.5.7. Penanganan Media

Tujuan
Untuk mencegah kebocoran data yang tidak terotorisasi, modifikasi, penghapusan, atau penghancuran aset, serta untuk melindungi informasi yang disimpan dari kerusakan, pencurian, dan akses yang tidak terotorisasi.

Risiko
Informasi dapat dirusak, dicuri, atau diakses oleh pihak yang tidak terotorisasi.

7.5.7.1. PENGELOLAAN *REMOVABLE MEDIA* YANG BERISI INFORMASI

1. Isi dari *re-usable media* harus dihapus dengan teknik *non-recoverable* pada saat data tersebut sudah tidak diperlukan.
2. Semua media yang berisi informasi sensitif harus disimpan di lingkungan yang aman dan sesuai kesepakatan dengan spesifikasi organisasi pembuat media tersebut.
3. Klasifikasi dan pendaftaran dari *removable media* harus diterapkan untuk mencegah kehilangan data.
4. Syarat dan alasan penggunaan *removable media drive* dan/atau media penyimpan yang hanya boleh digunakan jika ada alasan bisnis yang valid dan dibenarkan.

7.5.7.2. PENGHAPUSAN MEDIA YANG BERISI INFORMASI

Semua media informasi harus dikumpulkan dan dihapus dengan aman, dengan teknik *non-recoverable*.

7.5.7.3. PROSEDUR PENANGANAN INFORMASI

1. Prosedur harus diterapkan untuk proses pembuatan, penanganan, pendistribusian, dan penyimpanan informasi. Prosedur juga harus diterapkan untuk mengomunikasikan informasi yang sesuai dengan klasifikasinya.
2. Akses harus dibatasi untuk mencegah akses yang tidak terotorisasi.
3. Kontrol harus diambil untuk data masukan (*input*), pemrosesan data, dan data keluaran (*output*).
4. Kontrol harus diterapkan untuk melindungi sensitivitas data keluaran (*output*).

7.5.7.4. KEAMANAN ATAS DOKUMENTASI SISTEM

1. Dokumentasi sistem harus disimpan dengan aman.
2. Meminimalisasi akses ke dokumentasi sistem.
3. Daftar akses harus diotorisasi oleh administrator sistem.

7.5.8. Pertukaran Informasi di Dalam dan di Luar Institut Teknologi Telkom Purwokerto

Tujuan
Untuk memelihara keamanan pertukaran informasi dan *software* serta mencegah kehilangan, modifikasi, dan penyalahgunaan pertukaran informasi di dalam Institut Teknologi Telkom Purwokerto dan dengan pihak luar.

Risiko
Informasi sensitif dapat hilang atau terhambat selama proses pertukaran informasi berlangsung yang mengakibatkan kehilangan, modifikasi, atau penyalahgunaan informasi.

7.5.8.1. PROSEDUR DAN KEBIJAKAN PERTUKARAN INFORMASI

Prosedur mengenai pertukaran informasi ditetapkan sebagai berikut:

Klasifikasi Informasi	Ketentuan tentang Pertukaran
Strictly Confidential dan *Confidential*	Dipertukarkan secara terkontrol dan terproteksi, sebagai berikut: Untuk informasi dalam bentuk *softcopy* dan ditransmisikan melalui jaringan komputer/publik atau dipertukarkan melalui media portabel (*flash disk*, CDROM, dan sebagainya): a. Digunakan teknik enkripsi. b. Sebelum mempertukarkan informasi dilakukan konfirmasi terlebih dahulu. c. Sebelum mempertukarkan informasi, pihak penerima harus terlebih dahulu menandatangani perjanjian pertukaran informasi/perjanjian kerahasiaan. d. Khusus untuk dokumen *Strictly Confidential* pengiriman *softcopy* tidak diizinkan melalui jaringan komputer. e. Serah terima informasi *Confidential* untuk pertukaran informasi melalui email wajib mengaktifkan *Receipt Confirmation Status*. f. Serah terima pertukaran informasi melalui media portabel antara Perusahaan dengan *customer* atau pihak luar lainnya diberitaacarakan dengan waktu, tempat dan identitas serah terima tertulis secara jelas. Untuk informasi dalam bentuk *hardcopy*: a. Dipertukarkan menggunakan amplop tertutup yang bersegel. b. Sebelum mempertukarkan informasi, dilakukan konfirmasi terlebih dahulu. c. Sebelum mempertukarkan informasi, pihak penerima harus terlebih dahulu menandatangani perjanjian pertukaran informasi/perjanjian kerahasiaan. d. Serah terima diberitaacarakan dengan waktu, tempat dan identitas serah terima tertulis secara jelas. e. Dokumen harus selalu bersama minimal satu orang pegawai/kurir terpercaya sebelum diserahterimakan ke penerima informasi.
Internal Use Only	Dipertukarkan secara bebas antar pegawai Perusahaan.
Publik	Dapat dipertukarkan secara bebas.

7.5.8.2. PERJANJIAN PERTUKARAN INFORMASI DAN *SOFTWARE*

1. Perjanjian Pertukaran Informasi hanya untuk informasi rahasia.
2. Perjanjian Pertukaran Informasi berupa:
   a. Konfirmasi awal antara calon pemberi informasi dan calon penerima informasi. Konfirmasi awal dapat dilakukan secara lisan atau tertulis.
   b. Perjanjian Kerahasiaan yang harus terlebih dahulu ditandatangani oleh calon penerima informasi sebelum informasi tersebut diberikan/dikirimkan.

7.5.8.3. MEDIA FISIK DALAM PERJALANAN

1. Kontrol khusus harus diterapkan untuk menyebarkan informasi sensitif.
2. Kurir yang terotorisasi dan media transportasi yang dapat dipercaya harus digunakan dan dibuat daftarnya.

3. Kerusakan media harus dikelola dengan memberikan perlindungan terhadap penanganan yang direkomendasikan organisasi pembuat media, seperti pengemasan.
4. Kontrol harus diterapkan untuk melindungi informasi sensitif dari kebocoran dan modifikasi yang tidak terotorisasi.

7.5.8.4. PESAN ELEKTRONIK

Staf harus diberikan pengetahuan mengenai risiko penggunaan *email* dan kontrol harus diterapkan untuk mengurangi risiko tersebut, antara lain:
a. Perlindungan pesan dari akses yang tidak terotorisasi;
b. Memastikan alamat penerima pesan yang benar;
c. Tingkat otentikasi untuk mengakses melalui jaringan publik; dan
d. Pertimbangan hukum untuk penggunaan tandatangan elektronik.

7.5.9. Pemantauan Fasilitas Pemrosesan Informasi

Tujuan
Untuk mendeteksi akses yang tidak terotorisasi ke informasi dan aset.

Risiko
Akses yang tidak terotorisasi dapat terjadi melalui sistem operasi maupun aplikasi.

7.5.9.1. *AUDIT LOGGING* DARI *SECURITY EVENT*

Pada setiap fasilitas pemrosesan informasi yang digunakan untuk memroses informasi sensitif, *audit log* yang merekam aktifitas user, *exceptions* dan event keamanan informasi harus tersedia dan disimpan pada waktu yang cukup untuk dilakukan investigasi terhadap insiden keamanan informasi. *Audit log* harus mencakup paling tidak hal-hal berikut ini:
1. *User ID.*
2. Tanggal, waktu dan rincian event-event yang utama, seperti *log-on* dan *log-off*.
3. Identitas terminal yang digunakan.
4. Rekaman terkait keberhasilan/kegagalan terkait usaha-usaha untuk mengakses.
5. Perubahan konfigurasi sistem.
6. Penggunaan hak administrasi (*privilege*).
7. Aplikasi/*system utility* yang digunakan.
8. Alamat jaringan beserta protokolnya.
9. Aktivasi atau deaktivasi sistem proteksi keamanan informasi seperti anti virus, anti spam.

7.5.9.2. PEMANTAUAN PENGGUNAAN SISTEM

1. Penggunaan fasilitas pemrosesan informasi yang digunakan untuk memroses informasi sensitif harus dipantau.
2. Pemantauan setidaknya meliputi hal-hal berikut ini:

a. Akses yang terotorisasi, mencakup *User ID*, waktu dan tanggal, *file* yang diakses, program/utilitas yang digunakan.
b. Pengoperasian hak (*privilege*), mencakup penggunaan akun-akun special (*root, administrator*), aktifitas administrator (*start up*/*shut down* sistem, pemasangan/pelepasan perangkat, perubahan konfigurasi keamanan sistem).
c. Pelanggaran/usaha pelanggaran terhadap *acces policy*.
d. Penggunaan kapasitas untuk komponen-komponen utama dari sistem (memori, *harddisk*, jaringan).

3. Hasil dari aktifitas pemantauan harus ditinjau secara rutin dan tindakan perbaikan harus diambil jika diperlukan.

7.5.9.3. PERLINDUNGAN TERHADAP INFORMASI *LOG*

1. Informasi *log* harus disimpan pada tempat yang terlindungi sehingga tidak dapat terhapus/dihapus secara tidak sengaja.
2. Untuk mencegah *over-write* yang dilakukan oleh sistem, informasi *log* harus disimpan terpisah dari sistem yang menghasilkan *log* tersebut.
3. Akses terhadap informasi *log* harus dibatasi terhadap pengguna yang terotorisasi saja.
4. Aktifitas-aktifitas perubahan terhadap log (seperti perubahan isi dari *log* atau penghapusan log) harus terekam.

7.5.9.4. PERLINDUNGAN TERHADAP *LOG ADMINISTRATOR* DAN OPERATOR

1. Semua aktifitas operator dan administrator sistem harus dicatat dalam suatu informasi *log* dan ditinjau secara rutin.
2. *Log* harus mencakup waktu kejadian, informasi tentang kejadian, akun dan administrator yang terlibat, dan proses yang terlibat.

7.5.9.5. PENCATATAN KESALAHAN (*FAULT*) DARI FASILITAS PEMROSESAN INFORMASI

1. Setiap kesalahan *fault* yang terjadi pada fasilitas pemroesan informasi yang digunakan untuk memroses informasi sensitive harus dicatatkan dalam log, hal ini disebut sebagai *fault log.*
2. *Fault log* harus ditinjau secara rutin untuk memastikan pemecahan masalah yang memadai dan bahwa kontrol belum disepakati.

7.5.9.6. SINKRONISASI WAKTU DI DALAM WILAYAH ORGANISASI

1. Semua fasilitas pemrosesan informasi yang digunakan untuk memroses informasi sensitif harus memiliki waktu (*clock*) yang disinkronkan secara otomatis kepada sumber yang sama (*single clock reference*).
2. Format tanggal/waktu harus secara jelas didefinisikan untuk memastikan bahwa waktu yang tertera pada komputer merefleksikan tanggal/waktu yang sesungguhnya.

Prosedur harus ditetapkan untuk melakukan sinkronisasi waktu secara manual.

7.6. Kontrol Akses Logis (*Logical Access Control*)

7.6.1. Persyaratan Bisnis untuk Kontrol Akses

Tujuan
Untuk memastikan bahwa informasi, fasilitas pemrosesan informasi, dan dokumentasi hanya diakses oleh pengguna yang terotorisasi.

Risiko
Adanya akses yang tidak terotorisasi terhadap sistem informasi dan dokumentasi.

7.6.1.1. KEBIJAKAN KONTROL AKSES

1. Kebijakan kontrol akses baik secara fisik maupun logis harus diterapkan, didokumentasikan, dan ditinjau sesuai dengan kebutuhan bisnis dan keamanan akses.
2. Peraturan kontrol akses untuk masing-masing pengguna pada tiap aplikasi harus dijelaskan di dalam kebijakan kontrol akses.
3. Peraturan kontrol akses harus diterapkan dengan mempertimbangkan hal-hal berikut:
   a. Tingkat akses dan otorisasi dari semua staf untuk aplikasi bisnis/perdagangan dan perkantoran
   b. Mengidentifikasi semua informasi yang berkaitan dengan aplikasi dan risiko bisnis
   c. Konsistensi antara kontrol akses dan kebijakan klasifikasi informasi untuk sistem dan jaringan yang berbeda.
   d. Pemisahan antara peran kontrol akses (seperti permintaan akses, otorisasi akses, serta pengelolaan akses).

7.6.2. Pengelolaan Akses Pengguna Sistem Informasi

Tujuan
Untuk memastikan bahwa informasi dan aset hanya dapat diakses oleh pengguna yang terotorisasi dan mencegah akses yang tidak terotorisasi terhadap sistem informasi.

Risiko
Adanya akses yang tidak terotorisasi terhadap sistem informasi.

7.6.2.1. PENDAFTARAN DAN PENGHAPUSAN PENGGUNA SISTEM INFORMASI

1. Prosedur formal harus diterapkan untuk pendaftaran dan penghapusan pengguna.
2. Semua pengguna harus mempunyai identitas pengguna (*user ID*) yang unik.
3. Otorisasi akses harus diperoleh dari pemilik informasi.

4. Tingkat akses harus sesuai dengan tujuan bisnis dan konsisten dengan kebijakan.
5. Catatan formal harus dikelola untuk semua pengguna yang terdaftar pada sistem.
6. Segera menghapus atau memblok akses pengguna apabila pengguna berganti peran atau pekerjaan atau berhenti dari Institut Teknologi Telkom Purwokerto.
7. Memastikan bahwa tidak ada duplikasi *user ID*.

7.6.2.2. PENGELOLAAN ALOKASI HAK AKSES ISTIMEWA (*PRIVILEGED ACCESS*)

1. Alokasi dan penggunaan hak akses istimewa harus dibatasi dan dikontrol.
2. Hak akses istimewa untuk setiap sistem (sistem operasi, *database*, dan aplikasi) harus diidentifikasi.
3. Hak akses istimewa harus dialokasikan kepada pengguna berdasarkan kebutuhan (*need-to-use basis*) dan kegiatan (*event-by-event basis*) sesuai dengan kebijakan kontrol akses.
4. Sebuah proses otorisasi harus diterapkan untuk:
   a. Memberikan hak akses istimewa
   b. Mencatat semua hak akses istimewa yang dialokasikan
5. Hak istimewa sistem tidak boleh diberikan kepada akun pengguna yang digunakan untuk aktifitas bisnis normal.

7.6.2.3. PENGELOLAAN *PASSWORD* PENGGUNA

1. Kebijakan harus diterapkan untuk mengelola *password*.
2. Menetapkan prosedur untuk verifikasi identitas pengguna setelah memberikan password baru, *password* pengganti, atau *password* sementara.
3. *Password* sementara harus digunakan dengan aman dan mempunyai waktu kadaluwarsa.
4. *Password* sementara harus unik untuk setiap pengguna dan tidak dapat diterka.
5. *Default password* dari vendor harus diubah setelah instalasi.

7.6.2.4. TINJAUAN ATAS HAK AKSES PENGGUNA

1. Sebuah proses harus diterapkan untuk meninjau hak akses pengguna minimal setiap 6(enam) bulan atau apabila terjadi perubahan seperti kenaikan pangkat, transfer atau pemberhentian staf.
2. Otorisasi hak akses istimewa harus ditinjau lebih sering (minimal setiap 3 (tiga) bulan).
3. Alokasi hak akses istimewa harus dicek secara rutin untuk memastikan bahwa hak akses istimewa tidak diberikan kepada pengguna yang tidak terotorisasi.
4. Perubahan kepada akun istimewa (*privileged account*) harus dicatat untuk tinjauan secara berkala.

7.6.3. Tanggung Jawab Pengguna untuk Memelihara Efektivitas Kontrol Akses

Tujuan
Mencegah akses pengguna yang tidak terotorisasi, dan kompromi atau pencurian terhadap informasi dan fasilitas pemrosesan informasi.

Risiko
Akses yang tidak terotorisasi terhadap sistem informasi.

7.6.3.1. PENGGUNAAN *PASSWORD*

1. Pengguna harus menyimpan *password* dengan rahasia dan aman.
2. Hindari menyimpan catatan mengenai password dalam bentuk apa pun.
3. Password harus diubah jika terdapat indikasi bahwa sistem atau *password* telah dikompromikan.
4. *Password* harus kompleks yaitu terdiri dari alfabet(huruf besar, huruf kecil), angka dan karakter khusus (@#$%^&*(){}[]), serta *lower* dan *upper case*.
5. Password minimal terdiri dari 8(delapan) karakter.
6. Umur password maksimal 30(tiga puluh) hari.
7. *Password* yang sama hanya boleh digunakan kembali apabila telah dilakukan minimal 8(delapan) kali pergantian *password* yang berbeda.
8. Bila terjadi kesalahan dalam mengetikkan *password* sebanyak 3(tiga) kali makan akun akan dinonaktifkan secara otomatis.
9. *Password* sementara harus diubah pada waktu *logon* pertama kali.
10. *Password* pengguna tidak boleh disimpan dengan menggunakan prosedur *login* otomatis.
11. Pengguna tidak boleh menyebarkan *password*-nya kepada pengguna lain.
12. Pengguna yang dapat mengakses layanan, sistem, atau *platform* lebih dari 1 (satu), harus mempunyai beberapa *password* yang berbeda.

7.6.3.2. PERALATAN PENGGUNA YANG TIDAK DIJAGA

1. Pengguna harus memastikan bahwa peralatan yang tidak dijaga telah diproteksi dengan baik.
2. Untuk memberikan proteksi terhadap peralatan yang tidak dijaga, maka pengguna harus diberitahu untuk melakukan hal-hal di bawah ini:
   a. Mengakhiri *active session* pada saat telah selesai digunakan.
   b. Komputer atau *server* seharusnya di-*logoff* jika *session*-nya telah berakhir atau jika telah selesai digunakan.
   c. Mengamankan komputer dari akses yang tidak terotorisasi dengan menggunakan *password* atau *key lock.*

7.6.3.3. KEBIJAKAN ATAS KEBERSIHAN MEJA DAN LAYAR KOMPUTER

1. Media informasi harus disimpan di tempat yg terkunci pada saat di luar jam kerja dan pada saat tidak digunakan.

1. Kontrol harus diterapkan untuk melindungi tempat surat yang masuk/keluar dan mesin *facsimile* yang tidak dijaga.
2. Penggunaan yang tidak terotorisasi terhadap mesin fotokopi atau *scanner* harus dicegah.
3. Dokumen harus dipindahkan dari *printer* secara berkala khususnya apabila terdapat dokumen yang sensitif.

7.6.4. Kontrol Akses Terhadap Jaringan

Tujuan
Untuk memastikan bahwa informasi hanya dapat diakses oleh user yang terotorisasi dan untuk mencegah akses yang tidak terotorisasi ke dalam layanan jaringan internal dan eksternal.

Risiko
Akses yang tidak terotorisasi terhadap sistem informasi dan layanan jaringan.

7.6.4.1. KEBIJAKAN PENGGUNAAN LAYANAN JARINGAN

1. Pengguna hanya boleh diberikan akses ke layanan yang telah terotorisasi.
2. Kebijakan harus diterapkan terkait jaringan dan layanan jaringan yang boleh diakses.
3. Adanya prosedur otorisasi untuk menentukan pengguna yang dapat mengakses jaringan dan layanan jaringan.
4. Kontrol harus diterapkan untuk melindungi akses terhadap jaringan dan layanan jaringan tersebut.
5. Penentuan metode (seperti sistem *dial-up* atau *remote*) yang dapat digunakan untuk mengakses layanan jaringan.

7.6.4.2. OTENTIKASI PENGGUNA UNTUK KONEKSI EKSTERNAL

Metode otentikasi yang tepat harus diterapkan untuk mengontrol akses pengguna jarak jauh (*remote user*) seperti penggunaan teknik kriptografi, *token*, atau *protocol*.

7.6.4.3. IDENTIFIKASI PERALATAN PADA JARINGAN

Identifikasi peralatan secara otomatis harus diterapkan untuk mengotentikasi koneksi dari lokasi dan peralatan tertentu.

7.6.4.4. PERLINDUNGAN TERHADAP *REMOTE DIAGNOSTIC AND CONFIGURATION PORT*

1. Akses fisik terhadap *diagnostic and configuration port* harus dikontrol, antara lain dengan menggunakan *key lock* atau dengan adanya perjanjian antara kepala unit dari layanan komputer dan personel pendukung yang memerlukan akses.

2. *Port*, layanan, dan fasilitas serupa yang diinstal pada komputer dan jaringan yang tidak diperlukan dalam kegiatan bisnis, harus di-*disable* atau dihapus.

7.6.4.5. PEMBAGIAN DI DALAM JARINGAN

1. Jika memungkinkan, jaringan yang besar harus dibagi ke dalam domain logis yang lebih kecil untuk memisahkan kelompok layanan, pengguna, dan informasi. Kriteria pemisahan harus berdasarkan persyaratan kontrol akses.
2. Jaringan terpisah harus memiliki perimeter keamanan yang jelas dan terpisah oleh *gateway* yang aman atau bisa juga dengan melakukan pergantian IP.
3. Penilaian risiko harus diterapkan untuk mengidentifikasi kontrol untuk memelihara pemisahan jaringan.

7.6.4.6. KONTROL TERHADAP KONEKSI JARINGAN

Kapabilitas koneksi dari jaringan yang dibagi ke seluruh batasan IT Telkom Purwokerto harus dibatasi terutama untuk email, transfer *file*, dan akses terhadap aplikasi.

7.6.4.7. KONTROL TERHADAP JARINGAN PENGIRIMAN (*NETWORK ROUTING*)

1. Kontrol pengiriman (*routing control*) harus diterapkan untuk memastikan bahwa koneksi konputer dan alur informasi tidak melanggar kebijakan kontrol akses.
2. *Gateway* dapat digunakan untuk melakukan validasi alamat sumber dan tujuan pada titik kontrol jaringan internal dan eksternal.

7.6.5. Kontrol Akses Sistem Operasi

Tujuan
Untuk mencegah akses yang tidak terotorisasi terhadap sistem operasi.

Risiko
Akses yang tidak terotorisasi terhadap sistem operasi maupun aplikasi.

7.6.5.1. PROSEDUR KEAMANAN *LOGON*

1. Akses ke semua sistem harus mewajibkan adanya proses dan prosedur keamanan *logon*.
2. Prosedur *logon* hanya menampilkan informasi yang berkaitan dengan sistem tersebut seminimal mungkin.
3. Prosedur *logon* harus menampilkan peringatan yang menyebutkan bahwa sistem tersebut hanya dapat diakses oleh para pengguna yang mempunyai hak akses

4. Pesan dari sistem tidak boleh mengidentifikasikan penyebab *error* terjadi selama proses *logon.*
5. Jumlah upaya *logon* tidak sukses yang diperbolehkan dibatasi sebanyak 5(lima) kali.
6. Membatasi waktu yang diperbolehkan untuk melakukan proses *logon* dan apabila melebihi waktu yang ditentukan maka proses *logon* dihentikan.
7. Sesaat setelah upaya *logon* berhasil dilakukan, tanggal dan waktu dari *logon* sebelumnya harus ditampilkan bersamaan dengan upaya *logon* yang tidak berhasil sejak *logon* terakhir dilakukan.
8. Sistem *logon* seharusnya tidak menampilkan *password-password* yang dimasukkan. Karakter *password* dapat disembunyikan dengan menggunakan simbol.

7.6.5.2. OTENTIKASI DAN IDENTIFIKASI PENGGUNA

1. Identitas pengguna (*user ID*) tidak boleh mengindikasikan tingkat akses.
2. Prosedur otentikasi harus diterapkan untuk semua pengguna.
3. Identitas pengguna dapat digunakan untuk melacak aktifitas individu yang bertanggung jawab.
4. Jika otentikasi dan verifikasi identitas diperlukan, metode otentikasi *password* alternatif, seperti kriptografi, *smart card*, *token*, dapat digunakan.

7.6.5.3. PENGGUNAAN UTILITAS SISTEM (*SYSTEM UTILITY*)

1. Penggunaan utilitas sistem yang memiliki kemampuan untuk mengubah kontrol sistem atau fasilitas pemrosesan informasi yang digunakan untuk memroses informasi sensitif harus dikendalikan dengan ketat.
2. Utilitas sistem dari *software* aplikasi harus terpisah.
3. Utilitas sistem harus dihapuskan dari sistem apabila tidak dibutuhkan lagi.
4. Prosedur identifikasi, otentikasi, dan otorisasi harus diterapkan untuk utilitas sistem.

7.6.5.4. PEMBATASAN WAKTU KONEKSI

1. Aplikasi-aplikasi yang sensitif atau *terminal* dengan tingkat risiko tinggi harus dikonfigurasi dengan waktu koneksi yang terbatas.
2. Batasan waktu koneksi didasarkan pada hasil asesmen risiko.
3. Pembatasan waktu koneksi harus diterapkan, hal ini termasuk:
   a. Pembatasan waktu koneksi hanya pada jam kerja normal jika tidak ada persyaratan lembur atau perpanjangan jam operasi
   b. Mempertimbangkan otentikasi ulang pada selang waktu

7.6.6. *Mobile Computing* dan *Teleworking*

Tujuan
Untuk memastikan keamanan informasi pada saat menggunakan fasilitas *mobile computing* dan *teleworking*.

Risiko
Aset-aset yang merupakan bagian dari fasilitas pemrosesan informasi yang sensitif yang digunakan *off site* akan rusak atau informasi disalahgunakan oleh pihak yang tidak terotorisasi karena aset berada di luar dari kontrol keamanan informasi IT Telkom Purwokerto.

7.6.6.1. KEAMANAN INFORMASI UNTUK *MOBILE COMPUTING*

1. Setiap peralatan *mobile computing* yang memiliki informasi dengan klasifikasi rahasia didalamnya harus dilindungi secara logik dengan data enkripsi serta personal *firewall*. Khusus untuk telepon selular dan PDA memiliki kemampuan untuk menghapus data secara *remote*.
2. Setiap pengguna *mobile computing* harus memberikan pengamanan terhadap peralatan tersebut untuk mencegah adanya kegagalan dan kerusakan informasi akibat penyebaran *malware* maupun *malicious code*. Khusus untuk telepon selular dan PDA sebaiknya dilengkapi dengan peralatan untuk mencegah adanya kegagalan dan kerusakan informasi akibat penyebaran *malware* maupun *malicious code*.
3. Pembatasan akses melalui *access control* yang ketat harus diimplementasikan kepada Pengguna yang melakukan akses ke jaringan Organisasi melalui VPN.
4. Pengguna disarankan untuk melakukan virus *scanning* sebelum terkoneksi ke VPN organisasi dan anti-virus yang digunakan wajib dikinikan secara periodik.
5. Setiap pengguna *mobile computing* disarankan untuk menerapkan prinsip kehati–hatian dalam pengunaan peralatan tersebut antara lain:
   a. penggunaan *cable lock* pada *notebook* yang digunakan di tempat umum/publik, misal hotel, tempat *training* ataupun *meeting* di luar lingkungan Organisasi, dan sebagainya;
   b. Menghindari serta meningkatkan kewaspadaan pada saat menggunakan peralatan *mobile computing* di tempat umum/publik yang terbuka, terutama di area pusat keramaian yang terbuka di luar lingkungan organisasi,
   c. Mengimplementasikan penggunaan *password* yang aman untuk dapat akses ke dalam peralatan *mobile computing*,
   d. Menerapkan perlindungan dari akses yang tidak berhak pada saat perangkat *mobile computing* pada saat *idle*, misalnya *screen lock* pada telepon seluler*, screen saver* pada perangkat *notebook*.
   e. Menggunakan *user account* dengan *limited privileges* pada saat bekerja di tempat umum/publik.
   f. Menghindari akses dari pihak tidak berhak atas peralatan *mobile computing* yang digunakan.
6. Pengguna *mobile computing* disarankan melaksanakan *backup* secara periodik atas data–data organisasi dalam peralatan tersebut.

7.6.6.2. KEAMANAN INFORMASI UNTUK AKTIFITAS *TELEWORKING*

1. Kegiatan *teleworking* yang dilaksanakan harus menggunakan *site-to-site* VPN.
2. Pekerja organisasi yang akan melaksanakan kegiatan teleworking diharuskan memperhatikan lokasi tempat bekerja, antara lain sebagai berikut:
   a. Menghindari bekerja di tempat umum yang terbuka.
   b. Memperhatikan keamanan fisik sekitar lokasi tempat teleworking dilakukan, bila dianggap cukup rawan, disarankan untuk mencari lokasi baru.
3. Setiap jaringan *teleworking* yang dipersiapkan harus memperhatikan faktor keamanan.
4. Setiap akses ke dalam jaringan organisasi atas kegiatan *teleworking* harus melewati proses identifikasi dan otentikasi.

7.7. Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi

7.7.1. Kebutuhan Keamanan Sistem Informasi

Tujuan
Untuk memastikan bahwa keamanan menjadi bagian yang utuh dari sistem informasi.

Risiko
Sistem tanpa pertimbangan keamanan yang sesuai dapat mengakibatkan sistem dan informasi disalahgunakan oleh pihak yang tidak terotorisasi.

7.7.1.1. SPESIFIKASI DAN ANALISA KEBUTUHAN KEAMANAN

1. Identifikasi kebutuhan bisnis untuk sistem informasi baru, atau peningkatan dari sistem informasi yang sudah ada harus menjelaskan persyaratan persyaratan keamanan informasi. Persyaratan ini termasuk, tapi tidak terbatas untuk: sistem operasi, *database*, infrastruktur, aplikasi perdagangan dan perkantoran.
2. Spesifikasi persyaratan keamanan informasi harus mempertimbangkan kontrol otomatis serta kontrol manual sebagai pendukungnya. Pertimbangan yang serupa harus diterapkan pada saat mengevaluasi *software package* yang dikembangkan atau dibeli untuk aplikasi perdagangan dan perkantoran.
3. Kebutuhan sistem untuk keamanan informasi dan proses untuk mengimplementasikan keamanan harus diintegrasikan pada tahap awal proyek sistem informasi.
4. Jika produk sistem informasi dibeli, harus dilakukan analisis dan pengujian terkait dengan persyaratan keamanan dan kontrak dengan pemasok harus mengidentifikasikan persyaratan keamanan.

7.7.2. Pemrosesan yang Benar pada Aplikasi

Tujuan
Untuk mencegah *error*, kehilangan, dan modikasi yang tidak terotorisasi atau penyalahgunaan informasi pada aplikasi.

Risiko
Sistem tanpa kontrol yang tepat dapat mengakibatkan informasi dan/atau sistem disalahgunakan oleh pihak yang tidak terotorisasi.

7.7.2.1. VALIDASI DATA *INPUT*

1. Data *input* pada aplikasi harus divalidasi untuk memastikan bahwa data tersebut benar dan tepat.
2. Data *input* yang penting harus diperiksa, setidaknya meliputi hal-hal di bawah ini:
   a. Duplikasi data *input*
   b. Nilai di luar ruang lingkup (*out-of-range value*)
   c. Data yang kurang atau hilang
3. Tinjauan secara rutin terhadap *file* data untuk memastikan bahwa data valid dan kontrol berfungsi dengan baik.
4. Dokumen *input* harus ditinjau terkait dengan perubahan yang tidak terotorisasi.
5. Validasi otomatis dari data *input* harus dipertimbangkan, jika memungkinkan, untuk mengurangi risiko *error*, dan untuk mencegah penyerangan standar termasuk *buffer overflow* dan *code injection*.
6. Catatan dari aktifitas proses *input* data harus diterapkan.

7.7.2.2. KONTROL TERHADAP PEMROSESAN INTERNAL

1. Pengecekan validasi data harus dimasukkan pada aplikasi untuk mendeteksi informasi yang rusak karena *hardware error*, *processing error* atau *deliberate act*.
2. Kontrol harus diterapkan pada tahap desain dan implementasi aplikasi untuk memastikan bahwa risiko kegagalan pemrosesan yang dapat mengakibatkan hilangnya integritas data telah diminimalisasi.

7.7.2.3. INTEGRITAS PESAN

1. Persyaratan untuk memastikan otentikasi dan perlindungan integritas pesan pada aplikasi harus diidentifikasi, dan kontrol yang tepat harus diidentifikasi dan diimplementasi.
2. Teknik kriptografi dapat digunakan sebagai alat yang sesuai untuk pengimplementasian otentikasi pesan.
3. Sebuah penilaian risiko keamanan harus dilakukan untuk menentukan jika integritas data dibutuhkan dan untuk mengidentifikasi metode implementasi yang paling sesuai.

7.7.2.4. VALIDASI DATA *OUTPUT*

1. Data *output* dari aplikasi harus divalidasi untuk memastikan bahwa pemrosesan dari informasi yang disimpan adalah benar dan tepat.
2. Data *output* dari aplikasi harus divalidasi dengan:
   a. Pengecekan untuk memastikan bahwa data *output* masuk akal.
   b. Pengecekan rekonsiliasi untuk memastikan bahwa semua data telah diproses.
   c. Menyediakan informasi yang cukup bagi pembaca atau proses untuk memastikan bahwa informasinya akurat dan lengkap.

7.7.3. Kontrol Kriptografi

Tujuan
Untuk melindungi kerahasiaan, otentikasi, dan integritas informasi dengan menggunakan metode kriptografi.

Risiko
Informasi dapat disalahgunakan oleh pihak yang tidak terotorisasi tanpa kontrol enkripsi yang tepat.

7.7.3.1. KEBIJAKAN PENGGUNAAN KONTROL KRIPTOGRAFI

1. Teknik enkripsi (kriptografi) harus diterapkan untuk mempertukarkan serta menyimpan informasi rahasia.
2. Teknik enkripsi (kriptografi) yang digunakan ditentukan berdasarkan hasil asesmen risiko, biaya pengadaan sistem enkripsi serta kesepakatan dengan/persyaratan yang ditentukan oleh pihak-pihak eksternal yang terkait.

7.7.3.2. PENGELOLAAN KUNCI KRIPTOGRAFI

1. Pengelolaan kunci harus diterapkan untuk mendukung efektifitas penggunaan teknik kriptografi.
2. Kunci kriptografi harus selalu dilindungi dari modifikasi dan penghapusan.
3. Kunci kriptografi hanya dapat digunakan untuk jangka waktu tertentu.
4. Teknik kriptografi dapat digunakan untuk melindungi kunci kriptografi.
5. Staf internal harus merupakan satu-satunya orang yang mengelola kunci, tidak ada pihak ketiga yang diperbolehkan untuk mengelola kunci kriptografi.

7.7.4. Keamanan File Sistem

Tujuan
Untuk memastikan bahwa *file* sistem terlindungi dari akses ke sistem yang tidak terotorisasi dan campur tangan ke dalam aset informasi.

Risiko

Tanpa kontrol *file* sistem yang sesuai, dapat mengakibatkan adanya akses yang tidak terotorisasi ke dalam sistem dan informasi dan/atau data disalahgunakan oleh pihak yang tidak terotorisasi.

7.7.4.1. KONTROL TERHADAP *SOFTWARE* OPERASIONAL

1. Harus ada prosedur untuk mengontrol instalasi *software* pada sistem operasi.
2. Sistem operasional/produksi hanya boleh memegang *executable code* yang telah disetujui
3. Sistem operasional/produksi tidak boleh memegang *development code*.
4. *Executable code* harus diuji, *user acceptance* harus diperoleh, dan *source library* diperbaharui sebelum diimplementasikan ke dalam lingkungan operasional.
5. Prosedur *rollback* harus tersedia sebelum perubahan diimplementasikan.
6. *Audit log* harus dipelihara untuk semua pembaharuan terhadap perpustakaan program operasi (*operational program libraries*).
7. Versi sebelumnya dari *software* harus selalu dipertahankan.
8. *Software* lama harus diarsipkan bersama dengan semua informasi yang dibutuhkan dan parameter, prosedur, konfigurasi detil, dan *software* pendukung selama data disimpan di dalam arsip.
9. *Software patch* harus diterapkan jika dapat mengurangi kelemahan keamanan.
10. Akses fisik dan logis terhadap sistem produksi hanya dapat diberikan kepada *supplier* dengan tujuan mendukung jika dibutuhkan dan harus mendapatkan otorisasi dari manajemen.

7.7.4.2. PERLINDUNGAN TERHADAP SISTEM PENGUJIAN DATA

1. Penggunaan *database* operasional yang berisi informasi pribadi atau informasi sensitif untuk kepentingan pengujian harus dihindari. Jika informasi pribadi atau informasi sensitif digunakan untuk tujuan kepentingan pengujian, semua detil dan isi informasi sensitif harus dihapus sebelum digunakan.
2. Prosedur kontrol akses yang sesuai dengan sistem aplikasi operasional/produksi harus diterapkan juga ke dalam sistem aplikasi pengujian.
3. Otorisasi terpisah harus diterapkan setiap kali informasi operasional di-*copy* ke sistem aplikasi pengujian.
4. Informasi operasional harus dihapus dari sistem aplikasi pengujian secepatnya setelah pengujian selesai dilakukan.
5. Semua penduplikasian dan penggunaan data operasional harus dicatat ke dalam *audit trail* dan di-*review*.

7.7.4.3. KONTROL AKSES TERHADAP PROGRAM *SOURCE CODE*

1. Akses terhadap program *source code* harus dikontrol dengan ketat untuk menghindari perubahan yang tidak disengaja. Hal ini dapat dilakukan dengan mengontrol *program source library*.
2. Program *source library* tidak boleh berada dalam sistem produksi.
3. Akses terhadap program *source library* harus dibatasi hanya untuk personel yang terotorisasi.
4. Pembaharuan program *source library* hanya boleh dilakukan apabila otorisasi telah didapatkan.
5. *Audit log* harus dikelola terhadap semua akses ke dalam progam *source library* dan harus di-*review* secara rutin.

7.7.5. Keamanan di Dalam Proses Pengembangan dan Pendukung

Tujuan
Untuk memastikan bahwa keamanan diterapkan terhadap sistem informasi dan *software* sistem aplikasi.

Risiko
Jika keamanan tidak dipertimbangkan pada tingkat pengembangan sistem informasi, sistem lebih sering untuk terkena pelanggaran keamanan.

7.7.5.1. PROSEDUR KONTROL PERUBAHAN

1. Implementasi perubahan harus dikontrol dengan menggunakan prosedur kontrol perubahan formal untuk meminimalisasi gangguan terhadap ketersediaan layanan informasi serta ancaman terhadap keamanan informasi.
2. Pengenalan sistem baru dan perubahan penting terhadap sistem yang sudah ada harus mengikuti proses formal dokumentasi, spesifikasi, pengujian, pengendalian kualitas (*quality control*), dan bila diperlukan pengujian keamanan informasi.
3. Kontrol Perubahan harus mencakup proses penilaian risiko, analisis dampak perubahan, dan spesifikasi kontrol keamanan informasi yang dibutuhkan.
4. Kontrol Perubahan harus mencakup proses untuk memastikan bahwa pengguna yang terotorisasi menerima perubahan sebelum dilakukan implementasi.
5. *Audit trail* untuk semua permintaan perubahan harus dikelola.
6. Kontrol Perubahan harus mencakup proses untuk memastikan bahwa implementasi perubahan dilakukan pada waktu yang tepat dan tidak mengganggu proses bisnis.
7. Dokumentasi sistem harus diperbaharui untuk mencerminkan semua perubahan dan dokumentasi sistem yang lama harus diarsip.

7.7.5.2. TINJAUAN TEKNIS ATAS APLIKASI SETELAH PERUBAHAN SISTEM OPERASI

Ketika dilakukan perubahan terhadap sistem operasi, aplikasi bisnis dan perkantoran yang penting harus ditinjau dan diuji untuk memastikan bahwa tidak terdapat dampak yang merugikan terhadap operasi atau keamanan IT Telkom Purwokerto.

7.7.5.3. LARANGAN PERUBAHAN *SOFTWARE PACKAGE*

1. Modifikasi terhadap *software package* harus dihindari, dan semua perubahan harus dikontrol dengan ketat.
2. Ketika modifikasi tidak dapat dihindari, hal-hal di bawah ini harus dipertimbangkan:
   a. Memastikan bahwa kontrol yang diterapkan dan proses integritas tidak dicampurtangani.
   b. Memastikan apakah ijin dari *vendor* harus diperoleh.
   c. Mendapatkan hasil modifikasi dari *vendor* jika memungkinkan.
   d. Dampak jika *vendor* tidak mendukung perubahan tersebut.
   e. Menyimpan duplikasi dari versi yang tidak dimodifikasi.
3. Semua perubahan harus diuji dan didokumentasikan.

7.7.5.4. KEBOCORAN INFORMASI

Setiap kemungkinan terjadinya kebocoran informasi harus dicegah. Usaha-usaha untuk mencegah kebocoran informasi mencakup hal-hal berikut namun tidak terbatas kepada:

1. Melakukan *scanning* media dan komunikasi terhadap informasi tersembunyi.
2. Menggunakan sistem dan *software* yang memiliki integritas tinggi, seperti menggunakan produk yang telah dievaluasi oleh pihak independen.
3. Melakukan pemantauan secara rutin terhadap aktifitas personel dan sistem, seperti penggunaan kamera pengintai (CCTV).

7.7.5.5. PENGEMBANGAN *OUTSOURCED SOFTWARE*

Apabila diputuskan untuk melakukan pengembangan *outsource software*, maka harus dilakukan perlindungan-perlindungan berikut:

1. *Outsourced Software Developer* harus terbukti memiliki kemampuan dan reputasi yang baik dalam hal keamanan informasinya.
2. Persyaratan kualitas dan fungsi keamanan harus digarisbawahi di dalam kontrak.
3. Pengujian *source code* yang dibuat oleh *Outsourced Software Developer* harus dilakukan secara rutin untuk mendeteksi potensi adanya ancaman atau kelemahan terhadap keamanan informasi, sebelum *source code* tersebut dimasukkan ke dalam *source code* library milik organisasi.

7.7.6. Pengelolaan Kerentanan Teknis (*Technical Vulnerability*)

Tujuan
Untuk mengurangi risiko yang dihasilkan oleh eksploitasi kerentanan teknis.

Risiko
Tanpa adanya pengelolaan kerentanan yang tepat, terdapat risiko yang tinggi di dalam aset informasi terhadap kerentanan teknis.

7.7.6.1. KONTROL ATAS KERENTANAN TEKNIS (*TECHNICAL VULNERABILITY*)

1. Tanggung jawab terkait pemantauan penilaian risiko *technical vulnerability*, *technical vulnerability*, *implementasi patch* terkait fasilitas informasi yang digunakan untuk memroses informasi sensitif harus ditetapkan.
2. Harus dilakukan pengujian secara rutin untuk mengidentifikasi adanya kerentanan teknis pada fasilitas informasi yang digunakan untuk memroses informasi sensitif.
3. Semua informasi spesifik yang dibutuhkan untuk mendukung pengelolaan kerentanan teknis *(technical vulnerability*) termasuk *software vendor*, *version number*, daftar *software* beserta *patch update detil* harus tersedia.
4. Jika potensi kerentanan teknis (*technical vulnerability*) telah diidentifikasi, harus segera dilakukan tindakan perbaikan.

7.8. Pengelolaan Insiden Keamanan Informasi

7.8.1. Pelaporan Terhadap Peristiwa dan Kelemahan Terkait Keamanan Informasi

Tujuan
Untuk memastikan agar peristiwa dan kelemahan keamanan informasi yang berhubungan dengan sistem informasi dikomunikasikan secepat mungkin agar dapat diambil tindakan perbaikan yang tepat.

Risiko
Kelemahan dalam keamanan informasi yang tidak teridentifikasi dapat memicu hilangnya informasi sehingga berdampak pada hilangnya layanan TI dengan cepat.

7.8.1.1. PELAPORAN TERHADAP PERISTIWA (*EVENT*) TERKAIT KEAMANAN INFORMASI

1. Semua staf, kontraktor, dan pihak ketiga harus melaporkan ketika menemui peristiwa (*event*) keamanan informasi.
2. Prosedur pelaporan *event* keamanan informasi harus ditetapkan.

7.8.1.2. PELAPORAN TERHADAP KELEMAHAN KEAMANAN INFORMASI

1. Seluruh staf, kontraktor, dan pihak ketiga pengguna layanan dan sistem informasi diwajibkan untuk melakukan pecatatan dan melaporkan seluruh kelemahan keamanan in formasi yang terdeteksi.
2. Prosedur pelaporan kelemahan keamanan informasi harus ditetapkan.

7.8.2. Pengelolaan Insiden Keamanan Informasi

Tujuan
Untuk memastikan pendekatan yang efektif dan konsisten telah diaplikasikan ke dalam pengelolaan insiden keamanan informasi.

Risiko
Risiko yang berhubungan dengan insiden keamanan tidak dapat diestimasikan secara efektif tanpa adanya bukti dan pemantauan secara terus menerus.

7.8.2.1. PROSEDUR DAN TANGGUNG JAWAB TERKAIT PENANGANAN INSIDEN KEAMANAN INFORMASI

1. Insiden Keamanan Informasi harus dikelola, untuk dapat mengisolir dampaknya serta melakukan tindakan pemulihan yang relatif cepat.
2. Prosedur Pengeolaan Insiden Informasi dapat merupakan bagian dari Prosedur Pengelolaan Insiden Teknologi Informasi, namun harus ditentukan secara jelas:
   a. Kriteria yang membedakan antara insiden keamanan informasi dan insiden yang bukan keamanan informasi
   b. Tanggung jawab setiap pihak terkait proses pelaporan, pencatatan dan koordinasi tindakan perbaikan/pemulihan.

7.8.2.2. *LESSON LEARN* DARI INSIDEN DI DALAM KEAMANAN INFOMASI

Insiden keamanan informasi yang pernah terjadi harus dianalisis untuk diidentifikasi sehingga kontrol untuk mitigasi insiden keamanan informasi terkait frekuensi limit, kerusakan, dan biaya yang akan terjadi di masa yang akan datang dapat diimplementasikan.

7.8.2.3. PENGUMPULAN BUKTI DARI INSIDEN KEAMANAN INFORMASI

Jika tindak lanjut setelah insiden keamanan informasi melibatkan tindakan hukum, maka bukti harus dikumpulkan, disimpan dan disampaikan untuk memenuhi peraturan hukum yang relevan.

7.9. Manajemen Kesinambungan Bisnis (*Business Continuity Management*)

Untuk memastikan agar kegiatan penyediaan informasi dapat tetap berlangsung secara aman pada kondisi di luar normal, maka Organisasi harus menyusun suatu Rencana Keberlangsungan Bisnis yang disebut sebagai *Information Business Continuity Plan* atau disingkat dengan IBCP.

IBCP harus disusun berdasarkan *Business Impact Analysis* (BIA) yang merupakan suatu asesmen yang menilai dampak dari terhentinya penyediaan informasi dan kerusakan suatu aset informasi terhadap bisnis organisasi, yang diakibatkan oleh terjadinya kondisi di luar normal.

Sebuah prosedur penyusunan IBCP harus ditetapkan yang memuat langkah-langkah penyusunan BIA, penyusunan IBCP serta langkah-langkah pengujian IBCP.

Dokumen IBCP harus tersedia di seluruh unit kerja yang menyediakan pelayanan penyediaan informasi serta unit-unit kerja yang menggunakan sistem informasi. IBCP harus diuji secara berkala untuk memastikan keefetifannya terhadap penanganan kondisi di luar normal. Hasil pengujian harus dievaluasi untuk peningkatan.

7.9.1. Aspek Keamanan Informasi Atas Manajemen Kesinambungan Bisnis

Tujuan

Untuk menghadapi gangguan dalam aktifitas bisnis dan untuk memproteksi proses bisnis yang penting dari akibat kegagalan yang fatal (*major failure*) pada sistem informasi atau bencana dan untuk memastikan agar hal tersebut dapat ditangani tepat waktu.

Risiko

Aset informasi yang dibutuhkan tidak dapat dikembalikan/diperbaiki selama bencana, dimana gangguan terhadap bisnis ini dapat menyebabkan kerugian atas pendapatan.

7.9.1.1. KEAMANAN INFORMASI PADA PROSES MANAJEMEN KESINAMBUNGAN BISNIS

1. Proses yang formal perlu ditetapkan untuk mengembangkan dan mengelola rencana bisnis yang berkelanjutan.
2. Pemahaman atas dampak insiden keamanan informasi yang mungkin terjadi.
3. Mempertimbangkan pembelian asuransi yang tepat sebagai bagian dari pengelolaan risiko operasional.
4. Mengidentifikasi dan mempertimbangkan pengimplementasian kontrol pencegahan dan mitigasi tambahan.
5. Memastikan keamanan staf dan perlindungan fasilitas pemrosesan informasi dan properti IT Telkom Purwokerto.

7.9.1.2. PENILAIAN TERHADAP RISIKO DAN KESINAMBUNGAN BISNIS

1. Semua peristiwa yang dapat menyebabkan terjadinya gangguan proses bisnis harus diidentifikasi, begitu juga dengan kemungkinan dan dampak dari terjadinya gangguan tersebut serta konsekuensi keamanan informasinya.
2. Penilaian risiko kesinambungan bisnis harus melibatkan pemilik sumber daya dan proses bisnis.

Berdasarkan hasil penilaian risiko, rencana strategis kesinambungan bisnis harus diterapkan untuk menentukan pendekatan kesinambungan bisnis secara keseluruhan.

7.9.1.3. PENGEMBANGAN DAN PENGIMPLEMENTASIAN RENCANA KESINAMBUNGAN TERMASUK KEAMANAN INFORMASINYA

1. Rencana harus dikembangkan dan diimplementasikan untuk mengelola dan memulihkan operasi dan memastikan ketersediaan informasi pada jangka waktu yang ditentukan setelah terjadi gangguan proses bisnis yang penting.
2. Prosedur tanggung jawab dan kesinambungan bisnis harus diterapkan.
3. Kerugian/kehilangan yang terjadi harus diidentifikasi dan didokumentasikan.
4. Pengujian dan pembaharuan rencana kesinambungan bisnis harus dilakukan.
5. Pelatihan staf harus dilakukan terkait rencana kesinambungan bisnis.
6. Duplikasi atas rencana kesinambungan bisnis dan fasilitas yang diperlukan untuk melaksanakan rencana kesinambungan bisnis tersebut harus disimpan pada lokasi yang dapat dikendalikan dari jarak jauh untuk menghindari terjadinya kerusakan pada waktu terjadi bencana terhadap bangunan utama.
7. Jika alternatif lokasi sementara telah digunakan, maka tingkat kontrol keamanan harus disesuaikan dengan tingkat kontrol yang terdapat di bangunan utama.

7.9.1.4. KERANGKA RENCANA KESINAMBUNGAN BISNIS

1. Kerangka tunggal terkait rencana kesinambungan bisnis harus dikelola untuk memastikan semua rencana konsisten, mengidentifikasi persyaratan keamanan, serta prioritas pengujian dan pengelolaan.
2. Adanya penjelasan mengenai kondisi kapan rencana kesinambungan bisnis harus dijalankan (proses yang harus dilakukan, bagaimana menilai situasi, siapa saja yang terlibat).
3. Prosedur *fallback* yang menjelaskan tindakan yang harus diambil untuk memindahkan aktifitas bisnis yang penting atau layanan pendukung ke lokasi sementara, dan untuk mengembalikan operasional proses bisnis sesuai dengan jangka waktu yang dibutuhkan.
4. Prosedur *resumption* yang menjelaskan tindakan yang harus diambil untuk mengembalikan ke operasi bisnis yang normal.

Sumber daya dan aset penting yang dibutuhkan agar dapat menjalankan prosedur *fallback* dan *resumption.*

7.10. Kepatuhan Kebijakan Keamanan Informasi

7.10.1. Kepatuhan Terhadap Persyaratan Hukum

Tujuan

Untuk menghindari terjadinya pelanggaran terhadap hukum, regulasi, atau kewajiban kontraktual, kebijakan manajemen keamanan informasi, dan persyaratan keamanan lainnya.

Risiko

Ketidakpatuhan terhadap persyaratan regulasi dapat menyebabkan kontrol yang ada tidak dapat berjalan dengan baik.

7.10.1.1. IDENTIFIKASI ATAS PERATURAN YANG SESUAI

Persyaratan kontraktual dan peraturan yang relevan terkait dengan TI harus didefinisikan dan didokumentasikan.

7.10.1.2. HAK KEKAYAAN INTELEKTUAL

1. Penggunaan *software* dan informasi secara legal harus didefinisikan dan didokumentasikan untuk memastikan kepatuhan terhadap hak kekayaan intelektual.
2. Kontrol perlu dibentuk untuk memastikan jumlah pengguna *software* tidak melampaui yang diijinkan.
3. Hanya *software* dan produk yang terlisensi yang dapat diinstal dan pengecekan terhadap lisensi *software* secara rutin untuk memastikan bahwa kondisi lisensi telah sesuai dengan yang dipersyaratkan.
4. *Audit tool* sebaiknya digunakan untuk menguji kepatuhan terhadap kebijakan keamanan informasi.

7.10.1.3. PERLINDUNGAN TERHADAP DATA ORGANISASI

1. Perlu dikeluarkannya pedoman mengenai retensi, penyimpanan, penanganan, dan penghapusan atas data dan informasi.
2. Program dan material kunci kriptografi yang berhubungan dengan arsip yang terenkripsi (*encrypted archive*) atau *digital signature* harus disimpan untuk memungkinkan dilakukannya dekripsi data (*data decryption*).
3. Kontrol harus diterapkan untuk memproteksi data dan informasi dari kehilangan, kerusakan, dan pemalsuan.
4. Kontrol harus diterapkan untuk memastikan bahwa informasi dapat diakses secara tepat waktu ketika diperlukan.

7.10.1.4. PERLINDUNGAN DATA DAN PRIVASI ATAS INFORMASI PRIBADI

1. Data-data pribadi yang ada pada sistem informasi harus dilindungi untuk mencegah penyalahgunaan.
2. Data-data pribadi diklasifikasikan sebagai informasi rahasia, dan harus ditangani sebagaimana informasi rahasia lainnya.

7.10.1.5. PENCEGAHAN ATAS PENYALAHGUNAAN FASILITAS PEMROSESAN INFORMASI

1. Penggunaan aset informasi yang tidak terotorisasi harus dilaporkan kepada atasan dari individu yang terkait serta menerapkan tindakan disiplin yang sesuai.
2. Pendeteksian atas intrusi atau penyusupan, pemantauan konten dan perangkat pemantauan lainnya harus digunakan untuk mencegah dan mendeteksi penyalahgunaan terhadap fasilitas pemrosesan informasi.

7.10.2. Kepatuhan Terhadap Teknik, Standar, dan Kebijakan Keamanan

Tujuan
Untuk memastikan kepatuhan terhadap aturan dan kebijakan manajemen keamanan informasi pada IT Telkom Purwokerto.

Risiko
Kurangnya kepatuhan terhadap aturan keamanan dapat menyebabkan tidak berjalannya kontrol secara efektif.

7.10.2.1. KEPATUHAN TERHADAP STANDAR DAN KEBIJAKAN KEAMANAN

1. Tinjauan independen harus dilakukan secara berkala setiap tahun untuk memastikan bahwa prosedur, standar, dan kebijakan pengelolaan keamanan informasi telah diterapkan.
2. Terdapat mekanisme untuk memungkinkan persetujuan atas pengubahan penerapan kebijakan pengelolaan keamanan informasi.
3. Kepatuhan terhadap kebijakan keamanan juga akan dipantau oleh secara internal dan harus dilaksanakan secara rutin.

7.10.2.2. EVALUASI KEPATUHAN TEKNIS

1. Aset informasi perlu dievaluasi secara rutin untuk memastikan kepatuhan terhadap standar implementasi teknis.
2. Pengujian kepatuhan teknis perlu dilakukan oleh tenaga ahli teknis yang independen.
3. *Penetration test* atau *vulnerability assessment* dapat digunakan sebagai pendekatan evaluasi kepatuhan teknis yang perlu direncanakan, didokumentasikan serta dilaksanakan secara rutin.

7.10.3. Audit Sistem Informasi

Tujuan
Untuk mengoptimalkan efektivitas proses audit sistem informasi serta meminimalisasi interfensi terhadapnya.

Risiko
Kurangnya kepatuhan terhadap penerapan kontrol menyebabkan tindakan koreksi tidak dapat dilakukan dengan tepat waktu.

7.10.3.1. KONTROL *AUDIT* SISTEM INFORMASI

Audit terhadap sistem informasi harus direncanakan untuk meminimalisasi gangguan bisnis.

1. Kebutuhan dan ruang lingkup audit harus disetujui oleh pihak manajemen.
2. Evaluasi terhadap *software* dan data harus dibatasi pada tingkat otorisasi *read only*. Jika membutuhkan tingkat otorisasi yang lebih daripada itu,

maka akses dan data tersebut tersebut segera dihapuskan segera setelah digunakan.

3. Akses terhadap sumber informasi dan sistem selama proses audit harus dipantau dan dicatat.
4. Seluruh prosedur, persyaratan, dan tanggung jawab audit harus didokumentasikan.

7.10.3.2. PERLINDUNGAN ATAS *AUDIT TOOLS* SISTEM INFORMASI

1. Penggunaan serta penyimpanan *audit tool* sistem informasi harus dikendalikan untuk untuk mencegah terjadinya penyalahgunaan.
2. Otorisasi dari manajemen setingkat *wakil rektor* harus diperoleh sebelum dilakukan penggunaan terhadap *audit tool system* informasi.
3. Penggunaan *audit tool system* informasi harus didampingi oleh paling sedikit satu orang saksi dan penggunaannya diberitaacarakan.