BERITA NEGARA REPUBLIK INDONESIA

No.1584, 2018 LAPAN. Kebijakan dan Standar Sistem Manajemen Pengamanan Informasi.

PERATURAN LEMBAGA PENERBANGAN DAN ANTARIKSA NASIONAL
REPUBLIK INDONESIA
NOMOR 3 TAHUN 2018
TENTANG
KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN PENGAMANAN INFORMASI
DI LINGKUNGAN LEMBAGA PENERBANGAN DAN ANTARIKSA NASIONAL

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA LEMBAGA PENERBANGAN DAN ANTARIKSA NASIONAL
REPUBLIK INDONESIA,

Menimbang : a. bahwa dalam rangka melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi dan fasilitas pengolahannya di lingkungan Lembaga Penerbangan dan Antariksa Nasional dari berbagai bentuk ancaman keamanan informasi baik dari dalam maupun luar, perlu pengaturan tentang kebijakan dan standar sistem manajemen pengamanan informasi di lingkungan

Lembaga Penerbangan dan Antariksa Nasional;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Lembaga Penerbangan dan Antariksa Nasional tentang Kebijakan dan Standar Sistem Manajemen Pengamanan Informasi di Lingkungan Lembaga Penerbangan dan Antariksa Nasional;

Mengingat : 1. Undang-Undang Nomor 21 Tahun 2013 tentang Keantariksaan (Lembaran Negara Republik Indonesia Tahun 2013 Nomor 133, Tambahan Lembaran Negara Republik Indonesia Nomor 5435);

2. Peraturan Presiden Nomor 49 Tahun 2015 tentang Lembaga Penerbangan dan Antariksa Nasional (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 91);

3. Peraturan Kepala Lembaga Penerbangan dan Antariksa Nasional Nomor 8 Tahun 2015 tentang Organisasi dan Tata Kerja Lembaga Penerbangan dan Antariksa Nasional (Berita Negara Republik Indonesia Tahun 2017 Nomor 1573) sebagaimana telah diubah dengan Peraturan Lembaga Penerbangan dan Antariksa Nasional Nomor 8 Tahun 2017 tentang Perubahan atas Peraturan Kepala Lembaga Penerbangan dan Antariksa Nasional Nomor 8 Tahun 2015 tentang Organisasi dan Tata Kerja Lembaga Penerbangan dan Antariksa Nasional (Berita Negara Republik Indonesia Tahun 2017 Nomor 1723);

MEMUTUSKAN:

Menetapkan : PERATURAN LEMBAGA PENERBANGAN DAN ANTARIKSA NASIONAL TENTANG KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN PENGAMANAN INFORMASI DI LINGKUNGAN LEMBAGA PENERBANGAN DAN ANTARIKSA NASIONAL.

Pasal 1

(1) Kebijakan dan Standar Sistem Manajemen Pengamanan Informasi di lingkungan Lembaga Penerbangan dan Antariksa Nasional, yang selanjutnya disebut Kebijakan dan Standar SMPI LAPAN meliputi kebijakan dan standar dalam:
   a. pengendalian umum;
   b. pengendalian organisasi keamanan informasi;
   c. pengamanan sumber daya manusia;
   d. pengendalian pengelolaan aset informasi dan fasilitas pengolahannya;
   e. pengendalian akses;
   f. pengendalian terhadap penerapan kriptografi;
   g. pengendalian pengelolaaan pengamanan fisik dan lingkungan;
   h. pengendalian pengelolaan pengamanan operasional;
   i. pengendalian pengamanan komunikasi;
   j. pengendalian pengamanan informasi dalam akuisisi, pengembangan, dan pemeliharaan sistem informasi;
   k. pengendalian hubungan dengan pihak ketiga atau penyedia;

l. pengendalian pengelolaan insiden keamanan informasi;
m. pengendalian aspek keamanan informasi dalam pengelolaan kelangsungan kegiatan; dan
n. pengendalian kepatuhan.

(2) Kebijakan dan Standar SMPI LAPAN sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Lembaga ini.

Pasal 2

Kebijakan dan Standar SMPI LAPAN sebagaimana dimaksud dalam Pasal 1 digunakan sebagai pedoman bagi Satuan Kerja untuk melindungi keamanan aset informasi dan fasilitas pengolahan yang dimiliki.

Pasal 3

(1) Pelaksanaan Kebijakan dan Standar SMPI LAPAN dilakukan oleh Tim Pengamanan Informasi LAPAN.
(2) Tim Pengamanan Informasi LAPAN sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Kepala LAPAN.

Pasal 4

Kebijakan dan Standar SMPI LAPAN dikaji ulang secara berkala paling kurang setiap 1 (satu) tahun sekali untuk menjamin efektivitas pelaksanaannya.

Pasal 5

Pada saat Peraturan Lembaga ini mulai berlaku, setiap Satuan Kerja dalam melakukan pengamanan aset informasi dan fasilitas pengolahannya, wajib menyesuaikan dengan Kebijakan dan Standar SMPI LAPAN berdasarkan Peraturan Lembaga ini paling lambat 3 (tiga) tahun terhitung sejak Peraturan Lembaga ini diundangkan.

Pasal 6

Peraturan Lembaga ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Lembaga ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 30 November 2018

KEPALA LEMBAGA PENERBANGAN DAN ANTARIKSA NASIONAL REPUBLIK INDONESIA,

ttd

THOMAS DJAMALUDDIN

Diundangkan di Jakarta
pada tanggal 4 Desember 2018

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

WIDODO EKATJAHJANA

LAMPIRAN
PERATURAN LEMBAGA PENERBANGAN DAN ANTARIKSA NASIONAL
NOMOR 3 TAHUN 2018
TENTANG
KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN PENGAMANAN INFORMASI DI LINGKUNGAN LEMBAGA PENERBANGAN DAN ANTARIKSA NASIONAL

KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN PENGAMANAN INFORMASI DI LINGKUNGAN LEMBAGA PENERBANGAN DAN ANTARIKSA NASIONAL

1. PENDAHULUAN

1.1 Latar Belakang

Konvergensi Teknologi Informasi dan Komunikasi (TIK) menyebabkan berbagai jenis layanan TIK dapat diperoleh dimanapun, kapanpun dan dengan menggunakan perangkat apapun. Dengan adanya TIK, semua jenis informasi tersimpan di internet dan dapat diakses oleh siapapun. Informasi telah tersedia dengan berbagai macam ulasan dari mulai informasi pemberitaan, informasi hiburan, dan informasi pengetahuan. Pertukaran informasi dan penyebaran informasi melalui perangkat TIK melahirkan era baru yaitu era banjirnya informasi dan berujung pada munculnya isu ancaman Keamanan Informasi oleh pengirim informasi, penerima informasi, dan pengguna informasi.

Untuk Kementerian, Lembaga, dan Pemerintah Daerah, isu terkait Keamanan Informasi mulai mengemuka setelah diterbitkannya Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pada peraturan tersebut terdapat kewajiban pengamanan sistem elektronik bagi penyelenggara sistem elektronik untuk pelayanan publik.

Dalam peraturan tersebut dipaparkan bahwa lembaga publik baik instansi pemerintah ataupun swasta harus memiliki manajemen pengamanan informasi, yang bertujuan untuk mengurangi risiko akibat adanya insiden Keamanan Informasi yang bisa datang kapan saja dan menyerang perangkat atau sistem pengolah data dan informasi. Manajemen pengamanan informasi merupakan solusi untuk melindungi aset informasi dan fasilitas pengolahannya yang menjamin tiga hal penting yaitu: kerahasiaan *(confidentiality)*, keutuhan *(integrity)* dan ketersediaan *(availability)*.

Ketentuan di atas diperkuat dengan diterbitkannya Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi yang mengamanatkan bahwa penyelenggara sistem elektronik strategis dan penyelenggara sistem elektronik tinggi wajib memiliki sertifikat sistem manajemen pengamanan informasi dengan berbasis ISO/SNI 27001, maka LAPAN perlu menyusun dokumen Kebijakan dan Standar Sistem Manajemen Pengamanan Informasi berbasis ISO 27001.

1.2 Istilah Yang Digunakan

1. Sistem Manajemen Pengamanan Informasi (SMPI) adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penanggung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan Keamanan Informasi.
2. Pengamanan Informasi adalah perlindungan aset informasi dan fasilitas pengolahannya dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.
3. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi.
4. Aset Informasi dan fasilitas pengolahannya adalah informasi yang memiliki nilai bagi organisasi yang dihasilkan dari fasilitas pengolahan informasi yang terkait dengan Sistem Informasi, Infrastruktur dan Teknologi Informasi.
5. Informasi adalah hasil pemrosesan, rekayasa dan pengorganisasian data untuk pengambilan keputusan.
6. Data adalah catatan atas kumpulan fakta yang mempunyai arti baik secara kualitatif maupun kuantitatif.
7. Fasilitas adalah sarana untuk melancarkan pelaksanaan fungsi atau mempermudah sesuatu.
8. Perangkat Lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.
9. Sistem Informasi adalah serangkaian perangkat keras, perangkat lunak, sumber daya manusia, serta prosedur dan atau aturan yang dikelola secara terpadu untuk mengolah data menjadi informasi yang berguna untuk mencapai suatu tujuan.

10. Perangkat Pengolah Informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur.
11. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan Keamanan Informasi.
12. Hak Akses Khusus adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan (*storage devices*), file server, dan aplikasi-aplikasi sensitif yang hanya diberikan kepada Pengguna yang membutuhkan dan pemakaiannya terbatas dan dikontrol.
13. Akun adalah identifikasi pengguna yang diberikan oleh unit Pengelola teknologi informasi, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem teknologi informasi.
14. 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.
15. Kata Sandi adalah serangkaian kode yang dibuat pengguna, bersifat rahasia dan pribadi digunakan bersamaan dengan akun pengguna.
16. Sistem Teknologi Informasi adalah sistem operasi, sistem surat elektronik, sistem aplikasi, sistem basis data, sistem jaringan intranet/internet, dan sebagainya.
17. Perangkat Jaringan adalah peralatan jaringan komunikasi data.
18. Perangkat Pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras dan perangkat jaringan serta untuk melindungi dari kerusakan.
19. Malicious Code adalah semua macam program yang membahayakan termasuk makro atau script yang dapat diesekusi dan dibuat dengan tujuan untuk merusak sistem komputer.
20. Teleworking adalah penggunaan teknologi telekomunikasi yang memungkinkan pegawai LAPAN dapat bekerja di suatu lokasi yang berada di luar kantor untuk mengakses jaringan internal kantor.
21. Routing adalah sebuah mekanisme untuk mengarahkan dan menentukan rute yang akan dilewati paket data dari satu perangkat ke perangkat yang berada di jaringan lain.
22. System Administrator adalah akun khusus untuk mengelola sistem informasi.

23. Aset Fisik adalah jenis aset yang memiliki wujud fisik, misalnya perangkat komputer, perangkat jaringan dan komunikasi, removable media, dan perangkat pendukung lainnya.
24. Aset Tak Berwujud adalah jenis aset yang tidak memiliki wujud fisik, misalnya pengetahuan, pengalaman, keahlian, citra, dan reputasi.
25. Aset Personel adalah jenis aset yang dihasilkan dari Sumber Daya Manusia, misalnya kompentensi yang dimiliki oleh personel tersebut.
26. Denial of Service adalah suatu kondisi dimana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang tidak terkendali baik dari dalam maupun dari luar sistem.
27. 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.
28. Master Disk adalah media yang digunakan sebagai sumber dalam melakukan instalasi perangkat lunak.
29. Mobile Computing adalah penggunaan perangkat komputasi yang dapat dipindah (*portabel*) misalnya notebook dan personal data assistant (PDA) untuk melakukan akses, pengolahan data dan penyimpanan.
30. Perjanjian Escrow adalah perjanjian dengan pihak ketiga untuk memastikan apabila pihak ketiga tersebut bangkrut (mengalami *failure*) maka LAPAN berhak untuk mendapatkan jaminan kelangsungan kegiatan yang dilakukan oleh pihak ketiga.
31. Proses Pendukung (*Support Proceses*) adalah proses-proses penunjang yang mendukung suatu proses utama yang terkait. Contoh proses pendukung dalam pengembangan (*development*) adalah proses pengujian perangkat lunak, proses perubahan perangkat lunak.
32. 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.
33. Rollback adalah sebuah mekanisme yang digunakan untuk mengembalikan sistem ke kondisi semula sebelum perubahan diimplementasikan. Mekanisme ini biasanya terdapat pada sistem basis data.

34. Pencatatan Waktu (*Timestamp*) adalah catatan waktu dalam tanggal dan/atau format waktu tertentu saat suatu aktivitas/transaksi terjadi. Format ini biasanya disajikan dalam format yang konsisten, yang memungkinkan untuk membandingkan dua aktivitas/transaksi yang berbeda berdasarkan waktu.
35. Daftar Inventaris Aset Informasi dan fasilitas pengolahannya adalah kumpulan informasi yang memuat bentuk, pemilik, lokasi, retensi, dan hal-hal yang terkait dengan aset informasi.
36. Dokumen SMPI LAPAN adalah dokumen terkait pelaksanaan SMPI yang meliputi antara lain dokumen kebijakan, standar, prosedur, dan catatan penerapan SMPI di lingkungan LAPAN.
37. Koneksi Eksternal (*Remote Access*) adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.
38. Komite Teknologi Informasi adalah komite yang bertugas untuk memberikan arahan dan melakukan pengawasan serta evaluasi terhadap pelaksanaan Sistem Manajemen Pengamanan Informasi.
39. *Chief Information Security Officer* LAPAN yang selanjutnya disebut CISO LAPAN adalah pejabat tinggi pratama yang bertugas sebagai pengelola Sistem Manajemen Pengamanan Informasi di lingkungan LAPAN.
40. *Chief Information Security Officer* Satuan Kerja yang selanjutnya disebut CISO Satuan Kerja adalah pejabat yang bertugas sebagai pengelola Sistem Manajemen Pengamanan Informasi di lingkungan Satuan Kerja.
41. *Information Security Manager* LAPAN yang selanjutnya disebut IS *Manager* LAPAN adalah pejabat yang bertugas mengkoordinasikan pelaksanaan SMPI LAPAN.
42. *Information Security Manager* Satuan Kerja yang selanjutnya disebut IS *Manager* satuan Kerja adalah pejabat yang bertugas mengkoordinasikan pelaksanaan SMPI Satuan Kerja.
43. *Information Security Officer* LAPAN yang selanjutnya disebut IS *Officer* LAPAN adalah pejabat yang bertugas melaksanakan penyelesaian masalah/insiden Keamanan Informasi di LAPAN.
44. *Information Security Officer* Satuan Kerja yang selanjutnya disebut IS *Officer* Satuan Kerja adalah pejabat yang bertugas melaksanakan penyelesaian masalah/insiden Keamanan Informasi di Satuan Kerja.
45. *Service Desk* LAPAN adalah pejabat yang bertugas mencatat gangguan Keamanan Informasi.

46. Pengguna adalah pegawai LAPAN dan/atau pihak ketiga serta tidak terbatas pada pengelola teknologi informasi dan kelompok kerja yang diberikan hak mengakses sistem teknologi informasi di lingkungan LAPAN.
47. Satuan Kerja adalah unit kerja di lingkungan LAPAN yang melaksanakan kegiatan dan memiliki kewenangan dan tanggung jawab sebagai kuasa pengguna anggaran/kuasa pengguna barang.
48. Pihak Berwenang adalah pihak yang mempunyai kewenangan terkait suatu hal, seperti: kepolisian, instansi pemadam kebakaran, dan penyedia jasa telekomunikasi/internet.
49. Pemilik Aset Informasi dan fasilitas pengolahannya adalah Satuan Kerja yang memiliki kewenangan terhadap aset informasi dan fasilitas pengolahannya.
50. Komunitas Pengamanan Informasi adalah kelompok/komunitas yang memiliki pengetahuan/keahlian khusus dalam bidang Keamanan Informasi atau yang relevan dengan Keamanan Informasi.
51. Pihak Ketiga adalah semua unsur di luar pengguna unit teknologi informasi LAPAN yang bukan bagian dari LAPAN, namun memiliki hubungan kontraktual.

2. PENGENDALIAN UMUM

2.1 Tujuan

Pengendalian umum bertujuan untuk memberikan pedoman umum bagi CISO LAPAN dan CISO Satuan Kerja dalam pengelolaan Kebijakan dan Standar SMPI, untuk melindungi aset informasi dan fasilitas pengolahannya dari aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

2.2 Ruang Lingkup

Ruang lingkup pengendalian umum ini meliputi:

1. Pengelolaan pengamanan seluruh aset informasi dan fasilitas pengolahannya yang dilaksanakan oleh seluruh Satuan Kerja di lingkungan LAPAN, pegawai baik sebagai pengguna maupun pengelola Teknologi Informasi, dan pihak ketiga.
2. Aset informasi dalam bentuk:
   a) Informasi/dokumen yang merupakan hasil pelaksanaan tugas dan fungsi LAPAN, seperti: bahan dan hasil penelitian/perekayasaan, dokumen penawaran dan kontrak, dokumen perjanjian kerahasiaan, dokumen kebijakan lembaga, dokumen administrasi dan teknis;
   b) Perangkat lunak, seperti: perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat bantu pengembangan sistem;
   c) Aset fisik, seperti: perangkat komputer, perangkat jaringan dan komunikasi, *removable media*, dan perangkat pendukung;
   d) Layanan, seperti: layanan internet, layanan email, dan Layanan Pengadaan Secara Elektronik;
   e) Aset tak berwujud (*intangible*), seperti: pengetahuan, pengalaman, keahlian, citra, dan reputasi; dan
   f) Aset Personel, seperti: Pegawai Negeri Sipil, Pegawai Pemerintah Non Pegawai Negeri, dan pegawai kontrak.

2.3 Kebijakan

1. CISO LAPAN bertanggung jawab mengatur penerapan Kebijakan dan Standar SMPI LAPAN.
2. CISO Satuan Kerja bertanggung jawab menerapkan Kebijakan dan Standar SMPI LAPAN di lingkungan Satuan Kerja masing-masing dan berkoordinasi dengan CISO LAPAN.

3. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab menentukan sasaran Pengamanan Informasi (*information security objective*) sesuai kewenangan masing-masing dan secara berkala memantau pencapaiannya.
4. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab atas ketersediaan sumber daya yang diperlukan sesuai kewenangan masing-masing untuk penerapan Kebijakan dan Standar SMPI LAPAN yang ditetapkan dalam Peraturan ini.
5. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab untuk mengidentifikasi persyaratan dan kebutuhan Pengamanan Informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi sesuai kewenangan masing-masing.
6. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mengatur pelaksanaan pengamanan dan perlindungan aset informasi dan fasilitas pengolahannya sesuai kewenangan masing-masing dengan mengacu pada Kebijakan dan Standar SMPI LAPAN.
7. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab melaksanakan pengamanan aset informasi dan fasilitas pengolahannya sesuai kewenangan masing-masing dengan mengacu pada Kebijakan dan Standar SMPI LAPAN.
8. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab melaksanakan pengamanan aset teknologi informasi sesuai kewenangan masing-masing dengan mengacu pada Kebijakan dan Standar SMPI LAPAN.
9. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab meningkatkan pengetahuan, keterampilan dan kepedulian terhadap keamanan informasi pada seluruh pengguna sesuai kewenangan masing-masing.
10. CISO LAPAN dan CISO Satuan Kerja menerapkan manajemen risiko Pengamanan Informasi yang setidaknya mencakup kajian terhadap pemenuhan persyaratan dan kebutuhan Pengamanan Informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi sesuai kewenangan masing-masing.
11. Audit internal SMPI harus dilakukan untuk memastikan pengendalian, proses dan prosedur SMPI dilaksanakan secara efektif sesuai dengan Kebijakan dan Standar SMPI LAPAN dan dipelihara dengan baik dan setidaknya harus dilakukan satu tahun sekali.

12. CISO LAPAN dan CISO Satuan Kerja memastikan bahwa secara berkala dilakukan pemantauan dan evaluasi terhadap kepatuhan dan keefektifan pelaksanaan SMPI serta melakukan tindak lanjut yang diperlukan untuk secara berkesinambungan meningkatkan kepatuhan dan keefektifan implementasi SMPI di lingkungan kerja masing-masing.
13. CISO LAPAN dan CISO Satuan Kerja tidak bertanggung jawab atas kerugian atau kerusakan data maupun perangkat lunak milik pihak ketiga yang diakibatkan dari upaya untuk melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi dan fasilitas pengolahannya.

2.4 Standar

1. Sasaran Pengamanan Informasi (*information security objective*) setidaknya mencakup kriteria berikut ini:
   a. Terukur;
   b. Mencakup derajat pencapaian persyaratan dan kebutuhan Pengamanan Informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi;
   c. Mencakup derajat kepatuhan dan keefektifan implementasi SMPI terhadap Kebijakan dan Standar SMPI LAPAN.
2. Standar manajemen risiko Pengamanan Informasi mengikuti ketentuan mengenai Penerapan Manajemen Risiko di Lingkungan LAPAN.
3. Standar Dokumen Penerapan Kebijakan dan Standar SMPI LAPAN adalah sebagai berikut:
   a. CISO LAPAN dan CISO Satuan Kerja harus memastikan terdokumentasinya catatan penerapan Kebijakan dan Standar SMPI LAPAN, sehingga kepatuhan dan efektivitas penerapan SMPI dapat diukur.
   b. Dokumen penerapan Kebijakan dan Standar SMPI LAPAN setidaknya meliputi:
      1) Formulir-formulir sesuai prosedur operasional yang dijalankan;
      2) Catatan insiden keamanan informasi;
      3) Catatan dari sistem;
      4) Catatan pengunjung di *secure areas*;
      5) Kontrak dan perjanjian layanan;
      6) Perjanjian kerahasiaan (*confidentiality agreements*); dan
      7) Laporan hasil audit.

4. Dokumen pendukung kebijakan Pengamanan Informasi setidaknya memuat informasi-informasi sebagai berikut:
   a. Tujuan dan ruang lingkup dokumen pendukung kebijakan Pengamanan Informasi;
   b. Kerangka kerja setiap tujuan/sasaran pengendalian Pengamanan Informasi;
   c. Metodologi penilaian risiko *(risk assessment);*
   d. Penjelasan singkat mengenai standar, prosedur dan kepatuhan termasuk persyaratan peraturan yang harus dipenuhi, pengelolaan kelangsungan kegiatan, konsekuensi apabila terjadi pelanggaran;
   e. Tanggung jawab dari setiap bagian terkait; dan
   f. Dokumen referensi yang digunakan dalam menyusun dokumen pendukung kebijakan Pengamanan Informasi.

5. Standar pengendalian dokumentasi SMPI sebagai berikut:
   a. CISO LAPAN dan CISO Satuan Kerja harus mengendalikan dokumen SMPI untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan, dan mencegah akses oleh pihak yang tidak berwenang.
   b. CISO LAPAN dan CISO Satuan Kerja harus memastikan adanya penempatan dokumen SMPI di semua area operasional sehingga mudah diakses oleh pengguna di Satuan Kerja masing-masing sesuai peruntukannya.
6. Evaluasi kepatuhan dan implementasi SMPI setidaknya mencakup hal-hal sebagai berikut:
   a. Evaluasi terhadap hasil audit internal SMPI;
   b. Evaluasi terhadap pencapaian Sasaran Pengamanan Informasi *(information security objective);*
   c. Evaluasi terhadap pencapaian persyaratan dan kebutuhan persyaratan dan kebutuhan Pengamanan Informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi;
   d. Evaluasi terhadap umpan balik dari pihak-pihak di luar organisasi;
   e. Evaluasi dari penerapan manajemen risiko SMPI; dan
   f. Evaluasi terhadap kemungkinan-kemungkinan untuk peningkatan kinerja SMPI.

3. PENGENDALIAN ORGANISASI PENGAMANAN INFORMASI

3.1 Tujuan

Pengendalian Organisasi Pengamanan Informasi bertujuan untuk memberikan pedoman dalam membentuk organisasi fungsional Pengamanan Informasi yang bertanggung jawab untuk mengelola Keamanan Informasi dan perangkat pengolah informasi di lingkungan LAPAN termasuk hubungan dengan pihak luar.

3.2 Ruang Lingkup

Ruang lingkup kebijakan dan standar organisasi Pengamanan Informasi meliputi:

1. Struktur Tim Pengamanan Informasi di LAPAN dan Satuan Kerja;
2. Perjanjian kerahasiaan;
3. Pemisahan tugas;
4. Hubungan dengan pihak berwenang, Komunitas Pengamanan Informasi, dan pihak ketiga;
5. Pengamanan Informasi pada pengelolaan program/kegiatan; dan
6. Pengendalian terhadap *Mobile Device* dan *Teleworking*.

3.3 Kebijakan

1. Struktur Tim Pengamanan Informasi di LAPAN dan Satuan Kerja berikut tanggung jawab dan wewenangnya diuraikan dalam standar organisasi Pengamanan Informasi.
2. Tanggung jawab dan wewenang Tim Pengamanan Informasi di LAPAN dapat dipetakan dalam jabatan struktural dan/atau diperankan oleh Pejabat struktural dan/atau Pejabat fungsional.
3. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mengidentifikasi dan mengkaji secara berkala persyaratan untuk menjaga kerahasiaan aset informasi dan fasilitas pengolahannya yang dituangkan dalam dokumen perjanjian kerahasiaan.
4. Pemisahan Tugas:
   a. CISO LAPAN dan CISO Satuan Kerja harus memastikan pemisahan tugas untuk proses-proses yang berpotensi memiliki konflik kepentingan dan kewenangan guna mengurangi kesempatan terhadap akses ilegal, modifikasi yang tidak sah, dan penyalahgunaan aset informasi dan fasilitas pengolahannya.
   b. CISO LAPAN dan CISO Satuan Kerja harus memastikan pemisahan tugas untuk proses yang melibatkan informasi dengan klasifikasi SANGAT RAHASIA dan RAHASIA untuk menghindari

adanya pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan fasilitas pengolahannya.

5. Hubungan dengan Pihak Berwenang:
   a. CISO LAPAN bertanggung jawab mengidentifikasi dan menjalin kerjasama dengan pihak berwenang di luar LAPAN yang terkait dengan Keamanan Informasi.
   b. CISO Satuan Kerja dapat menjalin kerja sama dengan pihak berwenang di luar LAPAN yang terkait dengan Keamanan Informasi dan wajib berkoordinasi dengan CISO LAPAN.
6. Hubungan dengan Komunitas Pengamanan Informasi
   a. CISO LAPAN wajib berkoordinasi dengan CISO Satuan Kerja yang berwenang dalam hal menjalin kerja sama dengan Komunitas Pengamanan Informasi di luar LAPAN melalui pelatihan, seminar, atau forum lain yang relevan dengan Pengamanan Informasi.
   b. CISO Satuan Kerja wajib berkoordinasi dengan CISO LAPAN dan Satuan Kerja yang berwenang dalam hal menjalin kerja sama dengan Komunitas Pengamanan Informasi di luar LAPAN melalui pelatihan, seminar, atau forum lain yang relevan dengan Keamanan Informasi.
7. Pengendalian terhadap Pengamanan Informasi harus diterapkan dalam pengelolaan dan harus diaplikasikan pada seluruh fase dalam metodologi pengelolaan program/kegiatan.
8. Pengendalian terhadap *Mobile Device* dan *Teleworking*
   a. CISO LAPAN dan CISO Satuan Kerja membangun kepedulian pengguna perangkat *mobile device* dan *teleworking* akan risiko keamanan yang terus meningkat terhadap informasi yang tersimpan dalam perangkat *mobile device;* dan
   b. Pengguna perangkat *mobile device* dan *teleworking* harus mengikuti prosedur yang terkait penggunaan perangkat *mobile device* dan *teleworking* untuk menjaga keamanan perangkat dan informasi di dalamnya.

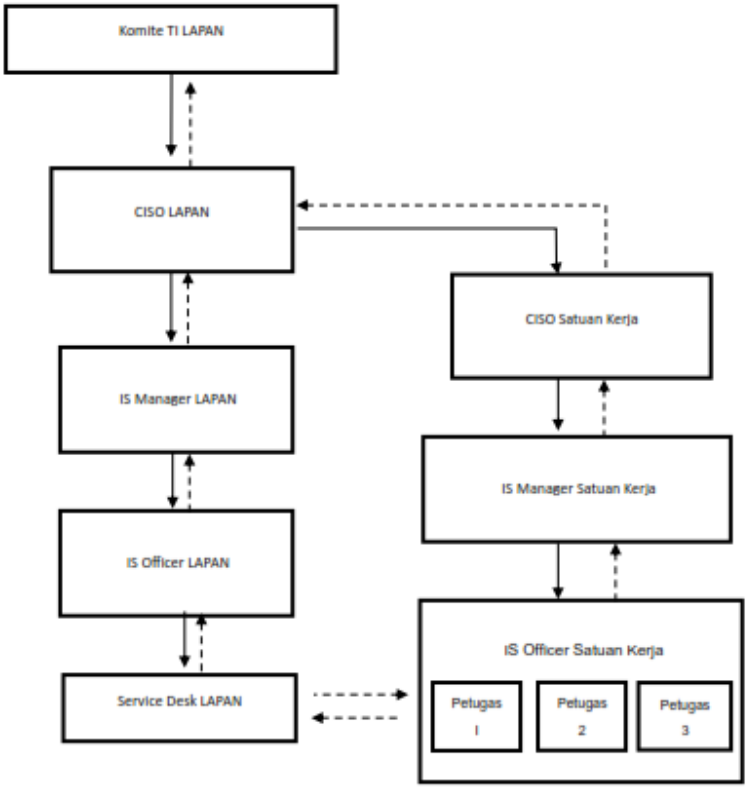
3.4 Standar

1. Tim Pengamanan Informasi, terdiri atas:
   a. Tim Pengamanan Informasi LAPAN, yang beranggotakan:
      1) Komite TI LAPAN;
      2) CISO LAPAN;
      3) IS *Manager* LAPAN;

4) IS *Officer* LAPAN;
5) CISO Satuan Kerja; dan
6) *Service Desk* LAPAN.

b. Tim Pengamanan Informasi Satuan Kerja, yang beranggotakan:
1) CISO Satuan Kerja;
2) IS *Manager* Satuan Kerja; dan
3) IS *Officer* Satuan Kerja.

2. Struktur Tim Pengamanan Informasi



——— Garis Koordinasi
------ Garis Laporan

3. Tugas dan tanggung jawab Tim Pengamanan Informasi LAPAN

a. Komite TI

Komite Teknologi Informasi bertugas dan bertanggungjawab untuk memberikan arahan dan melakukan pengawasan serta evaluasi terhadap pelaksanaan Sistem Manajemen Pengamanan Informasi.

b. CISO LAPAN
   1) CISO LAPAN bertugas sebagai pengelola SMPI LAPAN.
   2) CISO LAPAN bertanggung jawab untuk:
      a) mengkoordinasikan perumusan dan penyempurnaan Kebijakan dan Standar SMPI LAPAN;
      b) memelihara dan mengendalikan penerapan Kebijakan dan Standar SMPI LAPAN di seluruh area yang menjadi tujuan/sasaran pengendalian;
      c) menetapkan target Keamanan Informasi setiap tahunnya dan menyusun rencana kerja untuk kegiatan Pengamanan Informasi LAPAN, maupun yang bersifat lintas unit;
      d) memastikan efektivitas dan konsistensi penerapan Kebijakan dan Standar SMPI LAPAN dan mengukur kinerja keseluruhan; dan
      e) melaporkan kinerja penerapan Kebijakan dan Standar SMPI LAPAN dan pencapaian target kepada Komite Teknologi Informasi LAPAN.

c. *IS Manager* LAPAN
   1) *IS Manager* LAPAN bertugas mengkoordinasikan pelaksanaan SMPI LAPAN.
   2) *IS Manager* LAPAN bertanggung jawab untuk:
      a) memastikan Kebijakan dan Standar SMPI LAPAN diterapkan secara efektif;
      b) memastikan langkah-langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan dalam pelaksanaan evaluasi dan/atau audit penerapan Kebijakan dan Standar SMPI LAPAN;
      c) memastikan peningkatan kesadaran, kepedulian, dan kepatuhan seluruh pegawai terhadap Kebijakan dan Standar SMPI LAPAN;
      d) melaporkan kinerja penerapan Kebijakan dan Standar SMPI LAPAN sesuai ruang lingkup tanggung jawabnya kepada CISO LAPAN yang akan digunakan sebagai dasar peningkatan Pengamanan Informasi;
      e) mengkoordinasikan penanganan insiden Keamanan Informasi di lingkungan LAPAN; dan

f) memastikan terlaksananya audit internal terhadap penerapan Kebijakan dan Standar SMPI LAPAN paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

d. *IS Officer* LAPAN

1) *IS Officer* LAPAN bertugas melaksanakan penyelesaian masalah/insiden Keamanan Informasi di LAPAN.

2) *IS Officer* LAPAN bertanggung jawab untuk:

a) melaksanakan dan mengawasi penerapan Kebijakan dan Standar SMPI LAPAN;

b) memberi masukan peningkatan terhadap Kebijakan dan Standar SMPI LAPAN;

c) mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan Pengamanan Informasi bagi pegawai;

d) memantau, mencatat, dan menguraikan secara jelas insiden Keamanan Informasi yang diketahui atau laporan yang diterima, dan menindaklanjuti laporan tersebut sesuai prosedur pelaporan insiden Keamanan Informasi; dan

e) memberi panduan dan/atau bantuan penyelesaian insiden Keamanan Informasi.

3) CISO Satuan Kerja dan bertanggung jawab untuk:

a) melakukan koordinasi penerapan Kebijakan dan Standar SMPI LAPAN di lingkungan Satuan Kerja masing-masing; dan

b) melakukan evaluasi dampak insiden Keamanan Informasi untuk dilaporkan kepada CISO LAPAN, dan menindaklanjutinya.

4) *Service Desk* bertugas dan bertanggungjawab untuk menerima dan mencatat gangguan Keamanan Informasi.

4. Tugas dan tanggung jawab Tim Pengamanan Informasi LAPAN

a. CISO Satuan Kerja

1) CISO Satuan Kerja bertugas sebagai pengelola SMPI Satuan Kerja.

2) CISO Satuan Kerja bertanggung jawab untuk:

a) memelihara dan mengendalikan penerapan Kebijakan dan Standar SMPI LAPAN di seluruh area yang menjadi

tujuan/sasaran pengendalian pada Satuan Kerja masing-masing;

b) menetapkan target Pengamanan Informasi setiap tahunnya dan menyusun rencana kerja pada Satuan Kerja masing-masing;

c) mengukur efektivitas dan konsistensi penerapan Kebijakan dan Standar SMPI LAPAN pada Satuan Kerja masing-masing; dan

d) memberi masukan untuk meningkatkan penerapan Kebijakan dan Standar SMPI LAPAN.

b. *IS Manager* Satuan Kerja

1) *IS Manager* Satuan Kerja bertugas mengkoordinasikan pelaksanaan SMPI LAPAN di lingkungan Satuan Kerja.

2) *IS Manager* Satuan Kerja bertanggung jawab untuk:

a) memastikan Kebijakan dan Standar SMPI LAPAN diterapkan secara efektif pada Satuan Kerja masing-masing;

b) memastikan langkah-langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan dalam pelaksanaan evaluasi dan/atau audit penerapan Kebijakan dan Standar SMPI LAPAN pada Satuan Kerja masing-masing;

c) memastikan peningkatan kesadaran, kepeduulian, dan kepatuhan seluruh pegawai terhadap Kebijakan dan standar SMPI LAPAN pada Satuan Kerja masing-masing;

d) melaporkan kinerja penerapan Kebijakan dan Standar SMPI LAPAN pada Satuan Kerja masing-masing sesuai ruang lingkup tanggung jawabnya kepada CISO Satuan Kerja yang akan digunakan sebagai dasar peningkatan Keamanan Informasi;

e) mengkoordinasikan penanganan insiden Keamanan Informasi pada Satuan Kerja masing-masing;

f) memastikan evaluasi terhadap Kebijakan dan Standar SMPI LAPAN pada Satuan Kerja masing-masing terlaksana secara efektif dan efisien; dan

g) memastikan terlaksananya evaluasi dan/atau audit internal terhadap penerapan Kebijakan dan Standar SMPI LAPAN pada Satuan Kerja masing-masing paling sedikit 1

(satu) kali dalam 1 (satu) tahun.

c. IS *Officer* Satuan Kerja

1) IS *Officer* Satuan Kerja bertugas melaksanakan penyelesaian masalah/insiden keamanan informasi di Satuan Kerja.

2) IS *Officer* Satuan Kerja bertanggung jawab:

a) melaksanakan dan mengawasi penerapan Kebijakan dan Standar SMPI LAPAN pada Satuan Kerja masing-masing;

b) memberi masukan untuk meningkatkan penerapan Kebijakan dan Standar SMPI LAPAN pada Satuan Kerja masing-masing melalui CISO Satuan Kerja;

c) mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan Pengamanan Informasi bagi pegawai pada Satuan Kerja masing-masing;

d) memantau, mencatat, menguraikan, dan menindaklanjuti insiden Keamanan Infromasi yang diketahui atau dilaporkan sesuai prosedur pelaporan insiden Keamanan Informasi pada Satuan Kerja masing-masing; dan

e) memberikan panduan dan/atau bantuan penyelesaian insiden Keamanan Informasi pada Satuan Kerja masing-masing.

4. PENGAMANAN SUMBER DAYA MANUSIA

4.1 Tujuan

Pengamanan sumber daya manusia bertujuan untuk memastikan pegawai dan pihak ketiga di lingkungan LAPAN memahami tanggung jawab masing-masing, sadar atas ancaman Keamanan Informasi, serta mengetahui proses terkait Pengamanan Informasi sebelum, selama, dan setelah bertugas.

4.2 Ruang Lingkup

Kebijakan dan standar pengamanan sumber daya manusia ini mencakup peran dan tanggung jawab pegawai dan pihak ketiga di lingkungan LAPAN yang harus dipahami dan dilaksanakan. Peran dan tanggung jawab pegawai juga mengacu pada peraturan perundang-undangan yang berlaku.

4.3 Kebijakan

1. Pegawai bertanggung jawab untuk menjaga Keamanan Informasi LAPAN sesuai dengan tugas dan fungsinya.

2. Pihak ketiga harus menyetujui dan menandatangani syarat dan perjanjian untuk menjaga Keamanan Informasi LAPAN.
3. Peran dan tanggung jawab pegawai dan pihak ketiga terhadap Pengamanan Informasi didefinisikan, didokumentasikan, dan dikomunikasikan kepada pegawai dan pihak ketiga yang bersangkutan.
4. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab melakukan pemeriksaan data pribadi yang diberikan oleh pegawai baru dan pihak ketiga sesuai dengan kewenangan masing-masing.
5. Pegawai harus mendapatkan pendidikan, pelatihan, dan sosialisasi Pengamanan Informasi secara berkala sesuai tingkat tanggung jawabnya.
6. Pihak ketiga, jika diperlukan dapat diberikan sosialisasi untuk meningkatkan kepedulian terhadap Keamanan Informasi.
7. Pegawai dan pihak ketiga yang melanggar Kebijakan dan Standar SMPI LAPAN akan dikenai sanksi atau tindakan disiplin sesuai ketentuan yang berlaku.
8. Kepatuhan pegawai terhadap Kebijakan dan Standar SMPI LAPAN harus dievaluasi secara berkala oleh atasan masing-masing dan menjadi bagian dari penilaian kinerja pegawai.
9. CISO LAPAN dan CISO Satuan Kerja harus memastikan penghentian terhadap hak penggunaan aset informasi dan fasilitas pengolahannya bagi pegawai yang sedang menjalani pemeriksaan yang terkait dengan dugaan adanya pelanggaran Kebijakan dan Standar SMPI LAPAN dan/atau yang sedang menjalani proses hukum di Satuan Kerja masing-masing.
10. CISO LAPAN dan/atau CISO Satuan Kerja harus memastikan pencabutan hak akses terhadap aset informasi dan fasilitas pengolahannya yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak bekerja lagi di LAPAN.

4.4 Standar

Pengamanan Sumber Daya Manusia meliputi:

1. Peran dan tanggung jawab pegawai terhadap Pengamanan Informasi harus menjadi bagian dari penjabaran tugas dan fungsi, khususnya bagi yang memiliki akses terhadap aset informasi dan fasilitas pengolahannya.

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.
3. Peran dan tanggung jawab pegawai terhadap Pengamanan Informasi meliputi:
   a. melaksanakan dan bertindak sesuai dengan organisasi Pengamanan Informasi;
   b. melindungi aset informasi dan fasilitas pengolahannya dari akses yang tidak sah, penyingkapan, modifikasi, kerusakan atau gangguan;
   c. melaksanakan proses pengamanan atau kegiatan Pengamanan Informasi sesuai dengan peran dan tanggung jawabnya; dan
   d. melaporkan kejadian, potensi kejadian, atau risiko Pengamanan Informasi sesuai dengan Kebijakan dan Standar SMPI LAPAN.
4. Pemeriksaan latar belakang calon pegawai yang meliputi:
   a. ketersediaan referensi, dari referensi hubungan kerja dan referensi pribadi;
   b. pemeriksaan kelengkapan dan ketepatan dari riwayat hidup pemohon;
   c. konfirmasi kualifikasi akademik dan profesional yang diklaim;
   d. pemeriksaan independen identitas (KTP, paspor atau dokumen yang sama); dan
   e. pemeriksaan lebih rinci, seperti pemeriksaan dari catatan kriminal.

5. PENGENDALIAN PENGELOLAAN ASET INFORMASI DAN FASILITAS PENGOLAHANNYA

5.1 Tujuan

Pengendalian Pengelolaan aset informasi dan fasilitas pengolahannya bertujuan memberikan pedoman dalam mengelola aset informasi dan fasilitas pengolahannya di lingkungan LAPAN untuk melindungi dan menjamin keamanannya.

5.2 Ruang Lingkup

Kebijakan dan standar pengelolaan aset informasi dan fasilitas pengolahannya meliputi:

1. Tanggung jawab terhadap aset informasi dan fasilitas pengolahannya;
2. Pengklasifikasian aset informasi dan fasilitas pengolahannya;
3. Penanganan aset informasi dan fasilitas pengolahannya;
4. Penanganan *removable media*;
5. Pengamanan penggunaan kembali atau penghapusan/pemusnahan perangkat; dan
6. Pertukaran media informasi secara fisik.

5.3 Kebijakan

1. Tanggung Jawab terhadap aset informasi dan fasilitas pengolahannya, meliputi:
   a. CISO LAPAN bertanggung jawab dalam mengkoordinasikan identifikasi aset informasi dan fasilitas pengolahannya di lingkungan LAPAN dan mendokumentasikannya dalam daftar inventaris aset *(asset register)*. Daftar inventaris aset *(asset register)* dipelihara dan dikelola perubahannya oleh Penanggung Jawab Proses Pengelolaan Asset Informasi dan Fasilitas Pengolahannya.
   b. CISO Satuan Kerja bertanggung jawab dalam mengidentifikasi aset informasi dan fasilitas pengolahannya di lingkungan Satuan Kerja masing-masing dan mendokumentasikannya dalam daftar inventaris aset *(asset register)*. Daftar inventaris aset *(asset register)* dipelihara dan dikelola perubahannya oleh Penanggung Jawab Proses Pengelolaan Asset Informasi dan Fasilitas Pengolahannya.
   c. Kepala Satuan Kerja menetapkan jenis aset informasi dan fasilitas pengolahannya.

d. Kepala Satuan Kerja menetapkan pemilik aset informasi dan fasilitas pengolahannya pada masing-masing Satuan Kerja.
e. Pemilik aset menetapkan aturan penggunaan aset informasi dan fasilitas pengolahannya.
f. pegawai yang berhenti bekerja atau mutasi harus mengembalikan seluruh aset informasi dan fasilitas pengolahannya yang dipergunakan selama bekerja sesuai dengan ketentuan yang berlaku.
g. Pihak ketiga yang habis masa kontrak kerjanya harus mengembalikan seluruh aset informasi dan fasilitas pengolahannya yang dipergunakan selama bekerja di LAPAN.

2. Klasifikasi Aset Informasi, meliputi:
   a. CISO LAPAN bertanggung jawab dalam penetapan klasifikasi aset informasi.
   b. aset informasi diklasifikasikan sesuai tingkat kerahasiaan, nilai, tingkat kritikalitas, serta aspek hukumnya.
   c. ketentuan rinci klasifikasi aset informasi diuraikan dalam standar pengelolaan aset informasi dan fasilitas pengolahannya.
   d. pemberian label klasifikasi aset informasi harus dilakukan secara konsisten terhadap seluruh aset informasi.
3. CISO LAPAN bertanggung jawab mengkoordinasikan penyusunan kebijakan dan/atau prosedur penanganan aset informasi dan fasilitas pengolahannya sesuai dengan klasifikasi aset informasi yang telah ditetapkan.
4. CISO LAPAN bertanggung jawab mengkoordinasikan penyusunan kebijakan dan/atau prosedur penanganan *removable media* sesuai dengan klasifikasi aset informasi yang telah ditetapkan.
5. Pengamanan penggunaan kembali atau penghapusan/pemusnahan perangkat, meliputi:
   a. perangkat pengolah informasi dan penyimpan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dihapuskan/dimusnahkan; dan
   b. ketentuan penanganan perangkat pengolah informasi dan penyimpan data di LAPAN sesuai dengan standar penanganan media penyimpan data akan diatur dalam Peraturan Lembaga.
6. Pemindahan Media Fisik

   CISO LAPAN bertanggung jawab mengkoordinasikan penyusunan kebijakan dan/atau prosedur penyusunan kebijakan pemindahan

media fisik yang mengandung informasi untuk melindungi akses yang tidak sah, penyalahgunaan dan kerusakan saat proses pemindahan.

5.4 STANDAR

Pengelolaan Aset Informasi dan fasilitas pengolahannya, meliputi:

1. Pemilik Aset Informasi dan fasilitas pengolahannya menetapkan dan mengkaji secara berkala klasifikasi aset informasi;
2. Pemilik Aset Informasi dan fasilitas pengolahannya menetapkan pihak yang berwenang untuk mengakses aset informasi dan fasilitas pengolahannya;
3. Dalam pengelolaan aset informasi LAPAN, aset informasi diklasifikasikan seperti pada tabel berikut:

Tabel Klasifikasi Aset Informasi

KLASIFIKASI ASET	KETERANGAN
Sangat Rahasia (*Strictly Confidential*)	Informasi LAPAN yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian negara.
Rahasia (*Confidential*)	Informasi LAPAN yang apabila secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu citra dan reputasi LAPAN dan/atau yang menurut peraturan perundang-undangan dinyatakan rahasia.
Terbatas (*Internal Use Only*)	Informasi LAPAN yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu citra dan reputasi LAPAN.
Publik	Informasi yang dihasilkan, disimpan, dikelola, dikirim dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan badan publik lainya yang sesuai dengan undang-undang serta informasi lain yang berkaitan dengan kepentingan publik.

4. Penanganan Aset Informasi dan Fasilitas Pengolahannya:
   a. Penanganan aset informasi harus disertai dengan perlindungan atau Pengamanan Informasi, yaitu dengan prinsip *confidentiality, integrity, availability, authentication* dan *non-repudiation.*
      1) *Confidentiality*, bahwa informasi yang dilindungi bersifat/dalam klasifikasi rahasia (hanya dapat/boleh diakses oleh pihak yang memang memiliki hak (kewenangan)).
      2) *Integrity*, bahwa informasi yang dilindungi bila diakses, dipindah, dipertukarkan atau dikirimkan tetap utuh (tidak berubah).
      3) *Availability,* bahwa informasi yang dilindungi tetap disimpan yang bila dibutuhkan sewaktu-waktu dapat dengan mudah tersedia (tidak hilang).
      4) *Authentication,* bahwa informasi yang dilindungi bila diakses, dipindah, dipertukarkan atau dikirimkan harus dipastikan dilakukan oleh pihak yang sebenarnya sebagai pemilik identitas dan hak (bukan pemalsu identitas dan hak).
      5) *Non-Repudiation*, bahwa informasi yang dilindungi bila diakses, diperjanjikan, dipertukarkan, ditransaksikan, atau dikirimkan antar pihak harus dipastikan disertai bukti akses, persetujuan/perjanjian, transaksi, pengiriman dan penerimaan, sehingga tidak ada pihak yang mengelak atas proses akses, persetujuan, transaksi, pengiriman dan penerimaan.
   b. Pengelolaan aset informasi harus dilakukan secara tepat, jelas, dan tercatat, sesuai klasifikasi peruntukannya.
   c. Setiap informasi yang diproses melalui sarana elektronik termasuk dalam klasifikasi informasi di atas, harus disertai model kontrol yang tidak dipisahkan dengan dokumen Informasi tersebut, yang berisikan informasi:
      1) Waktu pengiriman dokumen;
      2) Alur pemeriksa yang dilalui;
      3) Alur distribusi dan pengiriman dokumen dari *originator* sampai di penerima; dan
      4) Kode klasifikasi informasi.
   d. Dokumen informasi dan lembar kontrol elektronik yang menjadi acuan adalah yang melalui format resmi LAPAN dan

penggunaanya telah dinyatakan berlaku pada saat terjadi pengiriman informasi.

e. Dokumen informasi elektronik dan lembar kontrol akan dihapuskan dari sistem dengan jangka waktu tertentu setelah persetujuan (*approval*).

5. Pengelolaan *Removable Media:*

a. media penyimpanan informasi *removable* yang digunakan oleh pegawai hanya untuk keperluan pekerjaan.

b. pegawai harus memberikan pengamanan terhadap media penyimpanan informasi *removable* untuk mencegah adanya kegagalan dan kerusakan informasi akibat penyebaran *malicious code.*

c. pegawai menggunakan dan menyimpan media penyimpanan informasi *removable* secara aman sehingga informasi yang tersimpan di dalamnya terlindung dari pihak yang tidak berwenang.

d. pegawai harus memastikan bahwa media penyimpanan informasi *removable* dalam keadaan bebas *malicious code* dengan cara selalu melakukan *scanning* ketika media penyimpanan informasi *removable* tersebut disambungkan ke PC/Notebook sebelum mengakses informasi di dalamnya.

e. pegawai harus menggunakan sistem penangkal *malicious code* yang dimiliki oleh LAPAN.

f. pegawai harus memastikan media penyimpanan informasi *removable* yang sudah tidak digunakan lagi untuk menyimpan informasi rahasia harus bersih dari segala bentuk informasi dengan melakukan format (tidak menggunakan format *quick*) pada media penyimpanan informasi *removable.*

g. pegawai harus memastikan media penyimpanan informasi yang sudah rusak dan kadaluarsa harus dimusnahkan (dihancurkan secara fisik).

h. Pemindahan media penyimpanan informasi *removable* ke luar dari lingkungan LAPAN menjadi tanggung jawab dari peminjam/pemilik media untuk melindungi informasi sesuai dengan klasifikasi informasi yang terkandung di dalamnya.

i. Apabila media-media penyimpanan informasi *removable* digunakan sebagai media *backup* informasi maka pegawai harus melindungi media penyimpanan informasi *removable* tersebut pada tempat penyimpanan yang aman dan terkendali.

j. Masa kadaluarsa media penyimpanan informasi *removable* harus dipastikan lebih lama dari masa retensi informasi yang tersimpan. Apabila tidak dimungkinkan maka media-media penyimpanan informasi *removable* harus dilakukan pembaharuan secara berkala.

k. Dalam melakukan transfer data menggunakan *removable media* harus mengikuti aturan teknis penggunaan dan memastikan data yang ditransfer maupun hasil transfer tidak terjadi kerusakan.

6. Penyimpanan Aset Informasi:

a. Informasi dengan aset klasifikasi sangat rahasia, rahasia, terbatas, dan publik dalam bentuk *soft copy* yang tersimpan di media *backup* harus disimpan di tempat yang aman. Informasi tersebut tidak boleh disimpan dalam komputer atau jaringan komputer yang dapat diakses tanpa ijin Pembuat Informasi (*Originator)* atau Pemelihara Informasi (*Custodian)* kecuali dilakukan enkripsi.

b. Periode waktu penyimpanan data *(data retention)* ditentukan oleh *Business Process Owner*, dengan mengacu kepada Peraturan Lembaga tentang Jadwal Retensi Arsip di Lingkungan LAPAN. Secara umum data penting berada di dalam sistem selama 5 (lima) tahun dan setelah itu data dipindahkan ke unit kearsipan satu atau yang disebut dengan kearsipan pusat untuk dimusnahkan sesuai dengan ketentuan dan prosedur yang berlaku.

7. Pemusnahan Aset Informasi:

a. Aset informasi dengan pertimbangan waktu penggunaan, kegunaan, dan situasi serta kondisi telah diputuskan untuk dimusnahkan, maka pemusnahannya harus dilakukan sesuai prosedur yang berlaku di LAPAN.

b. Jika informasi yang berklasifikasi sangat rahasia, rahasia dan terbatas, akan dimusnahkan maka proses pemusnahan data informasi harus bersifat total dengan menggunakan teknik/perangkat yang dapat menjamin bahwa seluruh informasi tadi tidak dapat di akses lagi, dan dituangkan dalam berita acara.

c. Jika pemusnahan data informasi di atas dalam prosesnya tidak dapat dimusnahkan secara total, maka dilakukan pemusnahan media penyimpanan secara fisik.

d. Informasi dengan klasifikasi publik pemusnahannya cukup dengan cara menghapus datanya saja atau diformat sehingga medianya masih dapat digunakan untuk keperluan lain.

8. Perjanjian Pertukaran Informasi:

a. Perjanjian Pertukaran Informasi harus dibuat sebelum pihak ketiga mempertukarkan informasi dengan klasifikasi sangat rahasia, rahasia dan terbatas milik LAPAN.

b. Perjanjian Pertukaran Informasi berupa:

1) Konfirmasi awal antara calon pemberi informasi dan calon penerima informasi yang harus dilakukan secara tertulis atau menggunakan kode elektronik.

2) Perjanjian kerahasiaan yang harus terlebih dahulu ditandatangani oleh calon penerima informasi sebelum informasi tersebut diberikan/dikirimkan.

6. PENGENDALIAN AKSES

6.1 Tujuan

Pengendalian akses bertujuan untuk memastikan otorisasi akses pengguna dan mencegah akses pihak yang tidak berwenang terhadap aset informasi dan fasilitas pengolahannya.

6.2 Ruang Lingkup

Kebijakan dan standar pengendalian akses ini meliputi:

1. Persyaratan untuk pengendalian akses;
2. Pengelolaan akses pengguna;
3. Tanggung jawab pengguna;
4. Pengendalian akses jaringan;
5. Pengendalian akses ke sistem operasi; dan
6. Pengendalian akses ke aplikasi dan sistem informasi.

6.3 Kebijakan

1. Persyaratan untuk Pengendalian Akses
   a. CISO LAPAN bertanggung jawab dalam menyusun, mendokumentasikan, dan mengkaji ketentuan akses ke aset informasi berdasarkan kebutuhan organisasi dan persyaratan Keamanan Informasi di lingkungan LAPAN.
   b. CISO Satuan Kerja bertanggung jawab dalam menyusun, mendokumentasikan, dan mengkaji ketentuan akses ke aset informasi berdasarkan kebutuhan organisasi dan persyaratan Keamanan Informasi di lingkungan Satuan Kerja masing-masing.
2. Pengelolaan Akses Pengguna:
   a. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab menyusun prosedur pengelolaan hak akses pengguna sesuai dengan peruntukannya sesuai dengan kewenangan masing-masing.
   b. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab membatasi dan mengendalikan hak akses khusus, sesuai dengan kewenangan masing-masing.
   c. Pengelolaan kata sandi pengguna:
      1) CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mengatur pengelolaan kata sandi pengguna sesuai dengan kewenangan masing-masing; dan
      2) Ketentuan pengelolaan kata sandi pengguna sesuai dengan standar akan diatur dalam Peraturan Lembaga.
   d. Kajian hak akses pengguna:
      CISO LAPAN dan CISO Satuan Kerja bertanggung jawab untuk memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya sesuai dengan kewenangan masing-masing.
3. Tanggung Jawab Pengguna:
   a. Pengguna harus mematuhi aturan pembuatan dan penggunaan kata sandi. Ketentuan tanggung jawab pengguna terhadap kata sandi sesuai dengan standar tanggung jawab pengguna akan diatur dalam Peraturan Lembaga.
   b. Pengguna harus memastikan fasilitas pengolah informasi yang digunakan mendapatkan perlindungan terutama pada saat ditinggalkan; dan

c. Pengguna harus melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang.

4. Pengendalian Akses Jaringan

a. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mengkoordinasikan pengelolaan akses pengguna jaringan/internet. Ketentuan akses pengguna jaringan/internet akan diatur dalam Peraturan Lembaga.

b. CISO LAPAN dan CISO Satuan Kerja harus menerapkan proses otorisasi pengguna untuk setiap akses ke dalam jaringan internal melalui koneksi eksternal (*remote access*) sesuai dengan kewenangan masing-masing.

c. Perlindungan terhadap diagnosa jarak jauh dan konfigurasi *port:*

1) Akses ke perangkat keras dan perangkat lunak untuk diagnosa harus dikendalikan berdasarkan prosedur dan hanya digunakan oleh pegawai yang berwenang untuk melakukan pengujian, pemecahan masalah, dan pengembangan sistem; dan

2) *Port* pada fasilitas jaringan yang tidak dibutuhkan dalam kegiatan atau fungsi layanan harus dinonaktifkan.

d. CISO LAPAN dan CISO Satuan Kerja harus menerapkan mekanisme pengendalian akses pengguna sesuai dengan kewenangan masing-masing sesuai dengan persyaratan pengendalian akses.

e. Pengendalian *routing* jaringan internal LAPAN harus dilakukan sesuai pengendalian akses dan kebutuhan layanan informasi.

5. Pengendalian Akses ke Sistem Operasi:

a. Akses ke sistem operasi harus dikontrol dengan menggunakan prosedur akses yang aman.

b. Identifikasi dan otorisasi pengguna

1) Setiap pengguna harus memililki akun yang unik dan hanya digunakan sesuai dengan peruntukannya; dan

2) Proses otorisasi pengguna harus menggunakan teknik autentikasi yang sesuai untuk memvalidasi identitas dari pengguna.

c. Sistem pengelolaan kata sandi harus mudah digunakan dan dapat memastikan kualitas kata sandi yang dibuat pengguna.

d. CISO LAPAN dan CISO Satuan Kerja harus membatasi dan mengendalikan penggunaan *system utilities* sesuai dengan kewenangan masing-masing. *System Utilities* meliputi sebuah sistem perangkat lunak yang melakukan suatu tugas/fungsi yang sangat spesifik, biasanya disediakan oleh sistem operasi, dan berkaitan dengan pengelolaan sumber daya sistem (*system resources*), seperti *memory*, *disk*, *printer*, dan sebagainya.

e. Fasilitas *session time-out* harus diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu.

f. CISO LAPAN dan CISO Satuan Kerja harus membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA sesuai dengan kewenangan masing-masing.

6. Pengendalian Akses ke Aplikasi dan Sistem Informasi:

a. CISO LAPAN dan CISO Satuan Kerja harus memastikan bahwa akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai peruntukannya.

b. Proses otorisasi pengguna harus menggunakan teknik autentikasi yang sesuai untuk memvalidasi identitas dari pengguna.

c. Aplikasi dan sistem informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus diletakkan pada lokasi terpisah untuk mengurangi kemungkinan diakses oleh pihak yang tidak berwenang.

6.4 STANDAR

1. Persyaratan untuk pengendalian akses mencakup:

a. Penentuan kebutuhan keamanan dari pengolah aset informasi; dan

b. Pemisahan peran pengendalian akses, seperti administrasi akses dan otorisasi akses.

2. Pengelolaan Akses Pengguna harus mencakup:

a. 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 diperbolehkan untuk kegiatan atau alasan operasional, dan harus disetujui oleh Kepala Satuan Kerja serta didokumentasikan. Akun Khusus

diberikan oleh unit Pengelola TI sesuai kebutuhan tetapi tidak terbatas pada pengelolaan TI (baik berupa aplikasi atau sistem), dan kelompok kerja (baik berupa acara kedinasan, tim, atau Satuan Kerja).

b. Pemeriksaan bahwa pengguna memiliki otorisasi dari pemilik sistem untuk menggunakan sistem informasi atau layanan, dan jika diperlukan harus mendapat persetujuan yang terpisah dari Kepala Satuan Kerja.
c. Pemeriksaan bahwa tingkat akses yang diberikan sesuai dengan tujuan kegiatan dan konsisten dengan Kebijakan dan Standar SMPI LAPAN;
d. Pemberian pernyataan tertulis kepada pengguna tentang hak aksesnya dan meminta pengguna menandatangani pernyataan ketentuan akses tersebut;
e. Pemastian penyedia layanan tidak memberikan akses kepada pengguna sebelum prosedur otorisasi telah selesai;
f. Pemeliharaan catatan pengguna layanan yang terdaftar dalam menggunakan layanan;
g. Penghapusan atau penonaktifan akses pengguna yang telah berubah tugas dan/atau fungsinya, setelah penugasan berakhir atau mutasi;
h. Pemeriksaan, penghapusan, serta penonaktifan akun secara berkala dan untuk pengguna yang memiliki lebih dari 1 (satu) akun; dan
i. Memastikan bahwa akun tidak digunakan oleh pengguna lain.

3. Pengelolaan hak akses khusus harus mempertimbangkan:
   a. Hak akses khusus setiap sistem dari pabrikan perlu diidentifikasi untuk dialokasikan/diberikan kepada pengguna yang terkait dengan produk, seperti sistem operasi, sistem informasi, dan aplikasi;
   b. Hak akses khusus hanya diberikan kepada pengguna sesuai dengan peruntukkannya berdasarkan kebutuhan dan kegiatan tertentu;
   c. 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;

d. Pengembangan dan penggunaan sistem rutin (misal *job scheduling*) harus diutamakan untuk menghindari kebutuhan dalam memberikan hak akses khusus secara terus menerus kepada pengguna; dan
e. Hak akses khusus harus diberikan secara terpisah dari akun yang digunakan untuk kegiatan umum, seperti akun *system administrator*, *database administrator*, dan *network administrator*.

4. Kajian hak akses pengguna harus mempertimbangkan:
   a. Hak akses pengguna harus dikaji paling sedikit 6 (enam) bulan sekali atau setelah terjadi perubahan pada sistem, atau struktur organisasi;
   b. 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; dan
   c. Pemeriksaan hak akses khusus harus dilakukan secara berkala, untuk memastikan pemberian hak akses khusus telah diotorisasi.
5. Pengendalian Akses Jaringan dilakukan dengan:
   a. Menerapkan prosedur otorisasi untuk pemberian akses ke jaringan dan layanan jaringan;
   b. Menerapkan teknik autentikasi akses dari koneksi eksternal, seperti teknik kriptografi, *token hardware*, dan *dial-back*; dan
   c. Melakukan penghentian/isolasi layanan jaringan pada area jaringan yang mengalami insiden Keamanan Informasi.

7. PENGENDALIAN TERHADAP PENERAPAN KRIPTOGRAFI

7.1 Tujuan

Pengendalian terhadap penerapan kriptografi bertujuan menambah jaminan dalam perlindungan kerahasiaan, keautentikan dan integritas informasi.

7.2 Ruang Lingkup

Kebijakan dan standar penerapan kriptografi meliputi:

1. Penentuan kondisi yang mengharuskan penerapan kriptografi; dan
2. Persyaratan penerapan kriptografi dan kunci kriptografi.

7.3 Kebijakan

1. CISO LAPAN dan CISO Satuan Kerja harus mengembangkan dan/atau menerapkan sistem kriptografi untuk perlindungan informasi dan membuat rekomendasi yang tepat untuk penerapannya; dan
2. Sistem kriptografi harus digunakan untuk melindungi aset informasi yang memiliki klasifikasi SANGAT RAHASIA, RAHASIA, dan TERBATAS.

7.4 Standar

Pengembangan dan/atau 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, dan tingkat perlindungan yang dibutuhkan;
2. Tingkat perlindungan yang dibutuhkan harus diidentifikasi berdasarkan penilaian risiko, dengan mempertimbangkan jenis, kekuatan, dan kualitas dari algoritma enkripsi yang akan digunakan;
3. Keperluan enkripsi untuk perlindungan informasi SANGAT RAHASIA, RAHASIA dan TERBATAS yang melalui perangkat *mobile computing*, *removable media*, atau jalur komunikasi;
4. Kemudahan dan teknologi yang diperlukan dalam pengelolaan kunci kriptografi, seperti perlindungan kunci kriptografi, siklus hidup kunci kriptografi, dan pemulihan informasi terenkripsi dalam hal kehilangan atau kerusakan kunci kriptografi; dan

5. Dampak penggunaan informasi terenkripsi, seperti pengendalian terkait pemeriksaan suatu konten, dan kecepatan pemrosesan pada sistem.

8. PENGENDALIAN PENGELOLAAN PENGAMANAN FISIK DAN LINGKUNGAN

8.1 Tujuan

Pengendalian pengelolaan pengamanan fisik dan lingkungan bertujuan mencegah akses fisik oleh pihak yang tidak berwenang, menghindari terjadinya kerusakan dan insiden terhadap informasi organisasi dan fasilitas pengolahannya.

8.2 Ruang Lingkup

Kebijakan dan standar pengendalian dan pengelolaan pengamanan fisik dan lingkungan meliputi:

1. Pengamanan area; dan
2. Pengamanan perangkat.

8.3 Kebijakan

1. Pengamanan Area
   a. Seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan LAPAN harus mematuhi aturan yang berlaku di LAPAN.
   b. Ketentuan tentang pengamanan area lingkungan kerja di LAPAN akan diatur dalam Peraturan Lembaga.
2. Pengamanan Perangkat:
   a. Perangkat pengolah informasi dan perangkat pendukung harus ditempatkan di lokasi yang aman dan diposisikan sedemikian rupa untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang.
   b. Perangkat pendukung harus dipasang untuk menjamin beroperasinya perangkat pengolah informasi dan secara berkala harus diperiksa dan diuji ulang kinerjanya.
   c. Pengamanan kabel
      1) Kabel sumber daya listrik harus dilindungi dari kerusakan; dan
      2) Kabel telekomunikasi yang mengalirkan informasi harus dilindungi dari kerusakan dan penyadapan.
   d. Perangkat harus dipelihara secara berkala untuk menjamin ketersediaan, keutuhannya (*integrity*), dan fungsinya.

e. Penggunaan perangkat yang dibawa ke luar dari lingkungan LAPAN harus disetujui oleh pejabat yang berwenang.

f. Pengamanan penggunaan kembali atau penghapusan atau pemusnahan perangkat:

1) Perangkat pengolah informasi penyimpan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dihapuskan atau dimusnahkan; dan

2) Ketentuan penanganan perangkat pengolah informasi penyimpan data di LAPAN sesuai dengan standar penanganan media penyimpan data akan diatur dalam Peraturan Lembaga.

g. Pengamanan perangkat yang tidak dalam pengawasan pengguna harus memiliki perlindungan yang tepat terhadap akses oleh pihak yang tidak berwenang.

h. Kebersihan meja kerja dan layar
Ketentuan terkait kebersihan meja kerja serta layar dari informasi penting perlu disusun dan diterapkan.

8.4 Standar

Pengamanan Area dan Perangkat:

1. Pemeliharaan terhadap perangkat keras atau perangkat lunak dilakukan hanya oleh pegawai yang berwenang. Perangkat harus dipelihara sesuai dengan petunjuk manual dan parameter keamanannya.
2. Untuk pemeliharaan yang dilakukan oleh pihak ketiga, harus diadakan Perjanjian Tingkat Layanan *(Service Level Agreement/ SLA)* yang mendefinisikan parameter keamanan, tingkat pemeliharaan yang disediakan dan tingkat kinerja yang harus dipenuhi pihak ketiga.
3. Akses ke ruang *server,* pusat data, 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, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus didampingi pegawai yang berwenang sepanjang waktu kunjungan. Waktu masuk dan keluar serta maksud kedatangan harus dicatat dan didokumentasikan.

5. Pengamanan kantor, ruangan dan fasilitas mencakup:
   a. Pengamanan kantor, ruangan, dan fasilitas harus sesuai dengan prosedur pengamanan area;
   b. Fasilitas utama harus ditempatkan khusus untuk menghindari akses publik. Fasilitas Utama adalah sarana utama gedung atau bangunan, seperti: pusat kontrol listrik, dan CCTV;
   c. Pembatasan pemberian identitas atau tanda-tanda keberadaan aktivitas pengolahan informasi; dan
   d. Direktori dan buku telepon internal yang mengidentifikasi lokasi perangkat pengolah informasi tidak mudah diakses oleh publik.
6. Perlindungan terhadap ancaman eksternal dan lingkungan harus mempertimbangkan:
   a. Bahan-bahan berbahaya atau mudah terbakar harus disimpan pada jarak yang aman dari *secure areas;*
   b. Perangkat *fallback* dan media *backup* harus diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama;
   c. Perangkat pemadam kebakaran harus disediakan dan diletakkan di tempat yang tepat; dan
   d. Perlindungan terhadap ancaman eksternal dan lingkungan meliputi bencana alam, serangan berbahaya *(malicious attack)*, dan kecelakaan kerja.
7. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab 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;
8. Pegawai dan pihak ketiga tidak diizinkan merokok, makan, minum di ruang *server* dan pusat data;
9. Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dilindungi secara memadai;
10. Dalam hal pemeliharaan perangkat tidak dapat dilakukan di tempat, maka pemindahan perangkat harus mendapatkan persetujuan pejabat yang berwenang terhadap data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA yang disimpan dalam perangkat tersebut harus dipindahkan terlebih dahulu;

11. Otorisasi penggunaan perangkat harus dilakukan secara tertulis dan data yang terkait dengan aset informasi yang digunakan, seperti nama pemakai aset, lokasi, dan tujuan penggunaan aset, harus dicatat dan disimpan;
12. 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;
13. 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 untuk mengurangi tingkat perlindungan atau perlakuan standar yang perlu dilakukan;
    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 elektromagnetik, 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.
14. Pengamanan 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. *Conduit* berupa sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja;
c. Pemisahan antara kabel sumber daya listrik dengan kabel telekomunikasi untuk mencegah interferensi;
d. Penandaan atau 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:
    1) Menggunaan *conduit*;
    2) Penggunaan ruangan terkunci pada tempat inspeksi dan titik pemutusan kabel;
    3) Penggunaan rute alternatif dan/atau media transmisi yang menyediakan keamanan yang sesuai;
    4) Penggunaan kabel serat optic *(fiber optic)*;
    5) Penggunaan lapisan elektromagnet untuk melindungi kabel;
    6) Inisiasi penghapusan teknikal *(technical sweeps)* dan pemeriksaan secara fisik untuk peralatan yang tidak diotorisasi saat akan disambungkan ke kabel; dan
    7) Penerapan akses kontrol ke panel *patch* dan ruangan kabel.

9. PENGENDALIAN PENGELOLAAN PENGAMANAN OPERASIONAL

9.1 Tujuan

Pengendalian pengelolaan pengamanan operasional bertujuan memastikan keamanan dalam pengoperasian fasilitas pengolahan informasi yang berada di lingkungan LAPAN.

9.2 Ruang Lingkup

Kebijakan dan standar pengendalian pengelolaan pengamanan operasional meliputi:

1. Prosedur operasional dan tanggung jawab;
2. Perlindungan terhadap *malware*;
3. *Information backup*;
4. *Logging* dan pemantauan;
5. Pengendalian instalasi perangkat lunak pada sistem operasional;
6. Pengelolaan kerentanan teknis; dan
7. Audit operasional.

9.3 Kebijakan

1. Prosedur Operasional dan Tanggung Jawab
   a. Dokumentasi prosedur operasional

      CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mendokumentasikan, memelihara, dan menyediakan seluruh prosedur operasional yang terkait dengan penggunaan perangkat pengolah informasi bagi pengguna sesuai dengan peruntukannya dan sesuai dengan kewenangan masing-masing.

   b. Pengelolaan perubahan perangkat TI

      CISO LAPAN dan CISO Satuan Kerja harus mengendalikan perubahan terhadap organisasi, proses bisnis, fasilitas pengolah informasi dan sistem yang mempengaruhi Pengamanan Informasi sesuai dengan kewenangan masing-masing. Pengelolaan perubahan layanan TI di LAPAN akan diatur dalam Peraturan Lembaga.

   c. Pengelolaan kapasitas

      CISO LAPAN dan CISO Satuan Kerja harus memastikan adanya pemantauan dan pengelolaan penggunaan sumber daya TI sesuai dengan kewenangan masing-masing serta menyusun proyeksi penggunaan sumber daya TI di masa mendatang, untuk menjamin ketersediaan layanan TI dalam hal pemrosesan dan penyimpanan informasi.

d. CISO LAPAN dan CISO Satuan Kerja harus memastikan adanya pemisahan perangkat pengembangan, pengujian, dan operasional sesuai dengan kewenangan masing-masing untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berwenang terhadap sistem operasional.

2. Perlindungan Terhadap *Malware*

a. CISO LAPAN dan CISO Satuan Kerja harus menerapkan sistem yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman perangkat lunak berbahaya (*malware*) serta dikomunikasikan kepada pengguna sebagai bentuk kepedulian terhadap Keamanan Informasi.

b. Ketentuan perlindungan terhadap ancaman perangkat lunak berbahaya (*malware*) di LAPAN akan diatur dalam Peraturan Lembaga.

3. *Information Backup*

a. CISO LAPAN dan CISO Satuan Kerja harus memastikan adanya kegiatan *information backup*, perangkat lunak dan sistem yang berada di Pusat Data secara berkala sesuai dengan kebutuhan masing-masing.

b. Ketentuan proses *backup* di LAPAN sesuai dengan standar *backup* data akan diatur dalam Peraturan Lembaga.

4. *Logging* dan Pemantauan

a. *Event logging*

CISO LAPAN dan CISO Satuan Kerja harus memastikan adanya pengaktifan dan peninjauan rutin terhadap *event logging* yang mencatat aktivitas pengguna, pengecualian, dan kejadian Keamanan Informasi sesuai dengan kewenangan masing-masing.

b. Pencatatan kesalahan (*fault logging*)

CISO LAPAN dan CISO Satuan Kerja harus menerapkan pencatatan kesalahan (*fault logging*) untuk dianalisis dan diambil tindakan penanganan yang tepat sesuai dengan kewenangan masing-masing.

c. Memantau penggunaan sistem

CISO LAPAN dan CISO Satuan Kerja harus memastikan adanya pemantauan penggunaan sistem dan mengkaji secara berkala hasil kegiatan pemantauan sesuai dengan kewenangan masing-masing.

d. Perlindungan terhadap informasi *log*

CISO LAPAN dan CISO Satuan Kerja harus memastikan perlindungan terhadap fasilitas *logging* dan informasi *log* agar terhindar dari kerusakan dan akses oleh pihak yang tidak berwenang.

e. Pencatatan *log system administrator* dan *system operator*

CISO LAPAN dan CISO Satuan Kerja harus memastikan agar kegiatan *system administrator* dan *system operator* tercatat di dalam *log* dan dikaji secara berkala.

f. Sinkronisasi waktu

CISO LAPAN dan CISO Satuan Kerja harus memastikan semua fasilitas pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati sesuai dengan kewenangan masing-masing.

5. CISO LAPAN dan CISO Satuan Kerja harus mengimplementasikan prosedur untuk pengendalian instalasi perangkat lunak pada sistem operasional.

6. Pengelolaan Kerentanan Teknis:

a. CISO LAPAN dan CISO Satuan Kerja harus memastikan adanya kegiatan pengumpulan informasi kerentanan teknis secara berkala dari seluruh sistem informasi yang digunakan maupun komponen pendukung sistem informasi sesuai dengan kewenangan masing-masing.

b. CISO LAPAN dan CISO Satuan Kerja harus memastikan adanya kegiatan evaluasi dan penilaian risiko terhadap kerentanan teknis yang ditemukan dalam sistem informasi serta menetapkan pengendalian yang tepat terhadap risiko terkait sesuai dengan kewenangan masing-masing.

c. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mengatur batasan instalasi *software* yang dilakukan oleh user sesuai dengan kewenangan masing-masing.

7. Audit yang mencakup verifikasi terhadap fasilitas pemrosesan informasi harus direncanakan dan disepakati dengan pihak terkait sehingga gangguan terhadap proses bisnis dapat diminimalisasi.

9.4 Standar

1. Prosedur operasional antara lain:
   a. Tata cara pengolahan dan penanganan informasi;
   b. Tata cara menangani kesalahan-kesalahan atau kondisi khusus yang terjadi beserta pihak yang harus dihubungi bila mengalami kesulitan teknis;
   c. Cara memfungsikan kembali perangkat dan cara mengembalikan perangkat ke keadaan awal saat terjadi kegagalan sistem;
   d. Tata cara *backup* dan *restore*; dan
   e. Tata cara pengelolaan jejak audit (*audit trails*) pengguna dan catatan kejadian atau kegiatan sistem. Jejak Audit (*Audit Trails*) berupa urutan kronologis catatan audit yang berkaitan dengan pelaksanaan suatu kegiatan.
2. Pemisahan perangkat pengembangan dan operasional harus mempertimbangkan:
   a. Pengembangan dan operasional perangkat lunak harus dioperasikan di sistem atau *processor* komputer dan domain atau direktori yang berbeda;
   b. Prosedur rilis dari pengembangan perangkat lunak ke operasional harus ditetapkan dan didokumentasikan;
   c. *Compiler*, *editor*, dan alat bantu pengembangan lain tidak boleh diakses dari sistem operasional ketika tidak dibutuhkan;
   d. Lingkungan sistem pengujian harus diusahakan sama dengan lingkungan sistem operasional;
   e. 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
   f. Informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA tidak boleh disalin ke dalam lingkungan pengujian sistem.
3. Prosedur *logging* dan pemantauan penggunaan sistem pengolah informasi ditetapkan untuk menjamin agar kegiatan akses yang tidak sah tidak terjadi. Prosedur ini mencakup pemantauan:
   a. Kegagalan akses (*access failures*);
   b. Pola-pola *log-on* yang mengindikasikan penggunaan yang tidak wajar;

c. Alokasi dan penggunaan hak akses khusus (*privileged access capability*);
d. Penelusuran transaksi dan pengiriman file tertentu yang mencurigakan; dan
e. Penggunaan sumber daya sensitif.

4. Prosedur pengendalian instalasi perangkat lunak pada sistem operasional mencakup:
   a. Pengendalian akses terhadap perangkat lunak sebelum dilakukan *deployment;*
   b. Petunjuk *deployment*, penggunaan lisensi, pengoperasian dan pemeliharaan perangkat lunak.
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 mengidentifikasi dan 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 insiden tersebut melalui pelaporan insiden 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:
      1) Mematikan *patch* yang berhubungan dengan kerentanan;
      2) Menambahkan pengendalian akses seperti *firewall;*
      3) Meningkatkan pengawasan untuk mengidentifikasi atau mencegah terjadinya serangan atau kejadian; dan
      4) Meningkatkan kepedulian terhadap kerentanan teknis;
   e. Penyimpanan *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.

6. Prosedur audit operasional dengan mencakup kegiatan verifikasi operasional harus disusun yang mencakup hal-hal sebagai berikut:
   a. Proses perencanaan audit;
   b. Proses pelaksanaan audit;
   c. Proses pelaporan dan pemantauan tindak lanjut audit; dan
   d. Persyaratan auditor.

10. PENGENDALIAN PENGAMANAN KOMUNIKASI

10.1 Tujuan

Pengendalian pengamanan komunikasi bertujuan memberikan perlindungan terhadap informasi yang ditransmisikan melalui jaringan komunikasi beserta fasilitas pengolahannya yang berada di lingkungan LAPAN.

10.2 Ruang Lingkup

Kebijakan pengendalian pengamanan komunikasi ini meliputi:

1. Pengelolaan pengamanan jaringan; dan
2. Pengamanan dalam transfer Informasi.

10.3 Kebijakan

1. Pengelolaan pengamanan jaringan:
   a. Pengendalian jaringan

      CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mengelola dan mengontrol jaringan untuk melindungi informasi pada sistem dan aplikasi; dan
   b. Pengamanan layanan jaringan

      CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mengidentifikasi mekanisme pengamanan, tingkat layanan dan kebutuhan pengelolaan jaringan serta mencantumkannya dalam kesepakatan penyediaan layanan jaringan yang disediakan oleh pihak ketiga.
   c. Pemisahan dalam jaringan

      CISO LAPAN dan CISO Satuan Kerja bertanggung jawab memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi sesuai dengan kewenangan masing-masing.
2. Pengamanan dalam transfer informasi
   a. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mengatur transfer informasi dan membuat prosedur transfer informasi.
   b. Pertukaran informasi dan perangkat lunak antara LAPAN dengan pihak ketiga hanya akan dilakukan atas kesepakatan tertulis kedua belah pihak.
   c. CISO LAPAN dan CISO Satuan Kerja harus menerapkan pengendalian pengamanan informasi untuk pengiriman informasi melalui surat elektronik atau pengiriman informasi melalui jasa layanan pengiriman dalam rangka menghindari akses pihak yang tidak berwenang.

d. Perjanjian kerahasiaan harus diidentifikasi, dikaji dan didokumentasikan untuk melindungi informasi.

e. Ketentuan rinci pertukaran informasi di LAPAN diuraikan dalam standar pengamanan dalam transfer informasi.

10.4 STANDAR

1. Pengelolaan pengamanan jaringan mencakup:
   a. Pemantauan kegiatan pengelolaan jaringan untuk menjamin bahwa perangkat jaringan digunakan secara efektif dan efisien;
   b. Pengendalian dan pengaturan tentang penyambungan atau perluasan jaringan internal atau eksternal LAPAN;
   c. Pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal LAPAN;
   d. Pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan LAPAN dan menerapkan pemantauan serta pencatatan kegiatan selama menggunakan jaringan;
   e. Pemutusan layanan tanpa pemberitahuan sebelumnya jika terjadi insiden Keamanan Informasi;
   f. Perlindungan jaringan dari akses yang tidak berwenang mencakup:
      1) Penetapan untuk penanggung jawab pengelolaan jaringan dipisahkan dari pengelolaan perangkat pengolah informasi;
      2) Penerapan pengendalian khusus untuk melindungi keutuhan informasi yang melewati jaringan umum antara lain dengan penggunaan enkripsi dan tanda tangan elektronik (*digital signature*); dan
      3) Pendokumentasian arsitektur jaringan seluruh komponen perangkat keras jaringan dan perangkat lunak.
   g. Penerapan pengamanan layanan jaringan mencakup:
      1) Teknologi pengamanan seperti autentikasi, enkripsi, dan pengendalian sambungan jaringan;
      2) Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan pengamanan dan aturan koneksi jaringan; dan
      3) Prosedur untuk penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.
   h. 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 tanpa bisa terhubung ke jaringan internal LAPAN.

2. Pengamanan dalam transfer informasi
   a. Prosedur pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
      1) Perlindungan pertukaran informasi dari pencegatan, penyalinan, modifikasi, *miss-routing*, dan perusakan;
      2) Pendeteksian dan perlindungan terhadap kode berbahaya yang dapat dikirim melalui penggunaan komunikasi elektronik;
      3) Perlindungan informasi elektronik dalam bentuk *attachment* yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA; dan
      4) 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:
      1) Pencegahan terhadap penyalahgunaan wewenang pegawai dan/atau pihak ketiga yang dapat membahayakan organisasi;
      2) Penggunaan teknik kriptografi;
      3) Penyelenggaraan penyimpanan dan penghapusan atau pemusnahan untuk semua korespondensi kegiatan, termasuk pesan, yang sesuai dengan ketentuan yang berlaku;
      4) Larangan meninggalkan informasi sensitif pada perangkat pengolah informasi;
      5) Pembatasan penerusan informasi secara otomatis;
      6) Peningkatan kepedulian atas ancaman pencurian informasi, misalnya terhadap:
         a) Pengungkapan informasi sensitif untuk menghindari mencuri dengar (penyadapan) saat melakukan panggilan telepon;
         b) Akses pesan di luar kewenangannya;
         c) Pemrograman mesin faksimili baik sengaja maupun tidak sengaja untuk mengirim pesan ke nomor tertentu; dan

d) Pengiriman dokumen dan pesan ke tujuan yang salah.

d. Peningkatan kepedulian atas pendaftaran data personal, seperti alamat surat elektronik atau informasi pribadi lainnya untuk menghindari pengumpulan informasi yang tidak sah.

e. Penyediaan informasi internal LAPAN bagi masyarakat umum harus disetujui oleh pemilik informasi dan sesuai dengan ketentuan yang berlaku.

f. Perjanjian kerahasiaan harus memuat unsur-unsur sebagai berikut:

1) Definisi dari informasi yang akan dilindungi;
2) Tanggung jawab dan tindakan penanda-tangan untuk menghindari pengungkapan informasi secara tidak sah;
3) Perlindungan kepemilikan informasi, rahasia organisasi, dan kekayaan intelektual;
4) Izin menggunakan informasi rahasia, dan hak-hak penanda-tangan untuk menggunakan informasi;
5) Hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia;
6) Proses untuk pemberitahuan dan pelaporan dari penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan informasi;
7) Syarat-syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian; dan
8) Tindakan yang akan diambil apabila terjadi pelanggaran terhadap perjanjian tersebut.

11. PENGENDALIAN PENGAMANAN INFORMASI DALAM AKUISISI, PENGEMBANGAN DAN PEMELIHARAAN SISTEM INFORMASI

11.1 Tujuan

Pengendalian Pengamanan Informasi dalam akuisisi, pengembangan, dan pemeliharaan sistem informasi bertujuan memastikan bahwa Pengamanan Informasi merupakan bagian yang terintegrasi dengan sistem informasi, mencegah terjadinya kesalahan, kehilangan, dan modifikasi oleh pihak yang tidak berwenang.

11.2 Ruang Lingkup

Kebijakan pengendalian pengamanan informasi dalam akuisisi, pengembangan dan pemeliharaan sistem informasi meliputi:

1. Persyaratan pengamanan pada sistem informasi;
2. Pengamanan dalam proses pengembangan dan pendukung (*support processes*); dan
3. Pengamanan dalam pengujian data.

11.3 Kebijakan

1. Persyaratan pengamanan pada sistem informasi mencakup setidaknya hal-hal berikut ini:
   a. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab untuk menetapkan dan mendokumentasikan secara jelas persyaratan Pengamanan Informasi yang relevan sebelum pengadaan, pengembangan, atau pemeliharaan sistem informasi baru dan sistem informasi saat ini sesuai dengan kewenangan masing-masing.
   b. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab melindungi informasi dalam layanan aplikasi yang melewati jaringan publik dari kecurangan, perselisihan kontrak, pengungkapan dan modifikasi yang tidak sah.
   c. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab melindungi informasi yang terdapat di dalam transaksi layanan aplikasi untuk mencegah pengiriman data yang tidak sempurna, *miss-routing,* perubahan, pengungkapan, duplikasi dan balasan data atau informasi yang tidak sah.
   d. Proses transaksi layanan aplikasi, mencakup:
      1) Validasi data yang masuk

         Data yang akan dimasukkan ke aplikasi harus diperiksa terlebih dahulu kebenaran dan kesesuaiannya.

2) Pengendalian proses internal

Pada setiap aplikasi harus disertakan proses validasi untuk mendeteksi bahwa proses yang dilakukan adalah benar dan informasi yang dihasilkan utuh dan sesuai dengan yang diharapkan.

3) Validasi data keluaran

Data keluaran aplikasi harus divalidasi untuk memastikan kebenaran data yang dihasilkan.

2. Pengamanan dalam proses pengembangan dan pendukung (*support processes*) mencakup:

a. Kebijakan pengamanan pengembangan perangkat lunak dan sistem operasi

CISO LAPAN harus membuat aturan pengamanan dalam pengembangan perangkat lunak dan sistem operasi.

b. Prosedur pengendalian perubahan sistem operasi

CISO LAPAN dan CISO Satuan Kerja harus mengendalikan perubahan pada sistem operasi sesuai dengan kewenangan masing-masing dengan menggunakan prosedur pengelolaan perubahan.

c. Prosedur pengendalian perubahan pada perangkat lunak

CISO LAPAN dan CISO Satuan Kerja harus mengendalikan perubahan terhadap perangkat lunak sesuai dengan kewenangan masing-masing, baik perangkat lunak yang dikembangkan sendiri maupun pihak ketiga.

d. Kajian teknis aplikasi setelah perubahan sistem operasi dan/atau perangkat lunak

CISO LAPAN dan CISO Satuan Kerja bertanggung jawab untuk meninjau dan menguji sistem operasi dan/atau perangkat lunak untuk memastikan tidak ada dampak merugikan pada proses operasional atau pengamanan informasi LAPAN pada saat terjadi perubahan sistem operasi dan/atau perangkat lunak, terutama pada perangkat lunak yang memproses informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.

e. Pembatasan perubahan paket perangkat lunak

Modifikasi paket perangkat lunak harus dibatasi pada perubahan yang dinilai sangat penting dan dikendalikan secara ketat.

f. Prinsip pengamanan rekayasa perangkat lunak
Prinsip pengamanan rekayasa perangkat lunak harus ditetapkan, didokumentasikan, dipelihara, dan diterapkan pada setiap sistem informasi.

g. Pengamanan lingkungan pengembangan
CISO LAPAN dan CISO Satuan Kerja harus menetapkan lingkungan yang aman untuk seluruh proses siklus hidup proses pengembangan sistem.

h. Pengembangan perangkat lunak oleh pihak ketiga
CISO LAPAN dan CISO Satuan Kerja harus melakukan pendampingan dan pemantauan terhadap pengembangan perangkat lunak oleh pihak ketiga sesuai dengan kewenangan masing-masing.

i. Pengujian Pengamanan sistem
CISO LAPAN dan CISO Satuan Kerja harus memastikan adanya pengujian Pengamanan sistem selama proses pengembangan.

j. Pengujian Penerimaan Sistem
CISO LAPAN dan CISO Satuan Kerja harus memastikan adanya pengujian penerimaan sistem disesuaikan dengan kriteria kebutuhan untuk sistem informasi baru dan pembaharuan versi.

3. Pengamanan data pengujian
Data pengujian harus diseleksi secara ketat, terlindungi, dan terkendali.

11.4 STANDAR

1. Spesifikasi kebutuhan perangkat pengolah informasi yang dikembangkan baik oleh internal maupun pihak ketiga harus didokumentasikan.
2. Standar proses transaksi layanan aplikasi sebagai berikut:
   a. Pemeriksaan data masukan harus mempertimbangkan:
      1) Penerapan masukan rangkap *(dual input)* atau mekanisme pengecekan masukan lainnya untuk mendeteksi kesalahan berikut:
         a) Di luar rentang/batas nilai-nilai yang diperbolehkan;
         b) Karakter tidak valid dalam *field* data;
         c) Data hilang atau tidak lengkap;
         d) Melebihi batas atas dan bawah volume data; dan
         e) Data yang tidak diotorisasi dan tidak konsisten.

2) Pengkajian secara berkala terhadap isi *field* kunci *(key field)* atau *file* data untuk mengkonfirmasi keabsahan dan integritas data;
3) Memeriksa dokumen *hard copy* untuk memastikan tidak adanya perubahan data masukan yang tidak melalui otorisasi;
4) Menampilkan pesan yang sesuai dalam menanggapi kesalahan validasi;
5) Prosedur untuk menguji kewajaran dari data masukan;
6) Menguraikan tanggung jawab dari seluruh pegawai yang terkait dalam proses perekaman data; dan
7) Sistem mampu membuat dari mengeluarkan catatan aktivitas terkait proses perekaman data.

b. Menyusun daftar pemeriksaan (*check list*) yang sesuai, mendokumentasikan proses pemeriksaan, dan menyimpan hasilnya secara aman. Proses pemeriksaan mencakup:
1) Pengendalian *session* atau *batch*, untuk mencocokkan data setelah perubahan transaksi;
2) Pengendalian *balancing* untuk memeriksa data sebelum dan sesudah transaksi;
3) Validasi data masukan yang dimasukkan pada sistem;
4) Keutuhan dan keaslian data yang diunduh/diunggah (*download/upload*);
5) *Hash totals* dari *record* dan *file*;
6) Aplikasi berjalan sesuai dengan rencana dan waktu yang ditentukan;
7) Program dijalankan sesuai urutan yang benar dan dihentikan sementara jika terjadi kegagalan sampai masalah diatasi; dan
8) Sistem mampu membuat dan mengeluarkan catatan aktivitas pengelolaan internal.

c. Pemeriksaan data keluaran harus mempertimbangkan:
1) Kewajaran dari data keluaran yang dihasilkan;
2) Pengendalian rekonsiliasi data untuk memastikan kebenaran pengolahan data;
3) Menyediakan informasi yang cukup untuk pengguna atau sistem pengolahan informasi untuk menentukan akurasi, kelengkapan, ketepatan, dan klasifikasi informasi;
4) Prosedur untuk menindaklanjuti validasi data keluaran;

5) Menguraikan tanggung jawab dari seluruh pegawai yang terkait proses data keluaran; dan
6) Sistem mampu membuat dan mengeluarkan catatan aktivitas dalam proses validasi data keluaran.

3. Pengamanan dalam pengujian data
   a. Pengembangan prosedur pengendalian perangkat lunak pada sistem operasional harus mempertimbangkan:
      1) Proses pemutakhiran perangkat lunak operasional, aplikasi, *library programme* hanya boleh dilakukan oleh *system administrator* terlatih setelah melalui proses otorisasi;
      2) Sistem operasional hanya berisi program aplikasi *executable* yang telah diotorisasi, tidak boleh berisi kode program (*source code*) atau *compiler;*
      3) Aplikasi dan perangkat lunak sistem operasi hanya dapat diimplementasikan setelah melewati proses pengujian yang ekstensif;
      4) Sistem pengendalian konfigurasi harus digunakan untuk mengendalikan seluruh perangkat lunak yang telah diimplementasikan beserta dokumentasi sistem;
      5) Strategi *rollback* harus tersedia sebelum suatu perubahan diimplementasikan;
      6) Catatan audit harus dipelihara untuk menjaga kemutakhiran *library programme* operasional;
      7) Versi lama dari suatu aplikasi harus tetap disimpan untuk keperluan kontingensi; dan
      8) Versi lama dari suatu perangkat lunak harus diarsip, bersama dengan informasi terkait dan prosedur, parameter, konfigurasi rinci, dan perangkat lunak pendukung.
   b. Perlindungan terhadap sistem pengujian data harus mempertimbangkan:
      1) Prosedur pengendalian akses, yang berlaku pada sistem aplikasi operasional, harus berlaku juga pada sistem aplikasi pengujian;
      2) Proses otorisasi setiap kali informasi atau data operasional digunakan pada sistem pengujian;
      3) Penghapusan informasi atau data operasional yang digunakan pada sistem pengujian segera setelah proses pengujian selesai; dan

4) Pencatatan jejak audit penggunaan informasi/data operasional.

c. Pengendalian akses ke kode program (*source code*) harus mempertimbangkan:

1) Kode program (*source code*) tidak boleh disimpan pada sistem operasional;
2) Pengelolaan kode program (*source code*) dan *library* harus mengikuti prosedur yang telah ditetapkan;
3) Pengelola TI tidak boleh memiliki akses yang tidak terbatas ke kode program (*source code*) dan *library*;
4) Proses pemutakhiran kode program (*source code*) dan item terkait, serta pemberian kode program (*source code*) kepada *programmer* hanya dapat dilakukan setelah melalui proses otorisasi;
5) kode program (*source code*) harus disimpan dalam *secure areas*;
6) Catatan audit dari seluruh akses ke kode program (*source code*) *library* harus dipelihara; dan
7) Pemeliharaan dan penyalinan kode program (*source code*) *library* harus mengikuti prosedur pengendalian perubahan.

4. Pengamanan dalam proses pengembangan dan pendukung (*support processes*)

a. Prosedur pengendalian perubahan sistem operasi dan perangkat lunak, mencakup:

1) Memelihara catatan persetujuan sesuai dengan kewenangannya;
2) Memastikan permintaan perubahan diajukan oleh pihak yang berwenang;
3) Melakukan identifikasi terhadap perangkat lunak, informasi, basis data, dan perangkat keras yang perlu diubah;
4) Mendapatkan persetujuan resmi dari pihak yang berwenang sebelum pelaksanaan perubahan;
5) Memastikan pihak yang berwenang menerima perubahan yang diminta sebelum dilakukan implementasi;
6) Memastikan bahwa dokumentasi sistem mutakhir dan dokumen versi lama diarsipkan;
7) Memelihara versi perubahan aplikasi;
8) Memelihara jejak audit perubahan aplikasi;

9) Memastikan dokumentasi penggunaan dan prosedur telah diubah sesuai dengan perubahan yang dilaksanakan; dan
10) Memastikan bahwa implementasi perubahan dilakukan pada waktu yang tepat dan tidak menganggu kegiatan.

b. Prosedur kajian teknis aplikasi setelah perubahan sistem operasi dan/atau perangkat lunak, mencakup:
1) Memastikan rencana dan anggaran *annual support* yang mencakup *review* dan sistem *testing* dari perubahan sistem operasi;
2) Memastikan pemberitahuan perubahan sistem informasi dilakukan dalam jangka waktu yang tepat untuk memastikan tes dan *review* telah dilaksanakan sebelum implementasi; dan
3) Memastikan bahwa perubahan telah diselaraskan dengan rencana kelangsungan kegiatan.

c. Pengembangan perangkat lunak oleh pihak ketiga harus mempertimbangkan:
1) Perjanjian lisensi, kepemilikan kode program (*source code)*, dan Hak Atas Kekayaan Intelektual (HAKI);
2) Perjanjian *escrow* (Jaminan Pelaksanaan);
3) Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan;
4) Persyaratan kontrak mengenai kualitas dan fungsi pengamanan aplikasi;
5) Uji coba terhadap aplikasi untuk memastikan tidak terdapat *malicious code* sebelum implementasi;

12. PENGENDALIAN HUBUNGAN DENGAN PIHAK KETIGA

12.1 Tujuan

Pengendalian hubungan dengan pihak ketiga bertujuan memastikan terlindungnya aset-aset organisasi di lingkungan LAPAN yang dapat diakses oleh pihak ketiga serta mempertahankan tingkat pengamanan informasi dan pelayanan yang telah disepakati dengan pihak ketiga.

12.2 Ruang Lingkup

Kebijakan dan standar pengendalian hubungan dengan pihak ketiga meliputi:

1. Pengendalian hubungan dengan pihak ketiga;
2. Pengamanan Informasi dalam kesepakatan dengan pihak ketiga;
3. Pengkajian terhadap kinerja pihak ketiga; dan
4. Pengelolaan perubahan terhadap layanan yang disediakan oleh pihak ketiga.

12.3 Kebijakan

1. CISO LAPAN dan CISO Satuan Kerja harus menerapkan pengendalian Pengamanan Informasi berdasarkan hasil penilaian risiko untuk mencegah atau mengurangi dampak risiko terkait dengan pemberian akses kepada pihak ketiga sesuai dengan kewenangan masing-masing;
2. CISO LAPAN dan CISO Satuan Kerja harus memastikan bahwa pengendalian Pengamanan Informasi, definisi layanan, dan tingkat layanan yang tercantum dalam kesepakatan penyediaan layanan telah diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga sesuai dengan kewenangan masing-masing;
3. CISO LAPAN dan CISO Satuan Kerja harus memastikan terdapat persyaratan untuk mengatasi risiko Pengamanan Informasi pada kesepakatan dengan pihak ketiga yang berhubungan dengan layanan teknologi informasi serta rantai pasokan produk sesuai dengan kewenangan masing-masing;
4. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab melakukan pemantauan dan kajian terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh pihak ketiga secara berkala sesuai dengan kewenangan masing-masing; dan
5. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab memperhatikan kritikalitas, proses yang terkait, dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan pihak ketiga sesuai dengan kewenangan masing-masing.

12.4 Standar

Standar pemantauan dan pengkajian penyediaan layanan, laporan, dan catatan yang disediakan oleh 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 atau kesepakatan;
3. Pemberian informasi tentang insiden Keamanan Informasi dan pengkajian informasi ini bersama pihak ketiga sebagaimana diatur dalam perjanjian atau kesepakatan;
4. Pemeriksaan jejak audit pihak ketiga dan pencatatan peristiwa keamanan, masalah operasional, kegagalan, dan insiden yang terkait dengan layanan yang diberikan; dan
5. Penyelesaian dan pengelolaan masalah yang teridentifikasi.

13. PENGENDALIAN PENGELOLAAN INSIDEN KEAMANAN INFORMASI

13.1 Tujuan

Pengendalian pengelolaan insiden Keamanan Informasi bertujuan memastikan kejadian dan kelemahan Pengamanan Informasi dapat dikomunikasikan untuk dilakukan perbaikan, serta dilakukan pendekatan yang konsisten dan efektif agar dapat dihindari atau tidak terulang kembali.

13.2 Ruang Lingkup

Kebijakan dan standar pengendalian pengelolaan insiden Keamanan Informasi meliputi pengelolaan insiden Keamanan Informasi dan perbaikannya.

13.3 Kebijakan

1. Prosedur dan tanggung jawab

   CISO LAPAN bertanggung jawab menyusun prosedur dan menguraikan tanggung jawab pegawai, terkait dalam rangka memastikan insiden Keamanan Informasi dapat ditangani secara cepat, efektif dan tertib.
2. Pegawai dan/atau pihak ketiga harus melaporkan kepada CISO LAPAN atau CISO Satuan Kerja, pada saat ditemukan kelemahan dan/atau terjadi insiden Keamanan Informasi dalam sistem atau layanan TI LAPAN. Proses penanganan insiden di LAPAN akan diatur dalam prosedur dan/atau Peraturan Lembaga.
3. Pengkajian terhadap kejadian Keamanan Informasi

   CISO LAPAN dan CISO Satuan Kerja bertanggung jawab melakukan pengkajian terhadap kejadian Keamanan Informasi serta memutuskan dari hasil kajian apakah kejadian tersebut tergolong ke dalam insiden Keamanan Informasi.
4. CISO LAPAN dan CISO Satuan Kerja memastikan bahwa seluruh insiden Keamanan Informasi harus ditanggapi sesuai dengan prosedur penanganan insiden Keamanan Informasi yang berlaku.
5. Peningkatan penanganan insiden Keamanan Informasi
   1) Seluruh insiden Keamanan Informasi yang terjadi dan tindakan mengatasinya harus dicatat dalam suatu basis data dan/atau buku catatan pelaporan insiden Keamanan Informasi, dan akan menjadi masukan pada proses peningkatan penanganan insiden Keamanan Informasi.

2) Seluruh catatan insiden Keamanan Informasi akan dievaluasi dan dianalisa untuk perbaikan dan pencegahan agar insiden Keamanan Informasi tidak terulang.

6. Pengumpulan bukti pelanggaran.

CISO LAPAN dan CISO Satuan Kerja bertanggung jawab untuk mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap Kebijakan dan Standar SMPI LAPAN sesuai dengan kewenangan masing-masing.

13.4 Standar

1. Insiden Keamanan Informasi dan Pelaporan Kejadian:
   a. Insiden Keamanan Informasi antara lain:
      1) Hilangnya layanan, perangkat, atau fasilitas TI;
      2) Kerusakan fungsi sistem atau kelebihan beban;
      3) Perubahan sistem diluar kendali;
      4) Kerusakan fungsi perangkat lunak atau perangkat keras;
      5) Pelanggaran akses ke dalam sistem TI;
      6) Kelalaian manusia; dan
      7) Ketidaksesuaian dengan ketentuan yang berlaku.
   b. Pelaporan insiden harus mencakup:
      1) Proses pemberitahuan penanganan insiden kepada pihak yang melaporkan kejadian insiden Keamanan Informasi;
      2) Formulir laporan insiden Keamanan Informasi untuk mendukung tindakan pelaporan dan membantu pelapor mengingat kronologis kejadian Keamanan Informasi;
      3) Perilaku yang benar dalam menghadapi insiden Keamanan Informasi, antara lain:
         a) Mencatat semua rincian penting insiden dengan segera, seperti jenis pelanggaran, jenis kerusakan, pesan pada layar, atau anomali sistem; dan
         b) Segera melaporkan insiden ke pihak berwenang sebelum melakukan tindakan penanganan sendiri.
      4) Bukti-bukti pendukung sebagai referensi yang digunakan dalam proses penanganan pelanggaran disiplin bagi pegawai dan/atau pihak ketiga yang melakukan pelanggaran Keamanan Informasi.

2. Prosedur Pengelolaan Insiden Keamanan Informasi

Prosedur pengelolaan insiden Keamanan Informasi harus mempertimbangkan:

a. Prosedur yang harus ditetapkan untuk menangani berbagai jenis insiden Keamanan Informasi, mencakup:
   1) Kegagalan sistem informasi dan hilangnya layanan;
   2) Serangan *malicious code;*
   3) Suatu kondisi dimana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang tidak terkendali baik dari dalam maupun dari luar sistem (*denial of service*);
   4) Kesalahan akibat data tidak lengkap atau tidak akurat;
   5) Pelanggaran kerahasiaan dan keutuhan; dan
   6) Penyalahgunaan sistem informasi.

b. Prosedur harus dilengkapi dengan rencana kontingensi, mencakup:
   1) Analisis dan identifikasi penyebab insiden;
   2) Mengkarantina atau membatasi insiden;
   3) Perencanaan dan pelaksanaan tindakan korektif untuk mencegah insiden berulang;
   4) Komunikasi dengan pihak-pihak yang terkena dampak pemulihan insiden; dan
   5) Pelaporan tindakan ke pihak berwenang.

c. Jejak audit dan bukti serupa harus dikumpulkan dan diamankan untuk:
   1) Analisis masalah internal;
   2) Digunakan sebagai bukti forensik yang berkaitan dengan potensi pelanggaran kontrak atau peraturan atau persyaratan dalam hal proses pidana atau perdata; dan
   3) Digunakan sebagai bahan tuntutan ganti rugi pada pihak ketiga yang menyediakan perangkat lunak dan layanan.

d. Tindakan untuk memulihkan keamanan dari pelanggaran dan perbaikan kegagalan sistem harus dikendalikan secara hati-hati, dan prosedur harus memastikan bahwa:
   1) Hanya pegawai yang sudah diidentifikasi dan berwenang yang diizinkan akses langsung ke sistem dan data;
   2) Semua tindakan darurat yang diambil, didokumentasikan secara rinci;
   3) Tindakan darurat dilaporkan kepada pihak berwenang; dan
   4) Keutuhan sistem dan pengendaliannya dikonfirmasikan dengan pihak-pihak terkait sesegera mungkin.

14. PENGENDALIAN ASPEK PENGAMANAN INFORMASI DALAM PENGELOLAAN KELANGSUNGAN KEGIATAN

14.1 Tujuan

Pengendalian aspek Pengamanan Informasi dalam pengelolaan kelangsungan kegiatan bertujuan melindungi aset informasi dan fasilitas pengolahannya, guna memastikan berlangsungnya kegiatan dan layanan pada saat keadaan darurat, serta memastikan pemulihan yang tepat.

14.2 Ruang Lingkup

Kebijakan dan standar aspek Pengamanan Informasi dalam pengelolaan kelangsungan kegiatan ini meliputi:

1. Penyusunan dan penerapan rencana kelangsungan kegiatan (*Business Continuity Plan/BCP*);
2. Menerapkan kelangsungan Pengamanan Informasi;
3. Proses pengelolaan kelangsungan kegiatan;
4. Penilaian risiko dan analisis dampak bisnis *(Business Impact Analysis/BIA);*
5. Pengujian, pengkajian ulang, dan evaluasi rencana kelangsungan kegiatan; dan
6. *Redundancies* (sistem *backup* yang memiliki fungsi yang sama).

14.3 Kebijakan

1. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab menyusun dan menerapkan rencana kelangsungan kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan.
2. CISO LAPAN dan CISO Satuan Kerja harus memelihara dan memastikan rencana-rencana yang termuat dalam rencana kelangsungan kegiatan masih sesuai, dan mengidentifikasi prioritas untuk kegiatan uji coba.
3. CISO LAPAN dan CISO Satuan Kerja harus memastikan adanya kegiatan uji coba rencana kelangsungan kegiatan secara berkala untuk memastikan rencana kelangsungan kegiatan dapat dilaksanakan secara efektif.
4. CISO LAPAN dan CISO Satuan Kerja harus menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol untuk memastikan tingkat kelangsungan

Pengamanan Informasi yang diperlukan selama terjadi situasi yang merugikan.

5. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mengelola proses kelangsungan kegiatan pada saat keadaan darurat di lingkungan kerja masing-masing.
6. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mengidentifikasi risiko, dan menganalisis dampak yang diakibatkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan.
7. Fasilitas pengolahan informasi perlu mengimplementasikan redundansi (*redundancy*) untuk menjamin ketersediaan terhadap data atau informasi organisasi.

14.4 Standar

1. Komponen yang harus diperhatikan dalam mengelola proses kelangsungan kegiatan pada saat keadaan darurat:
   a. Identifikasi risiko dan analisis dampak yang diakibatkan pada saat terjadi keadaan darurat;
   b. Identifikasi seluruh aset informasi yang menunjang proses kegiatan kritikal;
   c. Identifikasi sumber daya mencakup biaya, struktur organisasi, teknis pelaksanaan, pegawai, dan pihak ketiga;
   d. Memastikan keselamatan pegawai, dan perlindungan terhadap perangkat pengolah informasi dan aset organisasi;
   e. Penyusunan dan pendokumentasian rencana kelangsungan kegiatan sesuai dengan Rencana Strategis LAPAN, Rencana Strategis Pusat Teknologi Informasi dan Komunikasi Penerbangan dan Antariksa, dan Rencana Induk Teknologi Informasi LAPAN; dan
   f. Pelaksanaan uji coba dan pemeliharaan rencana kelangsungan kegiatan secara berkala.
2. Proses identifikasi risiko mengikuti ketentuan mengenai Penerapan Manajemen Risiko di Lingkungan LAPAN yang akan diatur dalam Peraturan Lembaga.
3. Proses analisis dampak kegiatan harus melibatkan pemilik proses bisnis dan dievaluasi secara berkala.
4. Penyusunan rencana kelangsungan kegiatan mencakup:
   a. Prosedur saat keadaan darurat, mencakup tindakan yang

harus dilakukan serta pengaturan hubungan dengan pihak berwenang;

b. 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 akan diatur dalam Peraturan Lembaga.
c. Prosedur saat kondisi telah normal *(resumption)*, adalah tindakan mengembalikan kegiatan operasional ke kondisi normal;
d. Jadwal uji coba, mencakup langkah-langkah dan waktu pelaksanaan uji coba serta proses pemeliharaannya;
e. Pelaksanaan pelatihan dan sosialisasi dalam rangka meningkatkan kepedulian dan pemahaman proses kelangsungan kegiatan dan memastikan proses kelangsungan kegiatan dilaksanakan secara efektif;
f. Tanggung jawab dan peran setiap pelaksana pengelolaan proses rencana kelangsungan kegiatan; dan
g. Daftar rencana kebutuhan informasi kritikal dan sumber daya untuk dapat menjalankan prosedur saat keadaan darurat, suatu tindakan pembalikan/menarik diri dari posisi awal (*fallback*) dan saat kondisi telah normal (*resumption*).

5. Uji coba rencana kelangsungan kegiatan harus dilaksanakan untuk memastikan setiap rencana yang disusun dapat dilakukan/dipenuhi pada saat penerapannya. Uji coba rencana kelangsungan kegiatan ini mencakup:
   a. Simulasi diutamakan untuk pengelola proses kelangsungan kegiatan;
   b. Uji coba pemulihan *(recovery)* sistem informasi untuk memastikan sistem informasi dapat berfungsi kembali;
   c. Uji coba proses pemulihan *(recovery)* di lokasi kerja sementara dalam rangka menjalankan proses bisnis secara paralel;
   d. Uji coba terhadap perangkat dan layanan yang disediakan oleh pihak ketiga; dan
   e. Uji coba keseluruhan mulai dari organisasi, petugas, peralatan, perangkat, dan prosesnya.

15. PENGENDALIAN KEPATUHAN

15.1 Tujuan

Pengendalian kepatuhan bertujuan menghindari pelanggaran terhadap peraturan perundang-undangan dan persyaratan lain yang terkait dengan Pengamanan Informasi.

15.2 RUANG LINGKUP

Kebijakan dan standar kepatuhan meliputi:

1. Kepatuhan terhadap peraturan perundang-undangan dan persyaratan lain yang terkait dengan Pengamanan Informasi;
2. Kepatuhan teknis; dan
3. Audit Pengamanan Informasi independen.

15.3 Kebijakan

1. Kepatuhan terhadap Peraturan Perundang-undangan dan persyaratan lain yang terkait dengan Pengamanan Informasi meliputi:
   a. Seluruh pegawai dan pihak ketiga harus menaati peraturan perundangan yang terkait dengan Pengamanan Informasi.
   b. CISO LAPAN dan CISO Satuan Kerja bertanggung jawab mengidentifikasi, mendokumentasikan dan memelihara kemutakhiran semua peraturan Perundang-undangan yang terkait dengan sistem Pengamanan Informasi.
   c. Hak Atas Kekayaan Intelektual:
      1) Perangkat lunak yang digunakan harus mematuhi ketentuan penggunaan lisensi.
      2) Penggandaan perangkat lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran.
   d. Perlindungan terhadap rekaman
      Rekaman milik LAPAN harus dilindungi dari kehilangan, kerusakan atau penyalahgunaan.
   e. Pengamanan data
      1) CISO LAPAN dan CISO Satuan Kerja bertanggung jawab

melindungi kepemilikan dan kerahasiaan data.

2) Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundangan dan kesepakatan.

2. Kepatuhan Teknis

CISO LAPAN dan CISO Satuan Kerja bertanggung jawab melakukan pemeriksaan kepatuhan teknis secara berkala untuk menjamin efektivitas standar dan prosedur Pengamanan Informasi yang ada di area operasional sesuai dengan kewenangan masing-masing.

3. Audit Pengamanan Informasi Independen

a. Pengendalian audit Pengamanan Informasi

Pengelolaan Pengamanan Informasi dan implementasi yang dilakukan oleh LAPAN harus dilakukan audit independen secara berkala atau pada saat terjadi perubahan yang signifikan.

b. Perlindungan terhadap alat bantu (*tools*) audit Pengamanan Informasi.

Penggunaan alat bantu baik perangkat lunak maupun perangkat keras untuk mengetahui kelemahan keamanan, memindai (*scanning*) kata sandi, atau menerobos sistem Pengamanan Informasi tidak diizinkan kecuali atas persetujuan Kepala Satuan Kerja.

15.4 Standar

1. Kepatuhan terhadap Hak Kekayaan Intelektual

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

a. Mendapatkan perangkat lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan hak cipta tidak dilanggar;

b. Memelihara daftar aset informasi dan fasilitas pengolahannya sesuai persyaratan untuk melindungi hak kekayaan intelektual;

c. Memelihara bukti kepemilikan lisensi, *master disk*, buku manual, dan lain sebagainya;

d. Menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;

e. Melakukan pemeriksaan bahwa hanya perangkat lunak dan produk berlisensi yang dipasang;

f. Patuh terhadap syarat dan kondisi untuk perangkat lunak dan informasi yang didapat dari jaringan publik;

g. Dilarang melakukan duplikasi, konversi ke format lain atau mengambil dari rekaman komersial (film atau *audio*), selain yang diperbolehkan oleh Undang-Undang Hak Cipta; dan

h. Tidak menyalin secara penuh atau sebagian buku, artikel, laporan, atau dokumen lainnya, selain yang diizinkan oleh Undang-Undang Hak Cipta.

2. Kepatuhan terhadap Kebijakan dan Standar

Hal yang perlu dilakukan jika terdapat ketidakpatuhan teknis meliputi:

a. Menentukan dan mengevaluasi penyebab ketidakpatuhan;

b. Menentukan tindakan yang perlu dilakukan berdasarkan hasil evaluasi agar ketidakpatuhan tidak terulang kembali;

c. Menentukan dan melaksanakan tindakan perbaikan yang sesuai; dan

d. Mengkaji tindakan perbaikan yang dilakukan.

3. Kepatuhan Teknis

Sistem TI harus diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan perangkat 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.

4. Kepatuhan terkait audit Pengamanan Informasi secara independen

Proses audit Pengamanan Informasi harus memperhatikan hal-hal berikut:

a. Persyaratan audit harus disetujui oleh CISO LAPAN dan/atau CISO Satuan Kerja;

b. Ruang lingkup pemeriksaan/audit harus disetujui dan dikendalikan oleh pihak berwenang;

c. Pemeriksaan perangkat lunak dan data harus dibatasi untuk akses baca saja *(read-only);*

d. Selain akses baca saja hanya diizinkan untuk salinan dari *file* sistem yang diisolasi, yang harus dihapus bila audit telah selesai, atau diberikan perlindungan yang tepat jika ada

kewajiban untuk menyimpan *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 TI yang 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.

KEPALA LEMBAGA PENERBANGAN DAN
ANTARIKSA NASIONAL REPUBLIK INDONESIA,

THOMAS DJAMALUDDIN