LAMPIRAN I
PERATURAN MENTERI PEKERJAAN UMUM
DAN PERUMAHAN RAKYAT REPUBLIK INDONESIA
NOMOR 17 /PRT/M/2016
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI DI KEMENTERIAN PEKERJAAN UMUM DAN PERUMAHAN RAKYAT

STANDAR KEAMANAN INFORMASI

1. TUJUAN

standar ini digunakan sebagai pedoman dalam rangka melindungi aset informasi Kementerian dari berbagai bentuk ancaman baik dari dalam maupun luar Kementerian, yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) aset informasi agar selalu terjaga dan terpelihara dengan baik.

2. RUANG LINGKUP

2.1 standar ini berlaku untuk pengelolaan pengamanan seluruh aset informasi Kementerian dan dilaksanakan oleh seluruh unit kerja, pegawai Kementerian baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi (TIK), dan pihak ketiga di lingkungan Kementerian.

2.2 Aset informasi Kementerian adalah aset dalam bentuk:

2.2.1 Seluruh data/dokumen/informasi sebagaimana diatur dalam klasifikasi informasi yang berlaku;

2.2.2 Piranti lunak, meliputi aplikasi, sistem operasi, sistem basis data, dan alat bantu (*tools*) aplikasi;

2.2.3 Aset fisik, meliputi perangkat komputer, perangkat jaringan dan komunikasi, media penyimpanan (*storage*), media lepas

pasang (*removable media*), dan perangkat pendukung (*peripheral*); dan

2.2.4 Aset tak berwujud (*intangible*), meliputi pengetahuan, pengalaman, keahlian, citra, dan reputasi.

3. KEBIJAKAN

3.1 Setiap Pimpinan Unit Organisasi dan Unit Kerja bertanggung jawab mengatur penerapan Kebijakan dan Standar Keamanan Informasi yang ditetapkan dalam Peraturan Menteri ini di Unit masing-masing.

3.2 Unit Organisasi dan Unit Kerja harus menerapkan Kebijakan dan Standar Keamanan Informasi yang ditetapkan dalam Peraturan Menteri ini di Unit masing-masing.

3.3 Setiap Pimpinan Unit Organisasi dan Unit Kerja bertanggung jawab mengatur pelaksanaan pengamanan dan perlindungan aset informasi di Unit masing-masing dengan mengacu pada Kebijakan dan Standar Keamanan Informasi di Kementerian yang ditetapkan dalam Peraturan Menteri ini.

3.4 Pusdatin dan Unit Organisasi bertanggung jawab meningkatkan pengetahuan, keterampilan, dan kepedulian terhadap keamanan informasi pada seluruh pengguna di lingkungan Unit Organisasi masing-masing.

3.5 Pusdatin dan Unit Organisasi menerapkan dan mengembangkan manajemen risiko dalam rangka pelaksanaan pengamanan dan perlindungan aset informasi.

3.6 Pihak ketiga harus bertanggung jawab untuk melindungi kerahasiaan, keutuhan, dan/atau ketersediaan aset informasi Kementerian.

3.7 Pusdatin dan Unit Organisasi melakukan evaluasi terhadap pelaksanaan Keamanan Informasi secara berkala untuk menjamin efektivitas dan meningkatkan keamanan informasi.

3.8 Inspektorat Jenderal Kementerian melakukan audit internal Keamanan Informasi di Kementerian untuk memastikan pengendalian, proses, dan prosedur Keamanan Informasi dilaksanakan secara efektif sesuai dengan Kebijakan dan Standar Keamanan Informasi di Kementerian.

3.9 Pusdatin dan Unit Organisasi menggunakan laporan audit internal Keamanan Informasi untuk meninjau efektivitas penerapan Keamanan Informasi dan melakukan tindak lanjut terhadap temuan auditor.

4. TANGGUNGJAWAB

4.1 Pihak-pihak yang terkait dalam keamanan informasi terdiri dari:
- 4.1.1 Pemilik aset informasi adalah Pimpinan Unit Organisasi yang memiliki kebutuhan akan keamanan informasi untuk mendukung tugas dan fungsinya;
- 4.1.2 Petugas keamanan informasi adalah pegawai Kementerian dan/atau Pihak Ketiga yang melaksanakan tanggung jawab terkait keamanan informasi;
- 4.1.3 Tim pengendali mutu keamanan informasi (*information security assurance*) adalah tim yang dibentuk untuk melaksanakan kegiatan penjaminan keamanan informasi;
- 4.1.4 Pengguna, adalah pegawai dan bukan pegawai Kementerian yang mengakses informasi Kementerian.

4.2 Pemilik aset informasi mempunyai tanggung jawab terhadap:
- 4.2.1 Menetapkan target keamanan informasi setiap tahunnya dan menyusun rencana kerja untuk Kementerian, masing-masing Unit Organisasi, maupun yang bersifat lintas unit;
- 4.2.2 Memastikan efektivitas dan konsistensi penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian; dan
- 4.2.3 Melaporkan kinerja penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian dan pencapaian target kepada tim pengendali mutu keamanan informasi (*information security assurance*).

4.3 Petugas keamanan informasi mempunyai tanggung jawab terhadap:
- 4.3.1 Melaksanakan dan mengawasi penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian;
- 4.3.2 Memberi masukan peningkatan terhadap Kebijakan dan Standar Keamanan Informasi di Kementerian;
- 4.3.3 Mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan keamanan informasi bagi pegawai;

4.3.4 Memantau, mencatat, dan menguraikan secara jelas gangguan keamanan informasi yang diketahui atau laporan yang diterima, dan menindaklanjuti laporan tersebut sesuai prosedur pelaporan gangguan keamanan informasi; dan

4.3.5 Memberi panduan dan/atau bantuan penyelesaian masalah-masalah keamanan informasi.

4.4 Tim pengendali mutu keamanan informasi (*information security assurance*) mempunyai tanggung jawab terhadap:

4.4.1 Pendampingan dan penjaminan keamanan informasi;

4.4.2 Penyusunan laporan evaluasi pengendali mutu keamanan informasi (*information security assurance*).

4.5 Pengguna mempunyai tanggung jawab terhadap pemberian masukan kepada pemilik aset informasi dan petugas keamanan informasi terkait keamanan informasi.

5. STANDAR

5.1 Standar Keamanan Informasi terdiri atas:

5.1.1 Standar Manajemen Keamanan Informasi;

5.1.2 Standar Pengendalian Pengelolaan Aset Informasi;

5.1.3 Standar Pengendalian Keamanan Sumber Daya Manusia;

5.1.4 Standar Pengendalian Keamanan Fisik dan Lingkungan;

5.1.5 Standar Pengendalian Pengelolaan Komunikasi dan Operasional;

5.1.6 Standar Pengendalian Akses;

5.1.7 Standar Pengendalian Keamanan Informasi dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem informasi;

5.1.8 Standar Pengendalian Pengelolaan Gangguan Keamanan Informasi;

5.1.9 Standar Pengendalian Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan; dan

5.1.10 Standar Pengendalian Kepatuhan.

5.2 Standar Manajemen Keamanan Informasi

5.2.1 Catatan Penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian

1) Pusdatin dan Unit Organisasi harus menggunakan catatan penerapan Kebijakan dan Standar Keamanan

Informasi di Kementerian untuk mengukur kepatuhan dan efektivitas penerapan keamanan informasi.

2) Catatan penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian harus meliputi:
   a. Formulir-formulir sesuai prosedur operasional yang dijalankan;
   b. Catatan gangguan keamanan informasi;
   c. Catatan dari sistem;
   d. Catatan pengunjung di area aman (*secure areas*);
   e. Kontrak dan perjanjian layanan;
   f. Perjanjian kerahasiaan (*confidentiality agreements*); dan
   g. Laporan audit.

5.2.2 Penyusunan dokumen pendukung kebijakan keamanan informasi harus memuat:

1) Tujuan dan ruang lingkup dokumen pendukung kebijakan keamanan informasi;
2) Kerangka kerja setiap tujuan sasaran pengendalian keamanan informasi;
3) Metodologi penilaian risiko (*risk assessment*);
4) Penjelasan singkat mengenai standar, prosedur, dan kepatuhan termasuk persyaratan peraturan yang harus dipenuhi, pengelolaan kelangsungan kegiatan, konsekuensi apabila terjadi pelanggaran;
5) Tanggung jawab dari setiap bagian terkait; dan
6) Dokumen referensi yang digunakan dalam menyusun dokumen pendukung kebijakan keamanan informasi.

5.2.3 Pengendalian Dokumen

1) Pusdatin dan Unit Organisasi harus mengendalikan dokumen keamanan informasi Kementerian untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan, dan mencegah akses oleh pihak yang tidak berwenang.
2) Pusdatin dan Unit Organisasi harus menempatkan dokumen keamanan informasi Kementerian di semua area operasional sehingga mudah diakses oleh pengguna di unit kerja masing-masing sesuai peruntukannya.

5.3 Standar Pengendalian Pengelolaan Aset Informasi

5.3.1 Pemilik Aset Informasi menetapkan dan mengkaji secara berkala klasifikasi aset informasi dan jenis perlindungan keamanannya.

5.3.2 Pemilik Aset Informasi menetapkan pihak yang berwenang untuk mengakses aset informasi.

5.3.3 Dalam pengelolaan aset informasi Kementerian, aset informasi diklasifikasikan mengacu kepada peraturan perundang-undangan yang berlaku.

5.4 Standar Pengendalian Keamanan Sumber Daya Manusia

5.4.1 Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menjadi bagian dari penjabaran tugas dan fungsi, khususnya bagi yang memiliki akses terhadap aset informasi;

5.4.2 Pimpinan dari pegawai berkeahlian khusus atau yang berada di posisi kunci (*key person*) harus memastikan ketersediaan pengganti pegawai tersebut dengan kompetensi yang setara apabila pegawai yang bersangkutan mutasi/berhenti;

5.4.3 Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menyertakan persyaratan untuk:

1) Melaksanakan dan bertindak sesuai dengan tanggung jawabnya terkait keamanan informasi;
2) Melindungi aset dari akses yang tidak sah, penyingkapan, modifikasi, kerusakan atau gangguan;
3) Melaksanakan proses keamanan atau kegiatan keamanan informasi sesuai dengan peran dan tanggung jawabnya; dan
4) Melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan Kebijakan dan Standar Keamanan Informasi di Kementerian.

5.4.4 Pemeriksaan latar belakang calon pegawai dan pihak ketiga Kementerian harus memperhitungkan privasi, perlindungan data pribadi dan/atau pekerjaan berdasarkan peraturan perundang-undangan yang berlaku, meliputi:

1) Ketersediaan referensi, dari referensi hubungan kerja, dan referensi pribadi;
2) Pemeriksaan kelengkapan dan ketepatan dari riwayat hidup pemohon;

3) Konfirmasi kualifikasi akademik dan profesional yang diklaim;
4) Pemeriksaan identitas (KTP, paspor atau dokumen sejenis); dan
5) Pemeriksaan lebih rinci, seperti pemeriksaan catatan kriminal.

5.5 Standar Pengendalian Keamanan Fisik dan Lingkungan

5.5.1 Pengamanan Perangkat

1) Penempatan dan perlindungan perangkat

Penempatan dan perlindungan perangkat harus mencakup:

a. Perangkat harus diletakkan pada lokasi yang meminimalkan akses yang tidak perlu ke dalam area kerja;

b. Perangkat pengolah informasi yang menangani informasi sensitif harus diposisikan dan dibatasi arah sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak yang tidak berwenang selama digunakan, dan perangkat penyimpanan diamankan untuk menghindari akses oleh pihak yang tidak berwenang;

c. Perangkat yang memerlukan perlindungan khusus seperti perangkat cetak khusus, perangkat jaringan di luar ruang server harus terisolasi;

d. Langkah-langkah pengendalian dilakukan untuk meminimalkan risiko potensi ancaman fisik, seperti pencurian, api, bahan peledak, asap, air termasuk kegagalan penyediaan air, debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetis, dan perusakan;

e. Kondisi lingkungan, seperti suhu dan kelembaban harus dimonitor untuk mencegah perubahan kondisi yang dapat mempengaruhi pengoperasian perangkat pengolah informasi;

f. Perlindungan petir harus diterapkan untuk semua bangunan dan filter perlindungan petir harus dipasang untuk semua jalur komunikasi dan listrik; dan

g. Perangkat pengolah informasi sensitif harus dilindungi untuk meminimalkan risiko kebocoran informasi.

2) Penyediaan perangkat pendukung

Perangkat pendukung harus dipasang untuk menjamin beroperasinya perangkat pengolah informasi dan secara berkala harus diperiksa dan diuji ulang kinerjanya.

3) Pengamanan kabel

Perlindungan keamanan kabel mencakup:

a. Pemasangan kabel sumber daya listrik dan kabel telekomunikasi ke perangkat pengolah informasi selama memungkinkan harus terletak di bawah tanah, atau menerapkan alternatif perlindungan lain yang memadai;

b. Pemasangan kabel jaringan harus dilindungi dari penyusupan yang tidak sah atau kerusakan, misalnya dengan menggunakan *conduit* atau menghindari rute melalui area publik;

c. Pemisahan antara kabel sumber daya listrik dengan kabel telekomunikasi untuk mencegah interferensi;

d. Penandaan/penamaan *kabel* dan perangkat harus diterapkan secara jelas untuk memudahkan penanganan kesalahan;

e. Penggunaan dokumentasi daftar *panel patch* diperlukan untuk mengurangi kesalahan; dan

f. Pengendalian untuk sistem informasi yang sensitif harus mempertimbangkan:

- Penggunaan *conduit*;

- Penggunaan ruangan terkunci pada tempat inspeksi dan titik pemutusan kabel;

- Penggunaan rute alternatif dan/atau media transmisi yang menyediakan keamanan yang sesuai;

- Penggunaan kabel fiber optik;

- Penggunaan lapisan elektromagnet untuk melindungi kabel;

- Inisiasi penghapusan teknikal (*technical sweeps*) dan pemeriksaan secara fisik untuk peralatan yang tidak diotorisasi saat akan disambungkan ke kabel; dan

- Penerapan akses kontrol ke *panel patch* dan ruangan kabel.

4) Pemeliharaan perangkat

a. Perangkat harus dipelihara secara berkala untuk menjamin ketersediaan, keutuhannya (*integrity*), dan fungsinya.

b. Perangkat harus dipelihara sesuai dengan petunjuk manualnya. Untuk pemeliharaan yang dilakukan oleh pihak ketiga, harus diadakan Perjanjian Tingkat Layanan (*Service Level Agreement/ SLA*) yang mendefinisikan tingkat pemeliharaan yang disediakan dan tingkat kinerja yang harus dipenuhi pihak ketiga.

c. Pemeliharaan terhadap perangkat keras atau piranti lunak dilakukan hanya oleh pegawai yang berwenang.

d. Dalam hal pemeliharaan perangkat tidak dapat dilakukan di tempat, maka pemindahan perangkat harus mendapatkan persetujuan Pejabat yang berwenang, dan terhadap data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA yang disimpan dalam perangkat tersebut harus dipindahkan terlebih dahulu.

e. Otorisasi penggunaan perangkat harus dilakukan secara tertulis dan data-data yang terkait dengan aset informasi yang digunakan, seperti nama pemakai aset, lokasi, dan tujuan penggunaan aset, harus dicatat dan disimpan.

5) Pengamanan perangkat di luar Kementerian.

Penggunaan perangkat yang dibawa ke luar dari Kementerian harus disetujui oleh Pejabat yang berwenang.

6) Pengamanan penggunaan kembali atau penghapusan/ pemusnahan perangkat.

Perangkat pengolah informasi penyimpan data yang sudah tidak digunakan harus disanitasi (*sanitized*) sebelum digunakan kembali atau dihapuskan/dimusnahkan.

5.5.2 Pengamanan Area

1) Seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan Kementerian harus mematuhi aturan yang berlaku di Kementerian.
2) Pusdatin dan Unit Organisasi menyimpan perangkat pengolah informasi di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain pintu elektronik, sistem pemadam kebakaran, alarm bahaya, dan perangkat pemutus aliran listrik;
3) Akses ke ruang server, *data center*, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dibatasi dan hanya diberikan kepada pegawai yang berwenang;

4) Pihak ketiga yang memasuki ruang server, pusat data (*data center*), dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus didampingi pegawai Pusdatin dan/atau Unit Organisasi sepanjang waktu kunjungan. Waktu masuk dan keluar serta maksud kedatangan harus dicatat dalam buku catatan kunjungan;
5) Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dilindungi secara memadai;
6) Pegawai dan pihak ketiga tidak diizinkan merokok, makan, minum di ruang *server* dan pusat data (*data center*); dan
7) Area keluar masuk barang dan area publik harus selalu dijaga, diawasi dan dikendalikan, dan jika memungkinkan disterilkan dari perangkat pengolah informasi untuk menghindari akses oleh pihak yang tidak berwenang.

5.5.3 Pengamanan Kantor, Ruangan, dan Fasilitas

Pengamanan kantor, ruangan, dan fasilitas mencakup:

1) Pengamanan kantor, ruangan, dan fasilitas harus sesuai dengan peraturan dan standar keamanan dan keselamatan kerja yang berlaku;
2) Fasilitas utama harus ditempatkan khusus untuk menghindari akses publik;
3) Pembatasan pemberian identitas atau tanda-tanda keberadaan aktivitas pengolahan informasi; dan
4) Direktori dan buku telepon internal yang mengidentifikasi lokasi perangkat pengolah informasi tidak mudah diakses oleh publik.

5.5.4 Perlindungan terhadap Ancaman Eksternal dan Lingkungan

Perlindungan terhadap ancaman eksternal dan lingkungan harus mempertimbangkan:

1) Bahan-bahan berbahaya atau mudah terbakar harus disimpan pada jarak yang aman dari area aman (*secure areas*);
2) Perlengkapan umum, seperti alat tulis, tidak boleh disimpan di dalam area aman (*secure areas*);

3) Perangkat *fallback* dan media cadangan (*media backup*) harus diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama; dan
4) Perangkat pemadam kebakaran harus disediakan dan diletakkan di tempat yang tepat dan aman.

5.6 Standar Pengendalian Pengelolaan Komunikasi dan Operasional

5.6.1 Dokumentasi Prosedur Operasional harus mencakup:
1) Tata cara pengolahan dan penanganan informasi;
2) Tata cara menangani kesalahan-kesalahan atau kondisi khusus yang terjadi beserta pihak yang harus dihubungi bila mengalami kesulitan teknis;
3) Cara memfungsikan kembali perangkat dan cara mengembalikan perangkat ke keadaan awal saat terjadi kegagalan sistem;
4) Tata cara pencadangan (*backup*) dan penyimpanan ulang (*restore*); dan
5) Tata cara pengelolaan jejak audit (*audit trails*) pengguna dan catatan kejadian/kegiatan sistem.

5.6.2 Pemisahan Perangkat Pengembangan dan Operasional harus mempertimbangkan:
1) Pengembangan dan operasional piranti lunak harus dioperasikan di sistem atau prosesor komputer dan domain atau direktori yang berbeda;
2) Intruksi Kerja (*working instruction*) rilis dari pengembangan piranti lunak ke operasional harus ditetapkan dan didokumentasikan;
3) Penjalan kode program (*compiler*), penyunting (*editor*), dan alat bantu pengembangan lain tidak boleh diakses dan sistem operasional ketika tidak dibutuhkan;
4) Lingkungan sistem pengujian harus diusahakan sama dengan lingkungan sistem operasional;
5) Pengguna harus menggunakan profil pengguna yang berbeda untuk sistem pengujian dan sistem operasional, serta aplikasi harus menampilkan pesan identifikasi dari sistem untuk mengurangi risiko kesalahan; dan
6) Data yang memiliki klasifikasi SANGAT RAHASIA dan

RAHASIA tidak boleh disalin ke dalam lingkungan pengujian sistem.

5.6.3 Pemantauan dan Pengkajian Layanan Pihak Ketiga Pemantauan dan pengkajian layanan dari pihak ketiga, serta laporan dan catatan dari pihak ketiga mencakup proses sebagai berikut:

1) Pemantauan tingkat kinerja layanan untuk memastikan kesesuaian kepatuhan dengan perjanjian;
2) Pengkajian laporan layanan pihak ketiga dan pengaturan pertemuan berkala dalam rangka pembahasan perkembangan layanan sebagaimana diatur dalam perjanjian kesepakatan;
3) Pemberian informasi tentang gangguan keamanan informasi dan pengkajian informasi ini bersama pihak ketiga sebagaimana diatur dalam perjanjian kesepakatan;
4) Pemeriksaan jejak audit pihak ketiga dan pencatatan peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan; dan
5) Penyelesaian dan pengelolaan masalah yang teridentifikasi.

5.6.4 Pengelolaan Keamanan Jaringan mencakup:

1) Pemantauan kegiatan pengelolaan jaringan untuk menjamin bahwa perangkat jaringan digunakan secara efektif dan efisien;
2) Pengendalian dan pengaturan tentang penyambungan atau perluasan jaringan internal atau eksternal Kementerian;
3) Pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal Kementerian;
4) Pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan Kementerian dan menerapkan pemantauan serta pencatatan kegiatan selama menggunakan jaringan.
5) Pemutusan layanan tanpa pemberitahuan sebelumnya jika terjadi gangguan keamanan informasi;
6) Perlindungan jaringan dari akses yang tidak berwenang mencakup:
   a. Penetapan untuk penanggung jawab pengelolaan jaringan dipisahkan dari pengelolaan perangkat pengolah informasi;
   b. Penerapan pengendalian khusus untuk melindungi

keutuhan informasi yang melewati jaringan umum antara lain dengan penggunaan enkripsi dan tanda tangan elektronik *(digital signature);* dan

c. Pendokumentasian arsitektur jaringan seluruh komponen perangkat keras jaringan dan piranti lunak.

7) Penerapan fitur keamanan layanan jaringan mencakup:
   a. Teknologi keamanan seperti autentikasi, enkripsi, dan pengendalian sambungan jaringan;
   b. Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan keamanan dan aturan koneksi jaringan; dan
   c. Prosedur untuk penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.
8) Pertukaran Informasi
   a. Prosedur pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
      - Perlindungan pertukaran informasi dari pencegatan, penyalinan, modifikasi, kesalahan penjaluran (*miss-routing*), dan perusakan;
      - Pendeteksian dan perlindungan terhadap kode berbahaya yang dapat dikirim melalui penggunaan komunikasi elektronik;
      - Perlindungan informasi elektronik dalam bentuk lampiran (*attachment*) yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA;
      - Pertimbangan risiko terkait penggunaan perangkat komunikasi nirkabel;
   b. Pertukaran informasi yang tidak menggunakan perangkat komunikasi elektronik, mengacu pada ketentuan yang berlaku.
   c. Pengendalian pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
      - Pencegahan terhadap penyalahgunaan wewenang pegawai dan pihak ketiga yang dapat membahayakan Organisasi;
      - Penggunaan teknik kriptografi;
      - Penyelenggaraan penyimpanan dan penghapusan/

pemusnahan untuk semua korespondensi kegiatan, termasuk pesan, yang sesuai dengan ketentuan yang berlaku;

- Larangan meninggalkan informasi sensitif pada perangkat pengolah informasi;
- Pembatasan penerusan informasi secara otomatis;
- Pembangunan kepedulian atas ancaman pencurian informasi, misalnya terhadap:
  i. Pengungkapan informasi sensitif untuk menghindari mencuri dengar saat melakukan panggilan telepon;
  ii. Akses pesan di luar kewenangannya;
  iii. Pemrograman mesin faksimili baik sengaja maupun tidak sengaja untuk mengirim pesan ke nomor tertentu; dan
  iv. Pengiriman dokumen dan pesan ke tujuan yang salah.

d. Pembangunan kepedulian atas pendaftaran data demografis, seperti alamat surat elektronik atau informasi pribadi lainnya untuk menghindari pengumpulan informasi yang tidak sah; dan
e. Penyediaan informasi internal Kementerian bagi masyarakat umum harus disetujui oleh pemilik informasi dan sesuai dengan ketentuan yang berlaku.

9) Pemantauan

Prosedur pemantauan penggunaan sistem pengolah informasi ditetapkan untuk menjamin agar kegiatan akses yang tidak sah tidak perIu terjadi. Prosedur ini mencakup pemantauan:

a. Kegagalan akses (*access failures*);
b. Pola-pola masuk (*log-on*) yang mengindikasikan penggunaan yang tidak wajar;
c. Alokasi dan penggunaan hak akses khusus (*privileged access capability*);
d. Penelusuran transaksi dan pengiriman dokumen (*file*) tertentu yang mencurigakan; dan
e. Penggunaan sumber daya sensitif.

5.7 Standar Pengendalian Akses

5.7.1 Persyaratan untuk Pengendalian Akses

Unit Organisasi harus menyusun, mendokumentasikan, dan mengkaji ketentuan akses ke aset informasi berdasarkan kebutuhan organisasi dan persyaratan keamanan. Persyaratan untuk pengendalian akses mencakup:

1) Penentuan kebutuhan keamanan dari pengolah aset informasi; dan
2) Pemisahan peran pengendalian akses, seperti administrasi akses dan otorisasi akses.

5.7.2 Pengelolaan Akses Pengguna

Pusdatin dan Unit Organisasi harus menyusun prosedur pengelolaan hak akses pengguna sesuai dengan peruntukannya. Prosedur pengelolaan akses pengguna harus mencakup:

1) Penggunaan akun yang unik untuk mengaktifkan pengguna agar terhubung dengan sistem informasi atau layanan, dan pengguna dapat bertanggung jawab dalam penggunaan sistem informasi atau layanan tersebut. Penggunaan akun khusus hanya diperbolehkan sebatas yang diperlukan untuk kegiatan atau alasan operasional, dan harus disetujui Pejabat yang berwenang serta didokumentasikan;
2) Pemeriksaan bahwa pengguna memiliki otorisasi dari pemilik sistem untuk menggunakan sistem informasi atau layanan, dan jika diperlukan harus mendapat persetujuan yang terpisah dari Pejabat yang berwenang;
3) Pemeriksaan bahwa tingkat akses yang diberikan sesuai dengan tujuan kegiatan dan konsisten dengan Kebijakan dan Standar Keamanan Informasi di lingkungan Kementerian;
4) Pemberian pernyataan tertulis kepada pengguna tentang hak aksesnya dan meminta pengguna menandatangani pernyataan ketentuan akses tersebut;
5) Pemastian penyedia layanan tidak memberikan akses kepada pengguna sebelum prosedur otorisasi telah selesai;
6) Pemeliharaan catatan pengguna layanan yang terdaftar dalam menggunakan layanan;
7) Penghapusan atau penonaktifan akses pengguna yang telah berubah tugas dan/atau fungsinya, setelah penugasan

berakhir atau mutasi;

8) Pemeriksaan, penghapusan, serta penonaktifan akun secara berkala dan untuk pengguna yang memiliki lebih dari 1 (satu) akun; dan
9) Pemastian bahwa akun tidak digunakan oleh pengguna lain.

5.7.3 Pengelolaan Hak Akses Khusus (*privilege management*)

Pusdatin dan Unit Organisasi harus membatasi dan mengendalikan penggunaan hak akses khusus. Pengelolaan hak akses khusus harus mempertimbangkan:

1) Hak akses khusus setiap sistem dari pabrikan perlu diidentifikasi untuk dialokasikan/diberikan kepada pengguna yang terkait dengan produk, seperti sistem operasi, sistem pengelolaan basis data, aplikasi;
2) Hak akses khusus hanya diberikan kepada pengguna sesuai dengan peruntukkannya berdasarkan kebutuhan dan kegiatan tertentu;
3) Pengelolaan proses otorisasi dan catatan dari seluruh hak akses khusus yang dialokasikan/diberikan kepada pengguna. Hak akses khusus tidak boleh diberikan sebelum proses otorisasi selesai;
4) Pengembangan dan penggunaan sistem rutin (misal *job scheduling*) harus diutamakan untuk menghindari kebutuhan dalam memberikan hak akses khusus secara terus menerus kepada pengguna;
5) Hak akses khusus harus diberikan secara terpisah dari akun yang digunakan untuk kegiatan umum, seperti akun administrator sistem (*system administrator*), administrator basis data (*database administrator*), dan administrator jaringan (*network administrator*).

5.7.4 Kajian Hak Akses Pengguna

Kajian hak akses pengguna harus mempertimbangkan:

1) Hak akses pengguna harus dikaji paling sedikit 6 (enam) bulan sekali atau setelah terjadi perubahan pada sistem, atau struktur Organisasi;
2) Hak akses khusus harus dikaji paling sedikit 6 (enam) bulan sekali dalam jangka waktu lebih sering dibanding jangka waktu pengkajian hak akses pengguna, atau apabila terjadi

perubahan pada sistem, atau struktur Organisasi;

3) Pemeriksaan hak akses khusus harus dilakukan secara berkala, untuk memastikan pemberian hak akses khusus telah diotorisasi.

5.7.5 Pengendalian Akses Jaringan

1) Menerapkan prosedur otorisasi untuk pemberian akses ke jaringan dan layanan jaringan;
2) Menerapkan teknik autentikasi akses dari koneksi eksternal, seperti teknik kriptografi; dan
3) Melakukan penghentian isolasi layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.

5.7.6 Pemisahan dalam Jaringan

Melakukan pemisahan dalam jaringan antara lain:

1) Pemisahan berdasarkan kelompok layanan informasi, pengguna, dan aplikasi; dan
2) Pemberian akses jaringan kepada tamu, hanya dapat diberikan akses terbatas misalnya internet dan/atau surat elektronik tanpa bisa terhubung ke jaringan internal Kementerian.

5.7.7 Perangkat Kerja Bergerak dan Jarak Jauh *(Mobile Computing dan Teleworking)*

1) Penggunaan perangkat kerja bergerak dan jarak jauh *(mobile computing dan teleworking)* harus mempertimbangkan:
   a. Memenuhi keamanan informasi dalam penentuan lokasi;
   b. Menjaga keamanan akses;
   c. Menggunakan anti kode berbahaya (*malicious code*);
   d. Memakai piranti lunak berlisensi; dan
   e. Mendapat persetujuan Pejabat yang berwenang/ atasan langsung pegawai.
2) Pencabutan hak akses dan pengembalian fasilitas perangkat jarak jauh (*teleworking*) apabila kegiatan telah selesai.

5.8 Standar Pengendalian Keamanan Informasi dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi

5.8.1 Spesifikasi kebutuhan perangkat pengolah informasi yang dikembangkan baik oleh internal atau pihak ketiga harus didokumentasikan secara formal.

5.8.2 Pengolahan Data pada Aplikasi

1) Pemeriksaan data masukan harus mempertimbangkan:
   a. Penerapan masukan rangkap (*dual input*) atau mekanisme pengecekan masukan Iainnya untuk mendeteksi kesalahan sebagai berikut:
      - Diluar rentang/batas nilai-nilai yang diperbolehkan;
      - Karakter tidak valid dalam *field* data;
      - Data hilang atau tidak lengkap;
      - Melebihi batas atas dan bawah volume data; dan
      - Data yang tidak diotorisasi dan tidak konsisten.
   b. Pengkajian secara berkala terhadap isi *field* kunci (*key field*) atau dokumen (*file*) data untuk mengkonfirmasi keabsahan dan integritas data;
   c. Memeriksa dokumen cetak (*hard copy*) untuk memastikan tidak adanya perubahan data masukan yang tidak melalui otorisasi;
   d. Menampilkan pesan yang sesuai dalam menanggapi kesalahan validasi;
   e. Prosedur untuk menguji kewajaran dari data masukan;
   f. Menguraikan tanggung jawab dari seIuruh pegawai yang terkait dalam proses perekaman data; dan
   g. Sistem mampu membuat dan mengeluarkan catatan aktivitas terkait proses perekaman data.
2) Menyusun daftar pemeriksaan (*check list*) yang sesuai, mendokumentasikan proses pemeriksaan, dan menyimpan hasilnya secara aman. Proses pemeriksaan mencakup:
   a. Pengendalian sesi (*session*) atau tumpak (*batch*), untuk mencocokkan data setelah perubahan transaksi;
   b. Pengendalian saldo (*balancing*) untuk memeriksa data sebelum dan sesudah transaksi;
   c. Validasi data masukan yang dihasilkan sistem;
   d. Keutuhan dan keaslian data yang diunduh/ diunggah (*download/upload*);
   e. *Hash tools* dari rekaman (*record*) dan dokumen (*file*);
   f. Aplikasi berjalan sesuai dengan rencana dan waktu yang ditentukan;
   g. Program dijalankan dalam urutan yang benar dan

menghentikan sementara jika terjadi kegagalan sampai masalah diatasi; dan

h. Sistem mampu membuat dan mengeluarkan catatan aktivitas pengelolaan internal.

3) Pemeriksaan data keluaran harus mempertimbangkan:

a. Kewajaran dari data keluaran yang dihasilkan;

b. Pengendalian rekonsiliasi data untuk memastikan kebenaran pengolahan data;

c. Menyediakan informasi yang cukup untuk pengguna atau sistem pengolahan informasi untuk menentukan akurasi, kelengkapan, ketepatan, dan klasifikasi informasi;

d. Prosedur untuk menindaklanjuti validasi data keluaran;

e. Menguraikan tanggung jawab dari seluruh pegawai yang terkait proses data keluaran; dan

f. Sistem mampu membuat dan mengeluarkan catatan aktivitas dalam proses validasi data keluaran.

5.8.3 Pengendalian dan Penggunaan Kriptografi

Pengembangan dan penerapan sistem kriptografi untuk perlindungan informasi harus mempertimbangkan:

1) Kondisi dari suatu kegiatan yang menentukan bahwa informasi harus dilindungi, seperti risiko kegiatan, media pengiriman informasi, tingkat perlindungan yang dibutuhkan;

2) Tingkat perlindungan yang dibutuhkan harus diidentifikasi berdasarkan penilaian risiko, antara lain jenis, kekuatan, dan kualitas dari algoritma enkripsi yang akan digunakan;

3) Keperluan enkripsi untuk perlindungan informasi SANGAT RAHASIA, RAHASIA, dan TERBATAS yang melalui perangkat bergerak (*mobile computing*), media lepas pasang (*removable media*), atau jalur komunikasi;

4) Pengelolaan kunci kriptografi (*kriptografi key*), seperti perlindungan kunci kriptografi (*kriptografi key*), pemulihan informasi ter-enkripsi dalam hal kehilangan atau kerusakan kunci kriptografi (*kriptografi key*); dan

5) Dampak penggunaan informasi ter-enkripsi, seperti pengendalian terkait pemeriksaan suatu konten, kecepatan pemrosesan pada sistem.

5.8.4 Keamanan Dokumen (*File*) Sistem

1) Pengembangan prosedur pengendalian piranti lunak pada sistem operasional harus mempertimbangkan:
   a. Proses pemutakhiran piranti lunak operasional, aplikasi, kumpulan program (*library program*) hanya boleh dilakukan oleh administrator sistem terlatih setelah melalui proses otorisasi;
   b. Sistem operasional hanya berisi program aplikasi yang dapat dieksekusi (*executable*) yang telah diotorisasi, tidak boleh berisi kode program (*source code*) atau penjalan kode program (*compiler*);
   c. Aplikasi dan piranti lunak sistem operasi hanya dapat diimplementasikan setelah melewati proses pengujian yang ekstensif;
   d. Sistem pengendalian konfigurasi harus digunakan untuk mengendalikan seluruh piranti lunak yang telah diimplementasikan beserta dokumentasi sistem;
   e. Strategi *rollback* harus tersedia sebelum suatu perubahan diimplementasikan;
   f. Catatan audit harus dipelihara untuk menjaga kemutakhiran catatan (*library*) program operasional;
   g. Versi terdahulu dari suatu aplikasi harus tetap disimpan untuk keperluan kontinjensi; dan
   h. Versi lama dari suatu piranti lunak harus diarsip, bersama dengan informasi terkait dan prosedur, parameter, konfigurasi rinci, dan piranti lunak pendukung.
2) Perlindungan terhadap sistem pengujian data harus mempertimbangkan:
   a. Prosedur pengendalian akses, yang berlaku pada sistem aplikasi operasional, harus berlaku juga pada sistem aplikasi pengujian;
   b. Proses otorisasi setiap kali informasi/data operasional digunakan pada sistem pengujian;
   c. Penghapusan informasi/data operasional yang digunakan pada sistem pengujian segera setelah proses pengujian selesai; dan

d. Pencatatan jejak audit penggunaan informasi/data operasional.

3) Pengendalian akses ke kode program (*source code*) harus mempertimbangkan:
   a. Kode program (*source code*) tidak boleh disimpan pada sistem operasional;
   b. Pengelolaan kode program (*source code*) dan catatan (*library*) harus mengikuti prosedur yang telah ditetapkan;
   c. Pengelola TIK tidak boleh memiliki akses yang tidak terbatas ke kode program (*source code*) dan catatan (*library*);
   d. Proses pemutakhiran kode program (*source code*) dan item terkait, serta pemberian kode program (*source code*) kepada *programmer* hanya dapat dilakukan setelah melalui proses otorisasi;
   e. Daftar (*listing*) program harus disimpan dalam area aman (*secure areas*);
   f. Catatan audit dari seluruh akses ke kode program (*source code*) *library* harus dipelihara; dan
   g. Pemeliharaan dan penyalinan kode program (*source code*) *library* harus mengikuti prosedur pengendalian perubahan.

5.8.5 Keamanan dalam proses pengembangan dan pendukung (*support proceses*)

1) Prosedur pengendalian perubahan sistem operasi dan piranti lunak, mencakup:
   a. Memelihara catatan persetujuan sesuai dengan kewenangannya;
   b. Memastikan permintaan perubahan diajukan oleh pihak yang berwenang;
   c. Melakukan kaji ulang *(review)* untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;
   d. Melakukan identifikasi terhadap piranti lunak, informasi, basis data, dan perangkat keras yang perlu

diubah;

e. Mendapatkan persetujuan formal dari pihak yang berwenang sebelum pelaksanaan perubahan;
f. Memastikan pihak yang berwenang menerima perubahan yang diminta sebelum dilakukan implementasi;
g. Memastikan bahwa dokumentasi sistem mutakhir dan dokumen versi sebelumnya diarsip;
h. Memelihara versi perubahan aplikasi;
i. Memelihara jejak audit perubahan aplikasi;
j. Memastikan dokumentasi penggunaan dan prosedur telah diubah sesuai dengan perubahan yang dilaksanakan; dan
k. Memastikan bahwa implementasi perubahan dilakukan pada waktu yang tepat dan tidak menganggu kegiatan.

2) Prosedur kajian teknis aplikasi setelah perubahan sistem operasi dan/atau piranti lunak, mencakup:
   a. Melakukan kaji ulang untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;
   b. Memastikan rencana dan anggaran yang mencakup kaji ulang dan pengujian sistem dari perubahan sistem operasi;
   c. Memastikan pemberitahuan perubahan sistem informasi dilakukan dalam jangka waktu yang tepat untuk memastikan tes dan kaji ulang telah dilaksanakan sebelum implementasi; dan
   d. Memastikan bahwa perubahan telah diselaraskan dengan rencana kelangsungan kegiatan.
3) Kebocoran informasi

   Pengendalian yang dapat diterapkan untuk membatasi risiko kebocoran informasi, antara lain:
   a. Melakukan pemantauan terhadap sistem dan aktivitas pegawai dan pihak ketiga, sesuai dengan ketentuan yang berlaku; dan
   b. Melakukan pemantauan terhadap aktivitas penggunaan komputer personal (*desktop*) dan perangkat bergerak

(*mobile*).

4) Pengembangan piranti lunak oleh pihak ketiga harus mempertimbangkan:
   a. Perjanjian lisensi, kepemilikan kode program (*source code*), dan Hak Atas Kekayaan Intelektual (HAKI);
   b. Perjanjian *escrow*;
   c. Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan;
   d. Persyaratan kontrak mengenai kualitas dan fungsi keamanan aplikasi;
   e. Uji coba terhadap aplikasi untuk memastikan tidak terdapat kode berbahaya (*malicious code*) sebelum implementasi.
5) Pengelolaan Kerentanan Teknis, mencakup:
   a. Penunjukan fungsi dan tanggung jawab yang terkait dengan pengelolaan kerentanan teknis termasuk di dalamnya pemantauan kerentanan, penilaian risiko kerentanan, *patching*, registrasi aset, dan koordinasi dengan pihak terkait;
   b. Pengidentifikasian sumber informasi yang dapat digunakan untuk meningkatkan kepedulian terhadap kerentanan teknis;
   c. Penentuan rentang waktu untuk melakukan aksi terhadap munculnya potensi kerentanan teknis. Apabila terjadi kerentanan teknis yang butuh penanganan maka harus diambil tindakan sesuai kontrol yang telah ditetapkan atau melaporkan kejadian tersebut melalui pelaporan kejadian dan kelemahan keamanan informasi;
   d. Pengujian dan evaluasi penggunaan *patch* sebelum proses instalasi untuk memastikan *patch* dapat bekerja secara efektif dan tidak menimbulkan risiko yang lain. Apabila *patch* tidak tersedia, harus melakukan hal sebagai berikut:
      - Mematikan layanan (*services*) yang berhubungan dengan kerentanan;
      - Menambahkan pengendalian akses seperti *firewall;*

- Meningkatkan pengawasan untuk mengidentifikasi atau mencegah terjadinya serangan atau kejadian;
- Meningkatkan kepedulian terhadap kerentanan teknis;

e. Penyimpanan catatan audit (*audit log*) yang memuat prosedur dan langkah-langkah yang telah diambil;
f. Pemantauan dan evaluasi terhadap pengelolaan kerentanan teknis harus dilakukan secara berkala; dan
g. Pengelolaan kerentanan teknis diutamakan terhadap sistem informasi yang memiliki tingkat risiko tinggi.

5.9 Standar Pengendalian Pengelolaan Gangguan Keamanan Informasi

5.9.1 Pelaporan Kejadian dan Kelemahan Keamanan Informasi

1) Gangguan keamanan informasi antara lain:
   a. Hilangnya layanan, perangkat, atau fasilitas TIK;
   b. Kerusakan fungsi sistem atau kelebihan beban;
   c. Perubahan sistem di luar kendali;
   d. Kerusakan fungsi piranti lunak atau perangkat keras;
   e. Pelanggaran akses ke dalam sistem pengolah informasi TIK;
   f. Kelalaian manusia; dan
   g. Ketidaksesuaian dengan ketentuan yang berlaku.
2) Pegawai dan pihak ketiga harus melaporkan kepada Pusdatin dan Unit Organisasi sesegera mungkin pada saat menemui kelemahan atau terjadi gangguan keamanan informasi dalam sistem atau layanan TIK Kementerian.
3) Pelaporan gangguan harus mencakup:
   a. Proses umpan balik yang sesuai untuk memastikan bahwa pihak yang melaporkan kejadian keamanan informasi mendapatkan pemberitahuan penanganan masalah;
   b. Formulir laporan gangguan keamanan informasi untuk mendukung tindakan pelaporan dan membantu pelapor mengingat kronologis kejadian keamanan informasi;
   c. Perilaku yang benar dalam menghadapi gangguan keamanan informasi, antara lain:
      - Mencatat semua rincian penting gangguan dengan segera, seperti jenis pelanggaran, jenis kerusakan,

pesan pada layar, atau anomali sistem; dan

- Segera melaporkan gangguan ke pihak berwenang sebelum melakukan tindakan penanganan sendiri.

4) Sebagai referensi yang digunakan dalam proses penanganan pelanggaran disiplin bagi pegawai dan pihak ketiga yang melakukan pelanggaran keamanan informasi.

5.9.2 Pengelolaan Gangguan Keamanan Informasi dan Perbaikannya

1) Pusdatin dan Unit Organisasi masing-masing harus menyusun prosedur dan menguraikan tanggung jawab pegawai, terkait dalam rangka memastikan gangguan keamanan informasi dapat ditangani secara cepat dan efektif.
2) Prosedur pengelolaan gangguan keamanan informasi harus mempertimbangkan:
   a. Prosedur yang harus ditetapkan untuk menangani berbagai jenis gangguan keamanan informasi, antara lain:
      - Kegagalan sistem informasi dan hilangnya layanan;
      - Serangan program yang membahayakan (*malicious code*);
      - Serangan *denial of service*;
      - Kesalahan akibat data tidak lengkap atau tidak akurat;
      - Pelanggaran kerahasiaan dan keutuhan; dan
      - Penyalahgunaan sistem informasi.
   b. Untuk melengkapi rencana kontijensi, prosedur harus mencakup:
      - Analisis dan identifikasi penyebab gangguan;
      - Mengkarantina atau membatasi gangguan;
      - Perencanaan dan pelaksanaan tindakan korektif untuk mencegah gangguan berulang;
      - Komunikasi dengan pihak-pihak yang terkena dampak pemulihan gangguan; dan
      - Pelaporan tindakan ke pihak berwenang.
   c. Jejak audit dan bukti serupa harus dikumpulkan dan diamankan untuk:
      - Analisis masalah internal;
      - Digunakan sebagai bukti forensik yang berkaitan dengan potensi pelanggaran kontrak atau peraturan

atau persyaratan dalam hal proses pidana atau perdata; dan

- Digunakan sebagai bahan tuntutan ganti rugi pada pihak ketiga yang menyediakan piranti lunak dan layanan.

d. Tindakan untuk memulihkan keamanan dari pelanggaran dan perbaikan kegagalan sistem harus dikendalikan secara hati-hati dan formal, prosedur harus memastikan bahwa:

- Hanya pegawai yang sudah diidentifikasi dan berwenang yang diizinkan akses langsung ke sistem dan data;
- Semua tindakan darurat yang diambil, didokumentasikan secara rinci;
- Tindakan darurat dilaporkan kepada pihak berwenang; dan
- Keutuhan sistem dan pengendaliannya dikonfirmasikan dengan pihak-pihak terkait sesegera mungkin.

3) Peningkatan penanganan gangguan keamanan informasi

a. Seluruh gangguan keamanan informasi yang terjadi dan tindakan mengatasinya harus dicatat dalam suatu basis data dan/atau buku catatan pelaporan gangguan keamanan informasi, dan akan menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi.

b. Seluruh catatan gangguan keamanan informasi akan dievaluasi dan dianalisis untuk perbaikan dan pencegahan agar gangguan keamanan informasi tidak terulang.

4) Pengumpulan bukti pelanggaran

Pusdatin dan Unit Organisasi harus mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap Kebijakan dan Standar Keamanan Informasi di Kementerian.

5.10 Standar Pengendalian Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan

5.10.1 Unit Organisasi harus mengelola proses kelangsungan kegiatan pada saat keadaan darurat di Unit Organisasi

masing-masing.

5.10.2 Unit Organisasi harus mengidentifikasi risiko, dan menganalisis dampak yang diakibatkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan.

5.10.3 Unit Organisasi harus menyusun dan menerapkan Rencana Kelangsungan Kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan.

5.10.4 Unit Organisasi harus memelihara dan memastikan rencana-rencana yang termuat dalam Rencana Kelangsungan Kegiatan masih sesuai, dan mengidentifikasi prioritas untuk kegiatan uji coba.

5.10.5 Unit Organisasi harus melakukan uji coba Rencana Kelangsungan Kegiatan secara berkala untuk memastikan Rencana Kelangsungan Kegiatan dapat dilaksanakan secara efektif.

5.10.6 Pengelolaan Kelangsungan Kegiatan pada saat Keadaan Darurat

Komponen yang harus diperhatikan dalam mengelola proses kelangsungan kegiatan:

1) Identifikasi risiko dan analisis dampak yang diakibatkan pada saat terjadi keadaan darurat;
2) Identifikasi seluruh aset informasi yang menunjang proses kegiatan kritikal;
3) Identifikasi sumber daya, mencakup biaya, struktur Organisasi, teknis pelaksanaan, pegawai dan pihak ketiga;
4) Memastikan keselamatan pegawai, dan perlindungan terhadap perangkat pengolah informasi dan aset Organisasi;
5) Penyusunan dan pendokumentasian Rencana Kelangsungan Kegiatan sesuai dengan Rencana Strategi (Renstra) Kementerian; dan
6) Pelaksanaan uji coba dan pemeliharaan Rencana Kelangsungan Kegiatan secara berkala.

5.10.7 Proses identifikasi risiko mengikuti ketentuan mengenai

Penerapan Manajemen Risiko di Kementerian.

5.10.8 Proses analisis dampak kegiatan harus melibatkan pemilik proses bisnis dan dievaluasi secara berkala.

5.10.9 Penyusunan Rencana Kelangsungan Kegiatan mencakup:

1) Prosedur saat keadaan darurat, mencakup tindakan yang harus dilakukan serta pengaturan hubungan dengan pihak berwenang;
2) Prosedur *fallback*, mencakup tindakan yang harus diambil untuk memindahkan kegiatan kritikal atau layanan pendukung ke lokasi kerja sementara, dan mengembalikan operasional kegiatan kritikal dalam jangka waktu sesuai dengan standar ketersediaan data yang ditetapkan;
3) Prosedur saat kondisi telah normal (*resumption*), adalah tindakan mengembalikan kegiatan operasional ke kondisi normal;
4) Jadwal uji coba, mencakup langkah-langkah, dan waktu pelaksanaan uji coba serta proses pemeliharaannya;
5) Pelaksanaan pelatihan dan sosialisasi dalam rangka meningkatkan kepedulian dan pemahaman proses kelangsungan kegiatan dan memastikan proses kelangsungan kegiatan dilaksanakan secara efektif;
6) Tanggung jawab dan peran setiap Petugas Pelaksana Pengelolaan Proses Kelangsungan;
7) Daftar kebutuhan aset informasi kritikal dan sumber daya untuk dapat menjalankan prosedur saat keadaan darurat, *fallback,* dan saat kondisi telah normal (*resumption*).

5.10.10 Uji Coba Rencana Kelangsungan Kegiatan harus dilaksanakan untuk memastikan setiap rencana yang disusun dapat dilakukan/dipenuhi pada saat penerapannya.

Kegiatan uji coba Rencana Kelangsungan Kegiatan ini mencakup:

1) Simulasi terutama untuk Petugas Pelaksana Pengelolaan Proses Kelangsungan Kegiatan;

2) Uji coba pemulihan (*recovery*) sistem informasi untuk memastikan sistem informasi dapat berfungsi kembali;
3) Uji coba proses pemulihan (*recovery*) di lokasi kerja sementara untuk menjalankan proses bisnis secara paralel;
4) Uji coba terhadap perangkat dan layanan yang disediakan oleh pihak ketiga; dan
5) Uji coba keseluruhan mulai dari Organisasi, petugas, peralatan, perangkat, dan prosesnya.

5.11 Standar Pengendalian Kepatuhan

5.11.1 Kepatuhan terhadap Peraturan Perundangan yang terkait Keamanan Informasi

1) Seluruh pegawai dan pihak ketiga harus menaati peraturan perundangan yang terkait dengan keamanan informasi.
2) Pusdatin dan Unit Organisasi harus mengidentifikasi, mendokumentasikan, dan memelihara kemutakhiran semua peraturan perundangan yang terkait dengan sistem keamanan informasi.
3) Hak Atas Kekayaan Intelektual

   Piranti lunak yang dikelola Pusdatin dan Unit Organisasi harus mematuhi ketentuan penggunaan lisensi. Penggandaan piranti lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran.
4) Perlindungan terhadap rekaman

   Rekaman milik Kementerian harus dilindungi dari kehilangan, kerusakan atau penyalahgunaan.
5) Pengamanan data

   Pusdatin dan Unit Organisasi melindungi kepemilikan dan kerahasiaan data. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundangan dan kesepakatan.

5.11.2 Kepatuhan Teknis

Pusdatin dan Unit Organisasi harus melakukan pemeriksaan kepatuhan teknis secara berkala untuk menjamin efektivitas standar dan prosedur keamanan informasi yang ada di area operasional.

5.11.3 Audit Sistem Informasi

1) Pengendalian audit sistem informasi

   Pusdatin dan Unit Organisasi bersama dengan Inspektorat Jenderal harus membuat perencanaan persyaratan, ruang lingkup, dan kegiatan audit yang melibatkan pemeriksaan sistem operasional untuk mengurangi kemungkinan risiko gangguan yang bisa terjadi terhadap kegiatan Kementerian selama proses audit.

2) Perlindungan terhadap alat bantu (*tools*) audit sistem informasi

   Penggunaan alat bantu (baik piranti lunak maupun perangkat keras) untuk mengetahui kelemahan keamanan, memindai (*scanning*) kata sandi, atau untuk melemahkan dan menerobos sistem keamanan inforrnasi tidak diizinkan kecuali atas persetujuan Pimpinan Pusdatin dan Unit Organisasi.

3) Proses audit sistem informasi harus memperhatikan hal berikut:

   a. Persyaratan audit harus disetujui oleh Pimpinan Unit Organisasi;
   b. Ruang lingkup pemeriksaan/audit harus disetujui dan dikendalikan oleh pihak berwenang;
   c. Pemeriksaan piranti lunak dan data harus dibatasi untuk akses baca saja (*read-only*);
   d. Selain akses baca saja hanya diizinkan untuk salinan dari dokumen (*file*) sistem yang diisolasi, yang harus dihapus bila audit telah selesai, atau diberikan perlindungan yang tepat jika ada kewajiban untuk menyimpan dokumen (*file*) tersebut di bawah persyaratan dokumentasi audit;
   e. Sumber daya untuk melakukan pemeriksaan harus secara jelas diidentifikasi dan tersedia;
   f. Persyaratan untuk pengolahan khusus atau tambahan harus diidentifikasi dan disepakati;
   g. Semua akses harus dipantau dan dicatat untuk menghasilkan jejak audit, dan untuk data dan sistem informasi sensitif harus mempertimbangkan pencatatan waktu (*timestamp*) pada jejak audit;

h. Semua prosedur, persyaratan, dan tanggung jawab harus didokumentasikan; dan
i. Auditor harus independen dari kegiatan yang diaudit.

5.11.4 Kepatuhan terhadap Hak Kekayaan Intelektual

Hal yang perIu diperhatikan dalam melindungi segala materi yang dapat dianggap kekayaan intelektual meliputi:

1) Mendapatkan piranti lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan hak cipta tidak dilanggar;
2) Memelihara daftar aset informasi sesuai persyaratan untuk melindungi hak kekayaan intelektual;
3) Memelihara bukti kepemilikan lisensi, cakram utama (*master disk*), buku manual, dan lain sebagainya;
4) Menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;
5) Melakukan pemeriksaan bahwa hanya piranti lunak dan produk berlisensi yang dipasang;
6) Patuh terhadap syarat dan kondisi untuk piranti lunak dan informasi yang didapat dari jaringan publik;
7) Dilarang melakukan duplikasi, konversi ke format lain atau mengambil dari rekaman komersial (film atau audio), selain yang diperbolehkan oleh Undang-Undang Hak Cipta; dan
8) Tidak menyalin secara penuh atau sebagian buku, artikel, laporan, atau dokumen lainnya, selain yang diizinkan oleh Undang-Undang Hak Cipta.

5.11.5 Kepatuhan terhadap Kebijakan dan Standar

Hal yang perlu dilakukan jika terdapat ketidakpatuhan teknis meliputi:

1) Menentukan dan mengevaluasi penyebab ketidakpatuhan;
2) Menentukan tindakan yang perlu dilakukan berdasarkan hasil evaluasi agar ketidakpatuhan tidak terulang kembali;
3) Menentukan dan melaksanakan tindakan perbaikan yang sesuai; dan
4) Mengkaji tindakan perbaikan yang dilakukan.

5.11.6 Kepatuhan Teknis

Sistem informasi harus diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan piranti lunak

telah diimplementasikan secara benar. Kepatuhan teknis juga mencakup pengujian penetrasi (*penetrating testing*) untuk mendeteksi kerentanan dalam sistem, dan memeriksa pengendalian akses untuk mencegah kerentanan tersebut telah diterapkan.

6. ISTILAH YANG DIGUNAKAN

6.1 Akun adalah identifikasi pengguna yang diberikan oleh unit Pengelola TIK, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem TIK.

6.2 Akun khusus adalah akun yang diberikan oleh unit Pengelola TIK sesuai kebutuhan tetapi tidak terbatas pada pengelolaan TIK (baik berupa aplikasi atau sistem), dan kelompok kerja (baik berupa acara kedinasan, tim, atau unit kerja).

6.3 Aset fisik adalah jenis aset yang memiliki wujud fisik, misalnya perangkat komputer, perangkat jaringan dan komunikasi, media lepas pasang (*removable media*), dan perangkat pendukung lainnya.

6.4 Aset tak berwujud adalah jenis aset yang tidak memiliki wujud fisik, misalnya pengetahuan, pengalaman, keahlian, citra, dan reputasi. Aset ini mempunyai umur lebih dari satu tahun (aset tidak lancar) dan dapat diamortisasi selama periode pemanfaatannya, yang biasanya tidak lebih dari empat puluh tahun.

6.5 *Conduit* adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.

6.6 Data adalah catatan atas kumpulan fakta yang mempunyai arti baik secara kualitatif maupun kuantitatif.

6.7 *Denial of service* adalah suatu kondisi di mana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang tidak terkendali baik dari dalam maupun dari luar sistem.

6.8 Direktori adalah hirarki atau *tree structure.*

6.9 Informasi adalah hasil pemrosesan, manipulasi, dan pengOrganisasian data yang dapat disajikan sebagai pengetahuan.
Catatan: dalam penggunaannya, data dapat berupa informasi yang menjadi data baru, sebaliknya informasi dapat berfungsi sebagai data untuk menghasilkan informasi baru.

6.10 *Fallback* adalah suatu tindakan pembalikan/menarik diri dari posisi awal.

6.11 Fasilitas adalah sarana untuk melancarkan pelaksanaan fungsi atau mempermudah sesuatu.

6.12 Fasilitas utama adalah sarana utama gedung atau bangunan, seperti pusat control listrik, CCTV.

6.13 Hak akses khusus adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan (*storage devices*), dokumen pada *server* (*file server*), dan aplikasi-aplikasi sensitif, hanya diberikan kepada pengguna yang membutuhkan dan pemakaiannya terbatas dan dikontrol.

6.14 *Hash totals* adalah nilai pemeriksa kesalahan yang diturunkan dari penambahan satu himpunan bilangan yang diambil dari data (tidak harus berupa data numerik) yang diproses atau dimanipulasi dengan cara tertentu.

6.15 Jejak audit (*audit trails*) adalah urutan kronologis catatan audit yang berkaitan dengan pelaksanaan suatu kegiatan.

6.16 Kata sandi adalah serangkaian kode yang dibuat pengguna, bersifat rahasia dan pribadi yang digunakan bersamaan dengan Akun Pengguna.

6.17 Keamanan informasi adalah perlindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.

6.18 Koneksi eksternal (*remote access*) adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.

6.19 Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan keamanan informasi. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi.

6.20 Kode berbahaya (*malicious code*) adalah semua macam program yang membahayakan termasuk makro atau *script* yang dapat diesekusi dan dibuat dengan tujuan untuk merusak sistem komputer.

6.21 Cakram utama (*master disk*) adalah media yang digunakan

sebagai sumber dalam melakukan instalasi piranti lunak.

6.22 Perangkat bergerak (*mobile computing*) adalah penggunaan perangkat komputasi yang dapat dipindah (*portabel*) misalnya komputer jinjing (*notebook*) dan telepon selular untuk melakukan akses, pengolahan data dan penyimpanan.

6.23 Pemilik aset informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi.

6.24 Perangkat jaringan adalah peralatan jaringan komunikasi data seperti *modem, hub, switch, router,* dan lain-lain.

6.25 Piranti lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.

6.26 Perangkat pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras dan perangkat jaringan serta untuk melindunginya dari kerusakan. Contoh perangkat pendukung adalah *Uninterruptible Power Supply (UPS)*, pembangkit tenaga listrik/generator, antena komunikasi.

6.27 Perangkat pengolah informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur. Contoh perangkat pengolah informasi adalah komputer, faksimili, telepon, mesin *fotocopy.*

6.28 Perjanjian *escrow* adalah perjanjian dengan pihak ketiga atau pembuat aplikasi untuk memastikan apabila pihak ketiga tersebut tidak beroperasi/bangkrut (mengalami *failure)* maka Kementerian berhak untuk mendapatkan kode program *(source code).*

6.29 Perjanjian kerahasiaan adalah perikatan antara para pihak yang mencantumkan bahan rahasia, pengetahuan, atau informasi yang mana pihak-pihak ingin berbagi satu sama lain untuk tujuan tertentu, tetapi ingin membatasi akses dengan pihak lain.

6.30 Pihak berwenang adalah pihak yang mempunyai kewenangan terkait suatu hal, seperti kepolisian, instansi pemadam kebakaran, dan penyedia jasa telekomunikasi/internet.

6.31 Pihak ketiga adalah semua unsur di Iuar pengguna unit TIK Kementerian yang bukan bagian dari Kementerian, misal mitra kerja Kementerian (seperti: konsultan, penyedia jasa komunikasi, pemasok dan pemelihara perangkat pengolah informasi), dan kementerian/lembaga lain.

6.32 Proses pendukung (*support processes*) adalah proses-proses penunjang yang mendukung suatu proses utama yang terkait. Contoh proses

pendukung dalam pengembangan (*development*) adalah proses pengujian piranti lunak, proses perubahan piranti lunak.

6.33 Rencana Kontijensi adalah suatu rencana ke depan pada keadaan yang tidak menentu dengan skenario, tujuan, teknik, manajemen, pelaksanaan, serta sistem penanggulangannya telah ditentukan secara bersama untuk mencegah dan mengatasi keadaan darurat.

6.34 *Rollback* adalah sebuah mekanisme yang digunakan untuk mengembalikan sistem ke kondisi semula sebelum perubahan diimplementasikan. Mekanisme ini biasanya terdapat pada sistem basis data.

6.35 *Routing* adalah sebuah mekanisme yang digunakan untuk mengarahkan dan menentukan rute/jalur yang akan dilewati paket dari satu perangkat ke perangkat yang berada di jaringan lain.

6.36 Sanitasi adalah proses penghilangan informasi yang disimpan secara permanen dengan menggunakan medan magnet besar atau perusakan fisik.

6.37 Manajemen Keamanan Informasi adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penangung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.

6.38 Sanitasi (*sanitized*) adalah proses pembersihan data dan informasi sehingga tidak ada ada data dan informasi yang dapat diambil kembali dari perangkat keras tersebut.

6.39 Sistem informasi adalah serangkaian perangkat keras, piranti lunak, sumber daya manusia, serta prosedur dan/atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi inforrnasi yang berguna untuk rnencapai suatu tujuan.

6.40 Sistem TIK adalah sistem operasi, sistem surat elektronik, sistem aplikasi, sistem basis data, sistem jaringan intranet/internet, dan sebagainya.

6.41 Administrator sistem (*system administrator*) adalah akun khusus untuk mengelola sistem informasi.

6.42 Perangkat jarak jauh (*teleworking*) adalah penggunaan teknologi telekomunikasi untuk memungkinkan pegawai bekerja di suatu lokasi yang berada di luar kantor untuk mengakses jaringan internal

kantor.

MENTERI PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT REPUBLIK INDONESIA,

ttd

M. BASUKI HADIMULJONO

Salinan sesuai dengan aslinya
KEMENTERIAN PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT
Kepala Biro Hukum,

Siti Martini
NIP. 195803311984122001