BERITA NEGARA REPUBLIK INDONESIA

No.1248, 2020 BAPETEN. Keamanan Informasi. Sistem Manajemen

PERATURAN BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA
NOMOR 8 TAHUN 2020
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN BADAN PENGAWAS TENAGA NUKLIR

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA,

Menimbang : a. bahwa dalam rangka melindungi kerahasiaan, integritas, dan ketersediaan aset informasi Badan Pengawas Tenaga Nuklir dari berbagai bentuk ancaman keamanan informasi baik dari dalam maupun luar lingkungan Badan Pengawas Tenaga Nuklir, perlu melakukan pengaturan pengelolaan keamanan informasi di lingkungan Badan Pengawas Tenaga Nuklir;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Badan Pengawas Tenaga Nuklir tentang Sistem Manajemen Keamanan Informasi di Lingkungan Badan Pengawas Tenaga Nuklir;

Mengingat : 1. Undang-Undang Nomor 10 Tahun 1997 tentang Ketenaganukliran (Lembaran Negara Republik Indonesia Tahun 1997 Nomor 23, Tambahan Lembaran Negara

Republik Indonesia Nomor 3676);

2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
3. Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Departemen sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Presiden Nomor 145 Tahun 2015 tentang perubahan kedelapan Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Departemen (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 322);
4. Keputusan Kepala Badan Pengawas Tenaga Nuklir Nomor 01.Rev.2/K.OTK/V-04 sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Badan Pengawas Tenaga Nuklir Nomor 1 Tahun 2019 tentang Perubahan Kedua atas Keputusan Kepala Badan Pengawas Tenaga Nuklir Nomor 01 Rev.2/K-Otk/V-04 Tahun 2004 tentang Organisasi dan Tata Kerja Badan Pengawas Tenaga Nuklir (Berita Negara Republik Indonesia Tahun 2019 Nomor 27);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN PENGAWAS TENAGA NUKLIR TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN BADAN PENGAWAS TENAGA NUKLIR.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:

1. Aset Informasi adalah aset dalam bentuk data atau dokumen, perangkat lunak, aset fisik, dan aset tak berwujud.
2. Badan adalah Badan Pengawas Tenaga Nuklir.
3. *Chief Information Officer* yang selanjutnya disingkat CIO adalah pejabat pengarah informasi yang dijabat oleh Sekretaris Utama sebagai koordinator penyelenggaraan tata kelola Teknologi Informasi dan Komunikasi di lingkungan Badan.
4. *Chief Information Security Officer* yang selanjutnya disingkat CISO adalah pejabat yang berperan sebagai koordinator dalam pelaksanaan implementasi kebijakan dan standar SMKI di Lingkungan Badan.
5. Keamanan Informasi adalah terjaganya kerahasiaan, keutuhan, dan ketersediaan informasi.
6. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah teknologi untuk mengumpulkan, menyiapkan, menyimpan, mengolah, mengumumkan, menganalisis, mengambil kembali, mengirim atau menerima data dan informasi.
7. Komite TIK adalah komite yang terdiri dari Deputi Perizinan dan Inspeksi, Deputi Pengkajian Keselamatan Nuklir, Manajemen Unit Pengelola TIK, dan Ahli TIK yang dibentuk dengan tujuan untuk memberikan dukungan teknis TIK dalam mendukung pelaksanaan tugas CIO.
8. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen yang meliputi 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.

9. Tim Keamanan Informasi adalah tim yang dibentuk dalam rangka perlindungan terhadap keamanan informasi Badan.
10. Unit Pemilik Proses Bisnis adalah unit kerja yang memiliki aplikasi sistem informasi dan/atau memiliki alat monitoring pengawasan ketenaganukliran.
11. Unit Pengelola TIK adalah unit kerja yang melakukan pengelolaan teknologi informasi dan komunikasi berupa mengumpulkan, menyiapkan, menyimpan, mengolah, mengumumkan, menganalisis, mengambil kembali, mengirim atau menerima data dan informasi.

Pasal 2

Peraturan Badan ini mengatur kebijakan dan standar SMKI yang digunakan sebagai pedoman dalam melindungi keamanan aset informasi milik Badan.

BAB II

PELAKSANA KEAMANAN INFORMASI

Pasal 3

Kebijakan dan standar SMKI sebagaimana dimaksud dalam Pasal 2 dikoordinasikan oleh Sekretaris Utama selaku CIO dan sekaligus CISO.

Pasal 4

(1) Dalam melaksanakan tugasnya, CISO sebagaimana dimaksud dalam Pasal 3 menetapkan Tim Keamanan Informasi.
(2) Tim Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. CISO;
    b. Unit Pengelola TIK; dan
    c. Unit Pemilik Proses Bisnis

Pasal 5

CISO sebagaimana dimaksud dalam Pasal 4 bertanggung jawab untuk:

a. mengkoordinasikan perumusan dan penyempurnaan kebijakan dan standar SMKI di Lingkungan Badan;
b. memelihara dan mengendalikan penerapan kebijakan dan standar SMKI di seluruh area di Lingkungan Badan yang menjadi tujuan sasaran pengendalian;
c. menetapkan target keamanan informasi setiap tahunnya serta menyusun rencana kerja;
d. memastikan efektivitas dan konsistensi penerapan kebijakan dan standar SMKI di Lingkungan Badan serta mengukur kinerja keseluruhan; dan
e. melaporkan kinerja penerapan kebijakan dan standar SMKI di Lingkungan Badan serta pencapaian target kepada Komite TIK.
f. menunjuk pihak yang berkompeten untuk melakukan audit terhadap penerapan kebijakan dan standar SMKI di Lingkungan Badan.

Pasal 6

Unit Pengelola TIK sebagaimana dimaksud dalam Pasal 4 bertanggung jawab untuk:

a. memastikan kebijakan dan standar SMKI di Lingkungan Badan 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 SMKI di Lingkungan Badan;
c. memastikan peningkatan kesadaran, kepedulian, dan kepatuhan seluruh pegawai terhadap kebijakan dan standar SMKI di Lingkungan Badan;
d. melaporkan kinerja penerapan kebijakan dan standar SMKI di Lingkungan Badan sesuai ruang lingkup tanggung jawabnya kepada CISO yang akan digunakan sebagai dasar peningkatan keamanan informasi;

e. mengkoordinasikan penanganan gangguan keamanan informasi Badan; dan
f. memastikan terlaksananya audit terhadap penerapan kebijakan dan standar SMKI pada masing-masing unit eselon I di lingkungan Badan paling sedikit 1 (satu) kali dalam 3 (tiga) tahun.

Pasal 7

Unit Pemilik Proses Bisnis sebagaimana dimaksud dalam Pasal 4 bertanggung jawab untuk:

a. melaksanakan dan mengawasi penerapan kebijakan dan standar SMKI di Lingkungan Badan;
b. memberi masukan peningkatan terhadap kebijakan dan standar SMKI di Lingkungan Badan;
c. mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan keamanan informasi bagi pegawai di Lingkungan Badan;
d. memantau, mencatat, dan menguraikan secara jelas gangguan keamanan informasi yang diketahui atau laporan yang diterima, dan menindaklanjuti laporan tersebut sesuai prosedur pelaporan gangguan keamanan informasi, dan
e. memberi panduan dan/atau bantuan penyelesaian masalah-masalah keamanan informasi di Lingkungan Badan;

Pasal 8

(1) Audit terhadap penerapan kebijakan dan standar SMKI di Lingkungan Badan sebagaimana dimaksud dalam Pasal 6 huruf f dilakukan dengan tujuan untuk memastikan pengendalian, proses dan prosedur SMKI dilaksanakan secara efektif dan dipelihara dengan baik.
(2) Audit sebagaimana dimaksud pada ayat (1) dilakukan oleh pihak yang berkompeten untuk melakukan audit yang ditunjuk oleh CISO.

(3) Pihak yang berkompeten untuk melakukan audit menyampaikan laporan hasil audit terhadap penerapan kebijakan dan standar SMKI di Lingkungan Badan kepada CISO.

Pasal 9

(1) CISO menyampaikan laporan hasil audit kepada Unit Pengelola TIK.
(2) Unit Pengelola TIK berkoordinasi dengan Unit Pemilik Proses Bisnis untuk melakukan tindak lanjut atas laporan hasil audit.
(3) Unit Pemilik Proses Bisnis menindaklanjuti laporan hasil audit.
(4) Unit Pemilik Proses Bisnis menyampaikan hasil tindak lanjut terhadap laporan hasil audit kepada Unit Pengelola TIK dalam laporan kinerja SMKI.

BAB III

PENGELOLAAN KEAMANAN INFORMASI

Pasal 10

Kebijakan dan standar SMKI sebagaimana dimaksud dalam Pasal 2 terdiri dari 11 sasaran pengendalian, yaitu:

a. Pengendalian Umum;
b. Pengendalian Organisasi Keamanan Informasi;
c. Pengendalian Pengelolaan Aset Informasi;
d. Pengendalian Keamanan Sumber Daya Manusia;
e. Pengendalian Keamanan Fisik dan Lingkungan;
f. Pengendalian Pengelolaan Komunikasi dan Operasional;
g. Pengendalian Kontrol Akses;
h. Pengendalian Keamanan Informasi dalam Pengadaan, Pengembangan dan Pemeliharaaan Sistem Informasi;
i. Pengendalian Pengelolaan Gangguan Keamanan Informasi;
j. Pengendalian Keamanan Informasi Dalam Pengelolaan Kelangsungan Kegiatan; dan
k. Pengendalian Kepatuhan

Pasal 11

Kebijakan dan standar SMKI sebagaimana dimaksud dalam Pasal 10 tercantum dalam lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

BAB IV

KETENTUAN PENUTUP

Pasal 12

Peraturan Badan ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Jakarta
pada tanggal 9 Oktober 2020

KEPALA BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA,

ttd

JAZI EKO ISTIYANTO

Diundangkan di Jakarta
pada tanggal 27 Oktober 2020

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

ttd

WIDODO EKATJAHJANA

LAMPIRAN
PERATURAN BADAN PENGAWAS TENAGA NUKLIR
NOMOR 8 TAHUN 2020
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN BADAN PENGAWAS TENAGA NUKLIR

BAB I
PENDAHULUAN

A. Latar Belakang

Keamanan informasi merupakan hal penting dalam penyelenggaraan layanan. Dengan semakin meningkatnya risiko dan insiden keamanan informasi dalam penyelenggaraan sistem elektronik, upaya pengamanan terhadap sistem elektronik yang memiliki data dan informasi strategis dan penting harus segera dilakukan. Keamanan informasi yang handal, akan meningkatkan kepercayaan masyarakat terhadap penyelenggaraan sistem elektronik untuk pelayanan publik.

Sehubungan dengan hal tersebut, dalam rangka keamanan data dan informasi di lingkungan Badan, perlu menyusun sebuah standar tentang manajemen keamanan informasi, yang mengatur bagaimana informasi menjadi aman agar kerahasiaan, integritas, dan ketersediaan informasi tetap terjaga.

B. Tujuan

Kebijakan dan standar SMKI ini digunakan sebagai pedoman atau standar dalam rangka melindungi aset informasi Badan dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan Badan, dengan tujuan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.

C. Ruang Lingkup

Standar ini berlaku untuk pengelolaan pengamanan seluruh informasi Badan yang dilaksanakan oleh seluruh unit kerja Badan dan pihak ketiga baik sebagai pengelola dan/atau pengguna Teknologi Informasi dan Komunikasi (TIK).

D. Pengertian Umum

1. Akun adalah identifikasi pengguna yang diberikan oleh Unit Pengelola TIK, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem TIK.
2. Akun khusus adalah akun yang diberikan oleh Unit Pengelola TIK sesuai kebutuhan tetapi tidak terbatas pada pengelolaan TIK (baik berupa aplikasi atau sistem), dan kelompok kerja (baik berupa acara kedinasan, tim, atau unit kerja).
3. Aset Informasi adalah aset dalam bentuk data/dokumen, perangkat lunak, aset fisik, dan aset tak berwujud.
4. *Audit logging* adalah catatan mengenai perubahan data dalam aplikasi, yang dicatat biasanya kolom mana yang berubah, siapa yang mengubah, diubah dari apa menjadi apa, kapan berubah.
5. Aset fisik adalah jenis aset yang memiliki wujud fisik, misalnya perangkat komputer, perangkat jaringan dan komunikasi, media yang dapat dipindahkan, dan perangkat pendukung lainnya.
6. Aset tak berwujud adalah jenis aset yang tidak memiliki wujud fisik, misalnya pengetahuan, pengalaman, keahlian, citra, dan reputasi, mempunyai umur lebih dari satu tahun (aset tidak lancar) dan dapat diamortisasi selama periode pemanfaatannya, yang biasanya tidak lebih dari 40 (empat puluh tahun).
7. *Backup* adalah sebuah proses pembuatan gandaan/duplikat/ cadangan dari aset informasi yang dilakukan sebagai upaya pengamanan dan pemulihan sebagai bagian dari manajemen risiko.
8. Badan adalah Badan Pengawas Tenaga Nuklir.
9. *Chief Information Officer* yang selanjutnya disingkat CIO adalah pejabat pengarah informasi yang dijabat oleh Sekretaris Utama sebagai koordinator penyelenggaraan tata kelola Teknologi Informasi dan Komunikasi di lingkungan Badan.
10. *Chief Information Security Officer* yang selanjutnya disingkat CISO adalah pejabat yang berperan sebagai koordinator dalam

pelaksanaan implementasi kebijakan dan standar SMKI di Lingkungan Badan.

11. *Conduit* adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.
12. Daftar inventaris aset informasi adalah kumpulan informasi yang memuat bentuk, pemilik, lokasi, retensi, dan hal-hal yang terkait dengan aset informasi.
13. Direktori adalah penamaan koleksi file (biasanya berbentuk hirarki), merupakan cara untuk mengelompokkan file sehingga mudah untuk dikelola.
14. Dokumen SMKI Badan adalah dokumen terkait pelaksanaan Kebijakan dan standar SMKI yang meliputi antara lain dokumen standar, prosedur, dan catatan penerapan kebijakan dan standar SMKI.
15. *Fallback* adalah suatu tindakan pembalikan/menarik diri dari posisi awal.
16. Hak akses khusus adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan, *file server*, dan aplikasi-aplikasi sensitif yang hanya diberikan kepada pengguna yang membutuhkan, pemakaiannya terbatas dan dikontrol.
17. Kata sandi adalah serangkaian kode yang dibuat Pengguna, bersifat rahasia dan pribadi yang digunakan bersamaan dengan Akun Pengguna.
18. Keamanan informasi adalah terjaganya kerahasiaan, keutuhan, dan ketersediaan informasi.
19. Komite TIK adalah komite yang terdiri dari Deputi Perizinan dan Inspeksi, Deputi, Pengkajian Keselamatan Nuklir, Manajemen Unit Pengelola TIK, dan Ahli TIK yang dibentuk dengan tujuan untuk memberikan dukungan teknis TIK dalam mendukung pelaksanaan tugas CIO.
20. Komunitas keamanan informasi adalah kelompok/komunitas yang memiliki pengetahuan/keahlian khusus dalam bidang keamanan informasi atau yang relevan dengan keamanan informasi, seperti: *Indonesia Security Incident Response Team on Internet and Infrastructure* (ID-SIRTII), Unit *cybercrime* POLRI, ISC2, ISACA.

21. Koneksi eksternal (*remote access*) adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.
22. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan keamanan informasi. Dalam kriptografi terdapat dua prinsip yaitu enkripsi dan dekripsi.
23. *Malicious code* adalah semua jenis program yang membahayakan termasuk makro atau *script* yang dapat dieksekusi dan dibuat dengan tujuan untuk merusak sistem komputer.
24. *Master disk* adalah media yang digunakan sebagai sumber dalam melakukan instalasi perangkat lunak.
25. *Mobile computing* adalah penggunaan perangkat komputasi yang dapat dipindah, misalnya *notebook* dan *personal data assistant* (PDA) untuk melakukan akses, pengolahan data, dan penyimpanan.
26. Pengguna adalah pegawai Badan dan atau pihak ketiga serta tidak terbatas pada pengelola TIK dan kelompok kerja yang diberikan hak mengakses sistem TIK di lingkungan Badan.
27. 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 dengan waktu.
28. Perangkat jaringan adalah peralatan jaringan komunikasi data seperti: *modem, hub, switch, router*, dan lain-lain.
29. Perangkat lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.
30. Perangkat pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras dan perangkat jaringan serta untuk melindunginya dari kerusakan. Contoh perangkat pendukung adalah *Uninterruptible Power Supply* (UPS), pembangkit tenaga listrik/ generator, antena komunikasi.
31. Perangkat pengolah informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur seperti komputer, faksimili, telepon, mesin *fotocopy*.

32. Perjanjian *escrow* adalah perjanjian dengan pihak ketiga untuk memastikan apabila pihak ketiga tersebut bangkrut (mengalami *failure*) maka Badan berhak untuk mendapatkan kode program (*source code*).
33. 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.
34. Petugas Pelaksana Pengelolaan Proses Kelangsungan Kegiatan adalah pegawai yang ditunjuk oleh Pimpinan Unit Eselon I untuk mengelola proses kelangsungan kegiatan pada saat keadaan darurat.
35. Pihak ketiga adalah semua unsur di luar pengguna Unit Pemilik Proses Bisnis Badan yang bukan bagian dari Badan, misal mitra kerja Badan (seperti: konsultan, penyedia jasa komunikasi, pemasok dan pemelihara perangkat pengolah informasi), dan kementerian/lembaga lain.
36. Rencana kontijensi adalah suatu rencana ke depan pada keadaan yang tidak menentu dengan skenario, tujuan, teknik, manajemen, pelaksanaan, serta sistem penanggulanggannya telah ditentukan secara bersama untuk mencegah dan mengatasi keadaan darurat.
37. *Routing* adalah sebuah mekanisme yang digunakan untuk mengarahkan dan menentukan rute/jalur yang akan dilewati paket dari satu perangkat ke perangkat yang berada di jaringan lain.
38. Sanitasi adalah proses penghilangan informasi yang disimpan secara permanen dengan menggunakan medan magnet besar atau perusakan fisik.
39. Sistem Informasi adalah serangkaian perangkat keras, perangkat lunak, sumber daya manusia, serta prosedur dan atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi informasi yang berguna untuk mencapai suatu tujuan.
40. Sistem Manajemen Keamanan Informasi yang selanjutnya disebut SMKI 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.

41. Standar Operasional Prosedur adalah sistem yang disusun untuk memudahkan, merapihkan dan menertibkan pekerjaan dan berisi urutan proses melakukan pekerjaan dari awal sampai akhir.
42. *System administrator* adalah sebuah akun khusus untuk mengelola sistem informasi.
43. *System utilities* adalah sebuah sistem perangkat lunak yang melakukan suatu tugas/fungsi yang sangat spesifik, biasanya disediakan oleh sistem operasi, dan berkaitan dengan pengelolaan sumber daya sistem, seperti *memory*, *disk*, *printer*, dan sebagainya.
44. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah teknologi untuk mengumpulkan, menyiapkan, menyimpan, mengolah, mengumumkan, menganalisis, mengambil kembali, mengirim atau menerima data dan informasi.
45. *Teleworking* adalah penggunaan teknologi telekomunikasi untuk memungkinkan pegawai bekerja di suatu lokasi yang berada di luar kantor untuk mengakses jaringan internal kantor.
46. Tim Keamanan Informasi adalah tim yang dibentuk dalam rangka perlindungan terhadap keamanan informasi Badan.
47. Unit Pemilik Aset Informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi yang terdiri dari Unit Pemilik Proses Bisnis dan Unit Pengelola TIK .
48. Unit Pemilik Proses Bisnis adalah unit kerja yang memiliki aplikasi sistem informasi dan/atau memiliki alat monitoring pengawasan ketenaganukliran.
49. Unit Pengelola TIK adalah unit kerja yang melakukan pengelolaan Teknologi Informasi dan Komunikasi berupa mengumpulkan, menyiapkan, menyimpan, mengolah, mengumumkan, menganalisis, mengambil kembali, mengirim atau menerima data dan informasi.

BAB II

KEBIJAKAN DAN STANDAR

I. PENGENDALIAN UMUM

A. TUJUAN

Kebijakan dan standar SMKI ini digunakan sebagai pedoman dalam rangka melindungi aset informasi Badan dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan Badan yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi agar selalu terjaga dan terpelihara dengan baik.

B. RUANG LINGKUP

1. Catatan Penerapan kebijakan dan standar SMKI di Lingkungan Badan
2. Penyusunan Dokumen Pendukung
3. Pengendalian Dokumen

C. KEBIJAKAN

1. Catatan Penerapan kebijakan dan standar SMKI di Lingkungan Badan

   Kebijakan dan standar ini berlaku untuk pengelolaan pengamanan seluruh aset informasi Badan dan dilaksanakan oleh seluruh unit kerja Badan, pegawai Badan baik pengguna maupun pengelola Teknologi Informasi dan Komunikasi (TIK), dan pihak ketiga di lingkungan Badan.
2. Penyusunan Dokumen Pendukung

   Aset informasi Badan adalah aset dalam bentuk:
   i. Data/dokumen, meliputi antara lain: data izin, data anggaran, data kepegawaian, kebijakan Badan, hasil inspeksi, hasil/laporan kajian, bahan pelatihan, prosedur operasional, rencana kelangsungan kegiatan, dan hasil audit;
   ii. Perangkat lunak, meliputi: perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat bantu pengembangan sistem;

iii. Aset fisik, meliputi: perangkat komputer, perangkat jaringan dan komunikasi, removable media, dan perangkat pendukung; dan

iv. Aset tak berwujud, meliputi: pengetahuan, pengalaman, keahlian, citra, dan reputasi.

3. Pengendalian Dokumen

1. Kebijakan dan standar SMKI di lingkungan Badan dikoordinasikan oleh Sekretaris Utama yang berperan sebagai CIO dan sekaligus CISO Badan;
2. CISO Badan menetapkan Tim Keamanan Informasi;
3. Unit Pemilik Proses Bisnis menerapkan kebijakan dan standar SMKI yang ditetapkan dalam Peraturan Badan;
4. Pimpinan Unit Pemilik Proses Bisnis bertanggung jawab mengawasi penerapan kebijakan dan standar SMKI di Unit Kerja masing-masing;
5. Unit Pemilik Proses Bisnis bertanggung jawab melaksanakan pengamanan aset informasi di unit kerja masing-masing dengan mengacu pada kebijakan dan standar SMKI;
6. Unit Pemilik Proses Bisnis bertanggung jawab meningkatkan pengetahuan, ketrampilan, dan kepedulian terhadap keamanan informasi pada seluruh pengguna di Unit Kerja masing-masing;
7. Unit Pemilik Proses Bisnis menerapkan prinsip manajemen risiko dalam rangka pelaksanaan pengamanan dan perlindungan aset informasi dengan mengikuti ketentuan mengenai Penerapan Manajemen Risiko di Lingkungan Badan;
8. Unit Pemilik Proses Bisnis membuat laporan pelaksanaan kebijakan dan standar SMKI secara berkala di unit kerja masing-masing;
9. Badan melakukan audit terhadap penerapan kebijakan dan standar SMKI di lingkungan Badan untuk memastikan pengendalian, proses dan prosedur SMKI dilaksanakan secara efektif dan dipelihara dengan baik;

10. CISO menunjuk pihak yang berkompeten untuk melakukan audit terhadap penerapan kebijakan dan standar SMKI di lingkungan Badan.
11. Unit Pengelola TIK berkoordinasi dengan Unit Pemilik Proses Bisnis untuk menindaklanjuti laporan hasil audit kebijakan dan standar SMKI;
12. Unit Pemilik Proses Bisnis menyampaikan hasil tindak lanjut audit kepada Unit Pengelola TIK dalam laporan kinerja kebijakan dan standar SMKI.

D. STANDAR

1. Menggunakan catatan penerapan kebijakan dan standar SMKI di Lingkungan Badan untuk mengukur kepatuhan dan efektivitas penerapan kebijakan dan standar SMKI, meliputi:
   a) Formulir sesuai prosedur operasional;
   b) Catatan gangguan keamanan informasi;
   c) Catatan pengunjung di *secure area*;
   d) Kontrak dan perjanjian layanan;
   e) Laporan audit; dan
   f) Perjanjian kerahasiaan.
2. Penyusunan dokumen pendukung kebijakan keamanan informasi memuat:
   a) Tujuan dan ruang lingkup dokumen pendukung kebijakan keamanan informasi;
   b) Kerangka kerja setiap tujuan/sasaran pengendalian keamanan informasi; dan
   c) Penjelasan singkat mengenai standar, prosedur dan kepatuhan termasuk persyaratan peraturan yang dipenuhi, pengelolaan kelangsungan kegiatan, konsekuensi apabila terjadi pelanggaran.
3. Mengendalikan dokumen kebijakan dan standar SMKI Badan untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan dan mencegah akses oleh pihak yang tidak berwenang;

4. Menempatkan dokumen kebijakan dan standar SMKI Badan di semua area operasional sehingga mudah diakses oleh pengguna di unit kerja sesuai peruntukkannya.

II. PENGENDALIAN ORGANISASI KEAMANAN INFORMASI

A. TUJUAN

Memberikan pedoman dalam membentuk tim keamanan informasi yang bertanggung jawab untuk mengelola keamanan informasi dan perangkat pengolah informasi di lingkungan Badan termasuk hubungan dengan pihak luar.

B. RUANG LINGKUP

1. Tim Keamanan Informasi
2. Perjanjian kerjasama;
3. Pengendalian keamanan informasi;
4. Hubungan dengan pihak terkait, komunitas keamanan informasi dan pihak ketiga.

C. KEBIJAKAN

1. Tanggung jawab Tim Keamanan Informasi diuraikan dalam standar organisasi keamanan informasi;
2. Unit Pemilik Aset Informasi mengkaji perjanjian kerahasiaan pihak-pihak internal dan eksternal secara berkala untuk menjaga aset informasi;
3. Menjalin kerja sama dengan pihak-pihak di luar Badan yang terkait dengan keamanan informasi;
4. Menjalin kerja sama dengan komunitas keamanan informasi di luar Badan melalui pelatihan, seminar, atau forum lain yang relevan dengan keamanan informasi;
5. Menerapkan pengendalian keamanan informasi berdasarkan hasil penilaian risiko untuk mencegah atau mengurangi dampak risiko terkait dengan pemberian akses kepada pihak ketiga; dan
6. Menerapkan pengendalian keamanan informasi terhadap penggunan perangkat komunikasi.

D. STANDAR

1. Tanggung jawab Tim Keamanan Informasi

a) Sekretaris Utama sebagai CISO Badan bertanggung jawab untuk:

(1) Mengkoordinasikan perumusan dan penyempurnaan kebijakan dan standar SMKI di lingkungan Badan;

(2) Memelihara dan mengendalikan penerapan kebijakan dan standar pengendalian;

(3) Menetapkan target keamanan informasi setiap tahunnya serta menyusun rencana kerja;

(4) Memastikan efektivitas dan konsistensi penerapan kebijakan dan standar SMKI serta mengukur kinerja keseluruhan;

(5) Melaporkan kinerja penerapan kebijakan dan standar SMKI di Lingkungan Badan serta pencapaian target kepada Komite TIK Badan; dan

(6) menunjuk tim audit yang akan melakukan audit terhadap penerapan kebijakan dan standar SMKI.

b) Unit Pengelola TIK bertanggung jawab untuk:

(1) Memastikan kebijakan dan standar SMKI di lingkungan Badan di terapkan secara efektif;

(2) Memastikan langkah-langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan dalam pelaksanaan evaluasi dan/atau audit penerapan kebijakan dan standar Memastikan peningkatan kesadaran, kepedulian dan kepatuhan seluruh pegawai terhadap kebijakan dan standar SMKI;

(3) Melaporkan kinerja penerapan kebijakan dan standar SMKI sesuai ruang lingkup tanggung jawab kepada CISO, untuk digunakan sebagai dasar peningkatan keamanan informasi;

(4) Mengkoordinasikan penanganan gangguan keamanan informasi di tingkat Badan; dan

(5) memastikan terlaksananya audit terhadap penerapan kebijakan dan standar SMKI pada

masing-masing unit eselon I di lingkungan Badan paling sedikit 1 (satu) kali dalam 3 (tiga) tahun.

c) Unit Pemilik Proses Bisnis bertanggung jawab untuk:
   (1) melaksanakan dan mengawasi penerapan kebijakan dan standar SMKI di Lingkungan Badan;
   (2) memberi masukan peningkatan terhadap kebijakan dan standar SMKI di Lingkungan Badan;
   (3) mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan keamanan informasi bagi pegawai;
   (4) memantau, mencatat, dan menguraikan secara jelas gangguan keamanan informasi yang diketahui atau laporan yang diterima, dan menindaklanjuti laporan tersebut sesuai prosedur pelaporan gangguan keamanan informasi, dan
   (5) memberi panduan dan/atau bantuan penyelesaian masalah-masalah keamanan informasi;

d) Perjanjian kerahasiaan memuat unsur-unsur antara lain:
   a) Definisi dari informasi yang akan dilindungi;
   b) Durasi yang diharapkan dari sebuah perjanjian kerahasiaan;
   c) Tanggungjawab dan tindakan penandatangan;
   d) Perlindungan kepemilikan informasi, rahasia organisasi dan kekayaan intektual;
   e) Izin menggunakan informasi rahasia;
   f) Hak penandatangan untuk menggunakan informasi;
   g) Hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia;
   h) Proses untuk pemberitahuan dan pelaporan dari penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan informasi;
   i) Tindakan yang diperlukan pada saat sebuah perjanjian kerahasiaan diakhiri;
   j) Syarat-syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian; dan
   k) Tindakan yang akan diambil apabila terjadi

pelanggaran terhadap perjanjian ini.

III. PENGENDALIAN PENGELOLAAN ASET INFORMASI

A. TUJUAN

Memberikan pedoman dalam mengelola aset informasi di lingkungan Badan untuk melindungi dan menjamin keamanan aset informasi.

B. RUANG LINGKUP

1. Tanggung jawab setiap unit kerja terhadap asset informasi; dan
2. Pengklasifikasian aset informasi.

C. KEBIJAKAN

1. Unit Pemilik Aset Informasi bertanggung jawab terhadap keamanan aset informasi berupa:
   a) Mengidentifikasi aset informasi dan mendokumentasikannya dalam daftar inventaris aset informasi;
   b) Menetapkan aset informasi yang terkait dengan perangkat pengolah informasi; dan
   c) menetapkan aturan penggunaan aset informasi.

2. Klasifikasi Aset Informasi

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

D. STANDAR

1. Unit Pemilik Aset Informasi menetapkan dan mengkaji secara berkala klasifikasi aset informasi dan jenis perlindungan keamanannya;
2. Unit Pemilik Aset Informasi menetapkan pihak yang berwenang untuk mengakses aset informasi;
3. Aset informasi Badan diklasifikasikan sebagai berikut:
   a) SANGAT RAHASIA, yaitu aset informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian yang berdampak pada ketahanan dan keutuhan nasional;

b) RAHASIA, yaitu aset informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan atau mengganggu citra dan reputasi Badan dan/atau yang menurut peraturan perundang-undangan dinyatakan rahasia;

c) TERBATAS, yaitu aset informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu kelancaran kegiatan Badan tetapi tidak akan mengganggu citra dan reputasi Badan;

d) PUBLIK, yaitu aset informasi yang secara sengaja disediakan Badan untuk diketahui masyarakat umum.

IV. PENGENDALIAN KEAMANAN SUMBER DAYA MANUSIA

A. TUJUAN

Memastikan bahwa seluruh pegawai dan pihak ketiga di lingkungan Badan memahami tanggung jawabnya masing-masing, sadar atas ancaman keamanan informasi, serta mengetahui proses terkait keamanan informasi.

B. RUANG LINGKUP

Kebijakan dan standar keamanan sumber daya manusia ini mencakup peran dan tanggung jawab seluruh pegawai dan pihak ketiga di lingkungan Badan yang 12 dipahami dan dilaksanakan. Peran dan tanggung jawab pegawai mengacu pada peraturan perundang-undangan yang berlaku.

C. KEBIJAKAN

1. Seluruh pegawai bertanggung jawab untuk menjaga keamanan informasi Badan sesuai tugas dan fungsinya;
2. Pihak ketiga menyetujui dan menandatangani syarat dan perjanjian untuk menjaga keamanan informasi Badan;
3. Peran dan tanggung jawab pegawai dan pihak ketiga terhadap keamanan informasi didefinisikan, diterapkan, dan dikomunikasikan kepada yang bersangkutan;

4. Unit Pemilik Aset Informasi melakukan pemeriksaan data pribadi yang diberikan oleh pegawai baru dan pihak ketiga sesuai dengan ketentuan yang berlaku;
5. Seluruh pegawai mendapatkan pendidikan/pelatihan/ sosialisasi keamanan sistem informasi secara berkala sesuai tingkat tanggung jawabnya;
6. Pihak ketiga diberikan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi (jika diperlukan);
7. Seluruh pegawai dan pihak ketiga yang melanggar kebijakan dan standar SMKI di lingkungan Badan akan diberikan sanksi atau tindakan disiplin sesuai dengan ketentuan yang berlaku;
8. Kepatuhan pegawai terhadap kebijakan dan standar SMKI di lingkungan Badan diawasi oleh atasan masing-masing ;
9. Pegawai yang berhenti bekerja atau mutasi harus mengembalikan seluruh aset informasi yang dipergunakan selama bekerja sesuai dengan ketentuan yang berlaku;
10. Pihak ketiga yang habis masa kontrak kerjanya harus mengembalikan seluruh aset informasi yang dipergunakan selama bekerja di Badan;
11. Unit Pemilik Aset Informasi menghentikan hak penggunaan aset informasi bagi pegawai yang sedang dalam pemeriksaan dan/atau menjalani proses hukum terkait dengan dugaan pelanggaran terhadap kebijakan dan standar SMKI di lingkungan Badan; dan
12. Unit Pemilik Aset Informasi mencabut hak akses terhadap akses informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi bekerja di Badan.

D. STANDAR

1. Peran dan tanggung jawab pegawai terhadap keamanan informasi menjadi bagian dan penjabaran tugas dan fungsi, khususnya bagi yang memiliki akses terhadap aset informasi dengan menyertakan persyaratan:
   a) Melaksanakan dan bertindak sesuai dengan organisasi keamanan informasi;
   b) Melindungi aset dari akses yang tidak sah, penyingkapan,

modifikasi, kerusakan atau gangguan;

c) Melaporkan kejadian, potensi kejadian atau risiko keamanan informasi sesuai kebijakan dan standar SMKI di lingkungan Badan.

2. Pimpinan dari pegawai berkeahlian khusus atau yang berada di posisi kunci memastikan ketersediaan pegawai pengganti dengan kompetensi yang setara apabila pegawai yang bersangkutan mutasi atau berhenti;

3. Pemeriksaan latar belakang calon pegawai dan pihak ketiga Badan memperhitungkan privasi, perlindungan data pribadi dan/atau pekerjaan yang meliputi:

a) Pemeriksaan kelengkapaan dan ketepatan dari riwayat hidup pemohon;

b) Konfirmasi kualifikasi akademik dan profesional yang diklaim; dan

c) Pemeriksaan identitas dan lebih rinci, seperti pemeriksaan kredit atau catatan kriminal.

V. PENGENDALIAN KEAMANAN FISIK DAN LINGKUNGAN

A. TUJUAN

Mencegah akses fisik oleh pihak yang tidak berwenang, menghindari terjadinya kerusakan pada perangkat pengolah informasi serta gangguan pada aktivitas organisasi.

B. RUANG LINGKUP

Kebijakan dan standar keamanan fisik dan lingkungan ini meliputi:

1. Pengamanan area; dan
2. Pengamanan perangkat.

C. KEBIJAKAN

1. Pengamanan area

a) Seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan area Pusat Data/Ruang Server Badan harus mematuhi aturan yang berlaku;

b) Ketentuan rinci tentang pengamanan area lingkungan kerja Badan diuraikan dalam standar keamanan fisik dan lingkungan.

2. Pengamanan perangkat
   a) Perangkat pengolah informasi dan perangkat pendukung ditempatkan di lokasi yang aman dan diposisikan sedemikian rupa untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang;
   b) Perangkat pendukung dipasang untuk menjamin beroperasinya perangkat pengolah informasi dan diperiksa dan diuji ulang kinerjanya secara berkala;
   c) Kabel sumber daya listrik harus dilindungi dari kerusakan, dan kabel telekomunikasi yang mengalirkan informasi harus dilindungi dari kerusakan dan penyadapan;
   d) Perangkat pengolah informasi dipelihara secara berkala untuk menjamin ketersediaan, keutuhan, dan fungsinya;
   e) Penggunaan perangkat yang dibawa ke luar dari lingkungan Badan disetujui oleh Pejabat yang berwenang;
   f) Perangkat pengolah informasi penyimpan data yang sudah tidak digunakan lagi disanitasi sebelum digunakan kembali atau dihapuskan/dimusnahkan;
   g) Penanganan perangkat pengolah informasi penyimpan data di lingkungan Badan sesuai dengan standar penanganan media penyimpan data yang ditetapkan dalam Standar Operasional Prosedur Pengelolaan Data Elektronik di lingkungan Badan.

D. STANDAR
   1. Perangkat diperlihara sesuai dengan petunjuk manualnya;
   2. Pemeliharaan terhadap perangkat keras atau perangkat lunak dilakukan oleh Unit Pemilik Aset Informasi;
   3. Untuk pemeliharaan yang dilakukan oleh pihak ketiga, diadakan Perjanjian Tingkat Layanan (*Service Level Agreement/SLA*) yang mendefinisikan tingkat pemeliharaan yang disediakan dan tingkat kinerja yang harus dipenuhi pihak ketiga;
   4. 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;

5. Otorisasi penggunaan perangkat dilakukan secara tertulis dan data-data yang terkait dengan aset informasi yang digunakan, seperti nama pemakai aset, lokasi dan tujuan penggunaan aset, dicatat dan disimpan;
6. Pengamanan Area
   a) Menyimpan perangkat pengolah informasi di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain pintu yang dilengkapi dengan *access door*, sistem pemadam kebakaran, alarm bahaya, CCTV, dan perangkat pemutus aliran listrik;
   b) Akses ke ruang server, pusat data dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA dibatasi dan hanya diberikan kepada pegawai yang diberi wewenang;
   c) Pegawai dan pihak ketiga yang akan memasuki ruang server, pusat data dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus menginformasikan terlebih dahulu kepada Unit Pengelola TIK dan pada pelaksanaannya harus didampingi oleh pegawai Unit Pengelola TIK sepanjang waktu kunjungan;
   d) Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA dilindungi secara memadai;
   e) Pegawai dan pihak ketiga tidak diizinkan merokok, makan, minum, dan istirahat di ruang *server* dan pusat data; dan
   f) Area keluar masuk barang dan area publik harus selalu dijaga, diawasi, dan dikendalikan atau jika memungkinkan disterilkan dari perangkat pengolah informasi untuk menghindari akses oleh pihak yang tidak berwenang.

7. Pengamanan Kantor, Ruangan, dan Fasilitas.
   a) Pengamanan kantor, ruangan, dan fasilitas dilakukan sesuai dengan aturan dan standar keamanan dan keselamatan kerja yang berlaku;
   b) Fasilitas utama ditempatkan khusus untuk menghindari akses publik; dan
   c) Pembatasan pemberian identitas atau tanda-tanda keberadaan aktitivitas pengolahan informasi;
8. Perlindungan terhadap Ancaman Eksternal dan Lingkungan.
   a) Bahan-bahan berbahaya atau mudah terbakar disimpan padajarak aman dari *secure areas*;
   b) Perlengkapan umum tidak boleh disimpan di *secure areas*;
   c) Perangkat pemulihan (*fallback)* dan media *backup* diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama; dan
   d) Perangkat pemadam kebakaran disediakan dan ditempatkan di area yang tepat.
9. Penempatan dan Perlindungan Perangkat.
   Penempatan dan perlindungan perangkat mencakup:
   a) Perangkat diletakkan pada lokasi yang meminimalkan akses yang tidak perlu ke dalam area kerja;
   b) Perangkat pengolah informasi yang menangani informasi sensitif diposisikan dan dibatasi arah sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak yang tidak berwenang selama digunakan, 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/perlakuan standar yang perlu dilakukan;
   d) Kondisi lingkungan, seperti suhu dan kelembaban dimonitor untuk mencegah perubahan kondisi yang dapat mempengaruhi pengoperasian perangkat pengolah informasi;

e) Perlindungan petir diterapkan untuk semua bangunan dan filter perlindungan petir dipasang untuk semua jalur komunikasi dan listrik; dan

f) Perangkat pengolah informasi sensitif dilindungi untuk meminimalkan risiko kebocoran informasi.

10. Pengamanan kabel.

a) Pemasangan kabel sumber daya listrik dan kabel telekomunikasi ke perangkat pengolah informasi harus menerapkan alternatif perlindungan yang memadai;

b) Pemasangan kabel jaringan harus terlindungi dari penyusupan yang tidak sah atau kerusakan, misal dengan menggunakan *conduit* atau menghindari rute area publik;

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

d) Penandaan/penamaan kabel dan perangkat 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 mempertimbangkan:

(1) Penggunaan *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 *fiber optic*;

(5) Penggunaan lapisan elektromagnetik untuk melindungi kabel; dan

(6) Penerapan akses *control* ke panel *patch* dan ruangan kabel.

VI. PENGENDALIAN PENGELOLAAN KOMUNIKASI DAN OPERASIONAL

A. TUJUAN

Memastikan komunikasi dan operasional yang aman dan benar

pada perangkat pengolah informasi, mengimplementasikan dan memelihara keamanan informasi, mengelola layanan yang diberikan pihak ketiga, meminimalkan risiko kegagalan, melindungi keutuhan dan ketersediaan informasi dan perangkat lunak, memastikan keamanan pertukaran informasi dan pemantauan terhadap proses operasional.

B. RUANG LINGKUP

Kebijakan dan standar pengelolaan komunikasi dan operasional, meliputi:

1. Prosedur operasional dan tanggungjawab;
2. Pengelolaan layanan oleh pihak ketiga;
3. Perencanaan dan penerimaan sistem;
4. Perlindungan terhadap ancaman program yang membahayakan (*malicious code*);
5. *Backup*;
6. Pengelolaan keamanan jaringan;
7. Penanganan media penyimpanan;
8. Pertukaran informasi; dan
9. Pemantauan.

C. KEBIJAKAN

1. Prosedur operasional dan tanggung jawab
   a) Mendokumentasikan, memelihara, dan menyediakan seluruh prosedur operasional yang terkait dengan penggunaan perangkat pengolah informasi sesuai dengan peruntukannya;
   b) Mengendalikan perubahan terhadap perangkat pengolah informasi;
   c) Melakukan pemisahan informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA untuk menghindari adanya pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya; dan
   d) Melakukan pemisahan perangkat pengembangan, pengujian, dan operasional untuk mengurangi risiko

perubahan atau akses oleh pihak yang tidak berwenang terhadap sistem operasional.

2. Pengelolaan layanan oleh pihak ketiga
   a) Memastikan bahwa pengendalian keamanan informasi, definisi layanan, dan tingkat layanan yang tercantum dalam kesepakatan penyediaan layanan telah diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga;
   b) Melakukan pemantauan terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh pihak ketiga secara berkala; dan
   c) Memperhatikan kritikalitas, proses yang terkait dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan pihak ketiga.
3. Perencanaan dan penerimaan sistem
   a) Unit Pemilik Proses Bisnis memantau penggunaan perangkat pengolah informasi dan membuat perkiraan pertumbuhan kebutuhan ke depan untuk memastikan ketersediaan kapasitas; dan
   b) Unit Pemilik Proses Bisnis menetapkan kriteria penerimaan untuk sistem informasi baru, pemutakhiran dan versi baru serta melakukan pengujian sebelum penerimaan.
4. Perlindungan terhadap ancaman program yang membahayakan (*malicious code*).
   Menerapkan sistem yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan.
5. *Backup*
   a) Melakukan *backup* informasi dan perangkat lunak yang berada di Pusat Data secara berkala; dan
   b) Proses *backup* di lingkungan Badan sesuai dengan *backup* data yang ditetapkan dalam Standar Operasional Prosedur Pengelolaan Data Elektronik di Lingkungan Badan.
6. Pengelolaan keamanan jaringan
   a) Mengelola dan melindungi jaringan dari berbagai bentuk ancaman; dan

b) Mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan serta mencantumkannya dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh pihak ketiga.

7. Penanganan media penyimpan data
   a) Unit Pengelola TIK mempunyai prosedur yang mengatur penanganan media penyimpan data untuk melindungi aset informasi; dan
   b) Penanganan media penyimpanan data di Badan sesuai dengan standar penanganan media penyimpan data yang ditetapkan dalam Standar Operasional Prosedur Pengelolaan Data Elektronik di Lingkungan Badan.
8. Pertukaran informasi
   a) Pertukaran informasi dan perangkat lunak antara Badan dengan pihak ketiga dilakukan atas kesepakatan tertulis kedua belah pihak;
   b) Unit Pemilik Aset Informasi melakukan penilaian risiko yang memadai sebelum melaksanakan pertukaran informasi; dan
   c) Menerapkan pengendalian keamanan informasi untuk pengiriman informasi melalui surat elektronik atau pengiriman informasi melalui jasa layanan pengiriman dalam rangka menghindari akses pihak yang tidak berwenang.
9. Pemantauan
   a) Menerapkan audit *logging* yang mencatat aktivitas pengguna, pengecualian, dan kejadian keamanan informasi dalam kurun waktu tertentu untuk membantu pengendalian akses dan investigasi di masa mendatang;
   b) Memantau penggunaan sistem dan mengkaji secara berkala hasil kegiatan pemantauan;
   c) Melindungi fasilitas pencatatan dan data yang dicatat dari kerusakan dan akses oleh pihak yang tidak berwenang;
   d) Menerapkan pencatatan kegiatan sistem administrator dan sistem operator;

e) Menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindakan penanganan yang tepat; dan

f) Memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.

D. STANDAR

1. Melaksanakan dokumentasi Standar Operasional Prosedur mencakup:
   a) Tata cara pengolahan dan penanganan informasi;
   b) Tata cara menangani kesalahan atau kondisi khusus yang terjadi beserta pihak yang dihubungi bila mengalami kesulitan teknis;
   c) Tata 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 pengguna dan catatan kejadian sistem.
2. Pemisahan Perangkat Pengembangan dan Operasional harus mempertimbangkan:
   a) Pengembangan dan operasional perangkat lunak dioperasikan di sistem atau prosesor komputer dan *domain* atau direktori yang berbeda;
   b) Instruksi kerja dari pengembangan perangkat lunak ke operasional ditetapkan dan didokumentasikan;
   c) *Compiler, editor*, dan alat bantu pengembangan lain tidak boleh diakses dari sistem operasional ketika tidak dibutuhkan;
   d) Lingkungan sistem pengujian diusahakan sama dengan lingkungan sistem operasional;
   e) Pengguna menggunakan profil pengguna yang berbeda untuk sistem pengujian dan sistem operasional, serta aplikasi menampilkan pesan identifikasi dari sistem

untuk mengurangi risiko kesalahan; dan

f) Data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA tidak boleh disalin ke dalam lingkungan pengujian sistem.

3. Pemantauan dan pengkajian layanan Pihak Ketiga, serta laporan dan catatan dari pihak ketiga mencakup proses sebagai berikut:
   a) Pemantauan tingkat kinerja layanan untuk memastikan kesesuaian kepatuhan dengan perjanjian;
   b) Pengkajian laporan layanan pihak ketiga dan pengaturan pertemuan berkala dalam rangka pembahasan perkembangan layanan sebagaimana diatur dalam perjanjian/kesepakatan;
   c) Pemberian informasi tentang gangguan keamanan informasi dan pengkajian informasi bersama pihak ketiga sebagaimana diatur dalam perjanjian/kesepakatan;
   d) Pemeriksaan jejak audit pihak ketiga dan pencatatan peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan; dan
   e) Penyelesaian dan pengelolaan masalah yang teridentifikasi.
4. Pengelolaan keamanan 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;
   c) Pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal;
   d) Pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan Badan dan menerapkan pemantauan serta pencatatan kegiatan selama menggunakan jaringan;
   e) Pemutusan layanan tanpa pemberitahuan sebelumnya jika terjadi gangguan keamanan informasi;
   f) Perlindungan jaringan dari akses yang tidak berwenang,

mencakup:

(1) Penetapan penanggungjawab pengelolaan jaringan dipisahkan dari pengelolaan perangkat pengolah informasi;

(2) Penerapan pengendalian khusus untuk melindungi keutuhan informasi yang melewati jaringan umum atara 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 fitur keamanan layanan jaringan mencakup:

(1) Teknologi keamanan seperti autentifikasi, enkripsi dan pengendalian sambungan jaringan;

(2) Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan keamanan dan aturan koneksi jaringan; dan

(3) Prosedur untuk penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.

5. Pertukaran 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 pihak ketiga yang dapat membahayakan organisasi;
(2) Penyalahgunaan teknik kriptografi;
(3) Penyelenggaraan penyimpanan dan penghapusan/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; dan
(6) Pembangunan kepedulian atas ancaman pencurian informasi

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

6. Pemantauan

Pemantauan penggunaan sistem pengolah informasi ditetapkan untuk menjamin agar kegiatan akses yang tidak sah tidak perlu terjadi. Kegiatan ini mencakup pemantauan:

a) Kegagalan akses;
b) Pola *log-on* yang mengindikasikan pengguna yang tidak wajar;
c) Alokasi penggunaan hak akses khusus;
d) Penelusuran transaksi dari pengiriman file tertentu yang mencurigakan; dan
e) Penggunaan sumber daya sensitif.

VII. PENGENDALIAN KONTROL AKSES

A. TUJUAN

Memastikan otorisasi akses pengguna dan mencegah akses pihak

yang tidak berwenang terhadap aset informasi khususnya perangkat pengolah informasi.

B. RUANG LINGKUP

Kebijakan dan standar pengendalian kontrol akses, meliputi:

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

C. KEBIJAKAN

1. Persyaratan untuk pengendalian kontrol akses.
   Menyusun, mendokumentasikan, dan mengkaji ketentuan akses ke aset informasi berdasarkan kebutuhan organisasi dan persyaratan keamanan.
2. Pengelolaan kontrol akses pengguna
   a) Menyusun prosedur pengelolaan hak akses pengguna sesuai dengan peruntukannya;
   b) Membatasi dan mengendalikan penggunaan hak akses khusus;
   c) Mengatur pengelolaan kata sandi pengguna; dan
   d) Memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya.
3. Tanggung jawab pengguna
   a) Mematuhi aturan pembuatan dan penggunaan kata sandi;
   b) Memastikan perangkat pengolah informasi yang digunakan mendapatkan perlindungan terutama saat ditinggalkan; dan
   c) Melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang.
4. Pengendalian kontrol akses jaringan

a) Mengatur akses pengguna dalam mengakses jaringan di lingkungan Badan sesuai dengan peruntukannya;
b) Menerapkan proses otorisasi pengguna untuk setiap akses ke dalam jaringan internal melalui koneksi eksternal;
c) Akses ke perangkat keras dan perangkat lunak untuk diagnosa dikontrol berdasarkan prosedur dan hanya digunakan oleh pegawai yang diberikan wewenang untuk melakukan pengujian, pemecahan masalah, serta pengembangan *system*, dan *port* pada fasilitas jaringan yang tidak dibutuhkan dalam kegiatan atau fungsi layanan harus dinonaktifkan;
d) Memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi;
e) Menerapkan mekanisme pengendalian akses pengguna sesuai dengan persyaratan pengendalian akses; dan
f) Pengendalian *routing* jaringan internal Badan dilakukan sesuai pengendalian akses dan kebutuhan layanan informasi.

5. Pengendalian kontrol akses ke sistem operasi
   a) Akses ke sistem operasi dikontrol dengan menggunakan prosedur akses yang aman;
   b) Setiap pengguna harus memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya, dan proses otorisasi pengguna menggunakan teknik autentikasi yang sesuai untuk memvalidasi identitas dari pengguna;
   c) Membatasi dan mengendalikan penggunaan *system utilities*;
   d) Fasilitas *session time-out* harus diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu; dan
   e) Membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.
6. Pengendalian kontrol akses ke aplikasi dan sistem informasi

a) Memastikan bahwa akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai peruntukannya; dan

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

7. Perangkat *Mobile* dan *teleworking*

a) Membangun kepedulian pengguna perangkat *mobile* akan risiko-risiko keamanan yang terus meningkat terhadap informasi yang tersimpan dalam perangkat *mobile*; dan

b) Menyusun prosedur pengendalian akses jarak jauh (*teleworking*).

D. STANDAR

1. Persyaratan untuk Pengendalian Kontrol Akses, mencakup:

a) Penentuan kebutuhan keamanan dari pengolah aset informasi; dan

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

2. Pengelolaan Kontrol Akses Pengguna

a) Penggunaan akun yang unik untuk mengaktifkan pengguna agar terhubung dengan sistem informasi atau layanan, dan pengguna dapat bertanggungjawab dalam penggunaan sistem informasi atau layanan. Penggunaan akun khusus hanya diperbolehkan sebatas yang diperlukan untuk kegiatan atau alasan operasional, dan harus disetujui Pejabat yang berwenang serta didokumentasikan;

b) Pemeriksaan bahwa pengguna memiliki otorisasi dari pemilik sistem untuk menggunakan sistem informasi atau layanan;

c) Pemeriksaan bahwa tingkat akses yang diberikan sesuai dengan tujuan kegiatan dan konsisten dengan kebijakan dan standar SMKI di Lingkungan Badan;

d) Pemastian penyedia layanan tidak memberikan akses

kepada pengguna sebelum prosedur otorisasi telah selesai;

e) Pemeliharaan catatan pengguna layanan yang terdaftar dalam menggunakan layanan;

f) Penghapusan atau penonaktifan akses pengguna yang telah berubah tugas dan/atau fungsinya, setelah penugasan berakhir atau mutasi;

g) Pemeriksaan, penghapusan, serta penonaktifan akun secara berkala dan untuk pengguna yang memiliki lebih dari 1 (satu) akun; dan

h) Membangun kesadaran pengguna bahwa akun tidak dipergunakan 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 pengelolaan basis data, 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 diutamakan untuk menghindari kebutuhan dalam memberikan hak akses khusus secara terus menerus kepada pengguna; dan

e) Hak akses khusus 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 perlu dikaji secara berkala atau setelah terjadi perubahan pada sistem atau struktur organisasi; dan

b) Pemeriksaan hak akses khusus dilakukan secara berkala,

untuk memastikan pemberian hak akses khusus telah di verfikasi atau telah selesai digunakan.

5. Pengendalian Akses jaringan
   a) Menerapkan pemberian akses ke jaringan dan layanan jaringan sesuai dengan ketentuan yang berlaku;
   b) Menerapkan Teknik autentikasi akses dari koneksi eksternal, seperti Teknik kriptografi, dan *dial-back*; dan
   c) Melakukan penghentian/isolasi layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.

6. Pemisahan dalam Jaringan

   Melakukan pemisahan dalam jaringan antara lain:
   a) Pemisahan berdasarkan kelompok layanan informasi, pengguna dan aplikasi; dan
   b) Pemberian akses jaringan kepada tamu, hanya dapat diberikan akses terbatas.

7. Perangkat *Mobile* dan *Teleworking*
   a) Penggunaan perangkat *mobile* dan *teleworking* harus mempertimbangkan;
      (1) Memenuhi keamanan informasi dalam penentuan lokasi;
      (2) Menjaga keamanan akses;
      (3) Menggunakan anti *malicious code*;
      (4) Memakai perangkat lunak berlisensi; dan
      (5) Mendapat persetujuan Pejabat yang berwenang/atasan langsung pegawai.
   b) Pencabutan hak akses dan pengembalian fasilitas perangkat *teleworking* apabila kegiatan telah selesai.

VIII. PENGENDALIAN KEAMANAN INFORMASI DALAM PENGADAAN, PENGEMBANGAN, DAN PEMELIHARAAN SISTEM INFORMASI

A. TUJUAN

Memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dengan sistem informasi, mencegah terjadinya kesalahan, kehilangan, serta modifikasi oleh pihak yang tidak

berwenang.

B. RUANG LINGKUP

Kebijakan dan standar keamanan informasi dalam pengadaan, pengembangan dan pemeliharaan sistem informasi, meliputi:

1. Keamanan Sistem Informasi;
2. Pengolahan informasi pada aplikasi;
3. Pengendalian penggunaan kriptografi;
4. Keamanan file sistem (*system files*);
5. Keamanan dalam proses pengembangan dan pendukung (*support proceses*); dan
6. Pengelolaan kerentanan teknis.

C. KEBIJAKAN

1. Keamanan Sistem Informasi:

   Menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengadaan, pengembangan, atau pemeliharaan sistem informasi baru.

2. Pengelolaan informasi pada aplikasi:
   a) Data yang akan dimasukkan ke aplikasi diperiksa terlebih dahulu kebenaran dan kesesuaiannya;
   b) Setiap aplikasi disertakan proses validasi untuk mendeteksi bahwa informasi yang dihasilkan utuh dan sesuai dengan yang diharapkan; dan
   c) Data keluaran aplikasi divalidasi untuk memastikan data yang dihasilkan adalah benar.
3. Pengendalian penggunaan kriptografi:
   a) Mengembangkan dan menerapkan sistem kriptografi untuk perlindungan informasi dan membuat rekomendasi yang tepat bagi penerapannya, dan
   b) Sistem kriptografi digunakan untuk melindungi aset informasi yang memiliki klasifikasi SANGAT RAHASIA, RAHASIA, dan TERBATAS.
4. Keamanan file system (*system file*)
   a) Mempunyai prosedur untuk pengendalian perangkat lunak pada sistem operasional;
   b) Menentukan sistem pengujian data, melindunginya dari

kemungkinan kerusakan, kehilangan atau perubahan oleh pihak yang tidak berwenang; dan

c) Mengendalikan ke kode program secara ketat dan salinan versi terkini dari perangkat lunak disimpan di tempat yang aman.

5. Keamanan dalam proses pengembangan dan pendukung (*support proceses*)
   a) Mengendalikan perubahan pada sistem operasi dengan penggunaan prosedur pengendalian perubahan;
   b) Mengendalikan perubahan terhadap perangkat lunak yang dikembangkan sendiri maupun pihak ketiga;
   c) Meninjau dan menguji sistem operasi dan/atau perangkat lunak untuk memastikan tidak ada dampak merugikan pada proses operasional atau keamanan informasi Badan pada saat terjadi perubahan sistem operasi dan/atau perangkat lunak, untuk informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA;
   d) Mencegah kemungkinan terjadinya kebocoran informasi; dan
   e) Melakukan supervisi dan memantau pengembangan perangkat lunak oleh pihak ketiga.
6. Pengelolaan kerentanan teknis
   a) Mengumpulkan informasi kerentanan teknis secara berkala dari seluruh sistem informasi yang digunakan maupun komponen pendukung sistem informasi; dan
   b) Melakukan evaluasi dan penilaian risiko terhadap kerentanan teknis yang ditemukan dalam sistem informasi serta menetapkan pengendalian yang tepat terhadap risiko terkait.

D. STANDAR
1. Spesifikasi kebutuhan perangkat pengolah informasi yang dikembangkan baik oleh internal atau pihak ketiga harus dikonsultasikan kepada Unit Pengelola TIK Badan dan ditentukan oleh internal serta didokumentasikan secara formal;
2. Pengembangan sistem informasi mengikuti standar dan

aturan yang sudah ditetapkan;

3. Pengolah Data pada Aplikasi

a) Pemeriksaan data masukan 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;

(e) Data yang tidak diotorisasi dan tidak konsisten; dan

(f) Duplikasi data atau data berulang;

(2) Pengkajian secara berkala terhadap isi *field* kunci (*key field*) atau field data untuk mengkonfirmasi keabsahan dan integritas data;

(3) Memeriksa dokumen *hardcopy* 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 dan 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) Validasi data masukan yang dihasilkan sistem;

(2) Aplikasi berjalan sesuai dengan rencana dan waktu yang ditentukan;

(3) Program dijalankan dalam urutan yang benar dan menghentikan sementara jika terjadi kegagalan

sampai masalah diatasi; dan

(4) Sistem mampu membuat dan mengeluarkan catatan aktivitas pengelolaan internal.

c) Pemeriksaan data keluaran 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) Menjabarkan tanggung jawab dari seluruh pegawai yang terkait proses data keluaran; dan

(6) Sistem mampu membuat dan mengeluarkan catatan aktivitas dalam proses validasi data keluaran.

4. Pengendalian dan Penggunaan Kriptografi untuk perlindungan informasi mempertimbangkan:

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

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

c) Keperluan enkripsi untuk perlindungan informasi kategori SANGAT RAHASIA, RAHASIA, dan TERBATAS yang melalui perangkat *mobile computing*, *removable media* atau jalur komunikasi;

5. Keamanan File Sistem

a) Pengembangan prosedur pengendalian perangkat lunak pada sistem operasional mempertimbangkan:

(1) Proses pemutakhiran perangkat lunak operasional, aplikasi dan *library* program hanya boleh dilakukan oleh *system administrator*;

(2) Aplikasi dan perangkat lunak sistem operasi hanya dapat diimplementasikan setelah melewati proses pengujian;
(3) Sistem pengendalian konfigurasi digunakan untuk mengendalikan seluruh perangkat lunak yang telah diimplementasikan beserta dokumentasi sistem;
(4) Versi terdahulu dari suatu aplikasi harus tetap disimpan untuk keperluan kontijensi; dan
(5) Versi lama dari suatu perangkat lunak harus diarsip, bersama dengan informasi terkait lainnya.

b) Perlindungan terhadap sistem pengujian data harus mempertimbangkan:
(1) Proses otorisasi setiap kali informasi/data operasional digunakan pada sistem pengujian;
(2) Penghapusan informasi/data operasional yang digunakan pada sistem pengujian segera setelah proses pengujian selesai;
(3) Pengendalian akses ke kode program (*source code*) harus mempertimbangkan:
(a) Proses pemutakhiran kode program (*source code*) dan item terkait serta pemberian kode program (*source code*) kepada *programmer* hanya dapat dilakukan setelah melalui proses otorisasi;
(b) Proses pemutakhiran kode program (*source code*) yang berjalan pada sistem aplikasi operasional hanya dapat dilakukan oleh *web administrator;*
(c) Pemeliharaan dan penyalinan kode program (*source code*) *library* mengikuti prosedur pengendalian perubahan; dan
(d) Jejak proses setiap pemutakhiran kode program (source code) harus tercatat dan terekam.

6. Keamanan dalam proses pengembangan dan pendukung (*support proceses*).
   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 *review* untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;
      (4) Melakukan identifikasi terhadap perangkat lunak, informasi, basis data, dan perangkat keras yang perlu diubah;
      (5) Memastikan permintaan perubahan sudah melalui prosedur yang berlaku;
      (6) Mendapatkan persetujuan formal dari pihak yang berwenang sebelum pelaksanaan perubahan;
      (7) Memastikan pihak yang berwenang menerima perubahan yang diminta dan memeriksa kesesuaian permintaan sebelum dilakukan implementasi;
      (8) Memastikan dokumentasi sistem mutakhir dan dokumen versi sebelumnya diarsip;
      (9) Memelihara versi perubahan aplikasi;
      (10) Memelihara jejak audit perubahan aplikasi; dan
      (11) Memastikan bahwa implementasi perubahan dilakukan tepat waktu dan tidak mengganggu kegiatan.
   b) Kegiatan kajian teknis aplikasi setelah perubahan sistem operasi dan/atau perangkat lunak, mencakup:
      (1) Melakukan *review* untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;
      (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) Kebocoran informasi

Pengendalian yang dapat diterapkan untuk membatasi risiko kebocoran informasi, antara lain:

(1) Melakukan pemantauan terhadap aktivitas pengelolaan sistem informasi yang dilakukan pegawai dan pihak ketiga sudah sesuai dengan ketentuan yang berlaku; dan

(2) Melakukan pemantauan terhadap aktivitas penggunaan *personal computer* dan perangkat *mobile*.

d) Pengembangan perangkat lunak oleh pihak ketiga harus mempertimbangkan:

(1) Perjanjian lisensi, kepemilikan source code, dan Hak Atas Kekayaan Intelektual (HAKI);

(2) Perjanjian *escrow*;

(3) Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan;

(4) Persyaratan kontrak mengenai audit terhadap kualitas dan fungsi keamanan aplikasi; dan

(5) Uji coba terhadap aplikasi untuk memastikan tidak terdapat *malicious code* sebelum implementasi.

7. Pengelolaan Kerentanan Teknis, mencakup:

a) Penentuan rentang waktu untuk melakukan aksi terhadap munculnya potensi kerentanan teknis. Apabila terjadi kerentanan teknis yang butuh penanganan maka diambil tindakan sesuai *control* yang telah ditetapkan atau melaporkan kejadian tersebut melalui pelaporan kejadian dan kelemahan keamanan informasi;

b) 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, perlu dilakukan hal sebagai berikut:

(1) Mematikan *services* 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.

c) Penyimpanan *audit log* yang memuat prosedur dan langkah-langkah yang telah diambil;

d) Pemantauan dan evaluasi terhadap pengelolaan kerentanan teknis dilakukan secara berkala; dan

e) Pengelolaan kerentanan teknis diutamakan terhadap sistem informasi yang memiliki tingkat risiko tinggi.

IX. PENGENDALIAN PENGELOLAAN GANGGUAN KEAMANAN INFORMASI

A. TUJUAN

Memastikan kejadian dan kelemahan keamanan informasi yang terhubung, dengan sistem informasi dikomunikasikan untuk dilakukan perbaikan, serta dilakukan pendekatan yang konsisten dan efektif agar dapat dihindari atau tidak terulang kembali.

B. RUANG LINGKUP

Kebijakan dan standar pengelolaan gangguan keamanan informasi meliputi:

1. Pelaporan kejadian dan kelemahan informasi; dan
2. Pengelolaan gangguan keamanan informasi dan perbaikannya.

C. KEBIJAKAN

1. Pelaporan kejadian dan kelemahan informasi

Pegawai dan pihak ketiga harus melaporkan kepada Unit Pemilik Aset Informasi sesegera mungkin pada saat menemukan kelemahan atau terjadi gangguan keamanan

informasi dalam sistem atau layanan TIK Badan.

2. Pengelolaan gangguan keamanan informasi dan perbaikannya
   a) Menyusun prosedur dan menguraikan tanggung jawab pegawai, terkait dalam rangka memastikan gangguan keamanan informasi dapat ditangani secara cepat dan efektif;
   b) Seluruh gangguan keamanan informasi yang terjadi dicatat dalam suatu basis data dan/atau buku catatan pelaporan gangguan keamanan informasi, yang menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi, serta dievaluasi dan dianalisa untuk perbaikan dan pencegahan agar gangguan keamanan informasi tidak terulang; dan
   c) Mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap kebijakan dan standar SMKI di Lingkungan Badan.

D. STANDAR

1. Pelaporan kejadian dan kelemahan keamanan informasi
   a) Gangguan keamanan informasi antara lain:
      (1) Hilangnya layanan, perangkat, atau fasilitas TIK;
      (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 pengolah informasi TIK;
      (6) Kelalaian manusia; dan
      (7) Ketidaksesuaian dengan ketentuan yang berlaku.
   b) Pegawai dan pihak ketiga melaporkan setiap gangguan keamanan informasi yang mencakup:
      (1) Formulir laporan gangguan keamanan informasi untuk mendukung tindakan pelaporan dan kronologis kejadian keamanan informasi;
      (2) Melaporkan gangguan yang terjadi kepada Unit Pemilik Aset Informasi sebelum melakukan tindakan penanganan sendiri;
      (3) Sebagai referensi yang dapat digunakan dalam

proses penanganan pelanggaran disiplin bagi pegawai atau pihak ketiga yang melakukan pelanggaran keamanan informasi; dan

(4) Mencatat semua rincian informasi gangguan, seperti jenis pelanggaran, jenis kerusakan, pesan pada layar atau anomali system, dan segera membuat laporan gangguan kepada Unit Pemilik Aset Informasi sebelum melakukan pengamanan sendiri.

2. Prosedur pengelolaan gangguan keamanan informasi harus mempertimbangkan:

a) Berbagai jenis gangguan keamanan informasi, antara lain:

(1) Kegagalan sistem informasi dan hilangnya layanan;

(2) Serangan program yang membahayakan (*malicious code*);

(3) Serangan *denial services*;

(4) Kesalahan akibat data tidak lengkap atau tidak akurat;

(5) Pelanggaran kerahasiaan dan keutuhan; dan

(6) Penyalahgunaan sistem informasi.

b) kegiatan rencana kontijensi mencakup:

(1) Analisis dan identifikasi penyebab gangguan;

(2) Membatasi gangguan;

(3) Melakukan perencanaan dan pelaksanaan tindakan korektif untuk mencegah gangguan berulang; dan

(4) Pelaporan tindakan ke pihak berwenang.

c) Bukti dan Jejak audit harus dikumpulkan dan diamankan;

d) Prosedur tindakan pemulihan keamanan dari pelanggaran dan perbaikan kegagalan sistem dikendalikan secara cermat untuk memastikan:

(1) Hanya pegawai yang memiliki hak akses dan berwenang yang diizinkan akses langsung ke sistem dan data;

(2) Semua tindakan darurat dilaporkan kepada pihak berwenang dan didokumentasikan secara rinci;

X. PENGENDALIAN KEAMANAN INFORMASI DALAM PENGELOLAAN KELANGSUNGAN KEGIATAN

A. TUJUAN

Melindungi sistem informasi, memastikan berlangsungnya kegiatan dan layanan pada saat keadaan darurat, serta memastikan pemulihan yang tepat.

B. RUANG LINGKUP

Kebijakan dan standar keamanan informasi dalam pengelolaan kelangsungan kegiatan ini meliputi:

1. Proses pengelolaan kelangsungan kegiatan;
2. Penilaian risiko dan analisis dampak bisnis;
3. Penyusunan dan penerapan rencana kelangsungan kegiatan; dan
4. Pengujian, pemeliharaan, dan pengkajian ulang rencana kelangsungan kegiatan

C. KEBIJAKAN

1. Mengelola proses kelangsungan kegiatan pada saat keadaan darurat di lingkungan Badan;
2. Mendefinisi risiko, dan menganalisis dampak yang diakibatkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan;
3. Menyusun dan menerapkan rencana kelangsungan kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan;
4. Memelihara dan memastikan rencana-rencana yang termuat dalam rencana kelangsungan kegiatan masih sesuai, dan mengidentifikasi prioritas untuk kegiatan uji coba; dan
5. Melakukan uji coba rencana kelangsungan kegiatan secara berkala untuk memastikan rencana kelangsungan kegiatan dapat dilaksanakan secara efektif.

D. STANDAR

1. Pengelolaan 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 Badan;
e) Penyusunan dan pendokumentasian rencana kelangsungan kegiatan harus disesuaikan dengan Rencana Strategis Badan; dan
f) Pelaksanaan uji coba dan pemeliharaan rencana kelangsungan kegiatan secara berkala.

2. Proses analisis dampak kegiatan harus melibatkan Unit Pemilik Aset Informasi dan dievaluasi secara berkala;
3. Uji coba rencana kelangsungan kegiatan harus dilaksanakan untuk memastikan setiap rencana yang disusun dapat dilakukan/dipenuhi pada saat penerapannya.
   a) Uji coba *recovery system* untuk memastikan sistem informasi dapat berfungsi kembali;
   b) Uji coba terhadap perangkat dan layanan yang disediakan oleh pihak ketiga; dan
   c) Uji coba secara keseluruhan mulai dari petugas/pegawai, peralatan, perangkat dan prosesnya.
   d) Jadwal uji coba, mencakup langkah-langkah dan waktu pelaksanaan uji coba serta proses pemeliharaannya.

XI. PENGENDALIAN KEPATUHAN

A. TUJUAN

Untuk menghindari pelanggaran terhadap peraturan perundangan yang terkait keamanan informasi.

B. RUANG LINGKUP

Kebijakan dan standar kepatuhan meliputi:

1. Kepatuhan terhadap peraturan perundangan yang terkait keamanan informasi;

2. Kepatuhan teknis; dan
3. Audit sistem informasi.

C. KEBIJAKAN

1. Kepatuhan terhadap peraturan perundang-undangan yang terkait keamanan informasi
   a) Seluruh pegawai dan pihak ketiga harus menaati peraturan perundang-undangan yang terkait dengan dengan keamanan informasi;
   b) Mengidentifikasi, mendokumentasikan, dan memelihara kemutakhiran semua peraturan perundang-undangan yang terkait dengan sistem keamanan informasi;
   c) Perangkat lunak yang dikelola Unit Pemilik Aset Informasi harus mematuhi ketentuan penggunaan lisensi. Pengadaan perangkat lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran;
   d) Rekaman milik Badan harus dilindungi dari kehilangan, kerusakan atau penyalahgunaan; dan
   e) Melindungi kepemilikan dan kerahasiaan data. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundang-undangan dan kesepakatan.
2. Kepatuhan teknis
   Melakukan pemeriksaan kepatuhan teknis secara berkala untuk menjamin efektivitas standar dan prosedur keamanan informasi yang ada di area operasional.
3. Audit sistem informasi
   a) Unit Pemilik Aset Informasi membuat perencanaan persyaratan, ruang lingkup, dan kegiatan audit yang melibatkan pemeriksaan sistem operasional untuk mengurangi kemungkinan risiko gangguan yang bisa terjadi terhadap kegiatan Badan selama proses audit;
   b) Penggunaan alat bantu (baik perangkat lunak maupun perangkat keras) untuk mengetahui kelemahan keamanan, memindai kata sandi, atau untuk melemahkan dan menerobos sistem keamanan informasi tidak diizinkan;
   c) Audit sistem informasi di Badan akan ditetapkan dalam

ketentuan tersendiri.

D. 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 (resmi/*official*) dan memiliki reputasi baik, untuk memastikan hak cipta tidak dilanggar;
   b) Memelihara daftar aset informasi 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 Teknis

   Sistem informasi diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan perangkat lunak telah diimplementasikan secara benar. Kepatuhan teknis juga mencakup pengujian penetrasi untuk mendeteksi kerentanan dalam sistem, dan memeriksa pengendalian akses untuk mencegah kerentanan diterapkan.

3. Kepatuhan terkait Audit Sistem Informasi

   Proses audit sistem informasi harus memperhatikan hal berikut:

   a) Persyaratan audit harus disetujui CISO;

b) Ruang lingkup pemeriksaan/audit harus disetujui dan dikendalikan pihak terkait;

c) Pemeriksaan perangkat lunak dan data dibatasi hanya 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 keharusan untuk menyimpan file tersebut di bawah persyaratan dokumentasi audit;

e) Semua akses dipantau dan dicatat untuk menghasilkan jejak audit dan untuk data dan sistem informasi sensitif harus mempertimbangkan pencatatan waktu (*time stamp*) pada jejak audit;

f) Semua prosedur, persyaratan dan tanggung jawab harus didokumentasikan; dan

g) Auditor harus *independent*.

BAB III

PENUTUP

Peraturan Badan ini ditetapkan sebagai pedoman dalam melindungi aset informasi Badan dari berbagai bentuk ancaman baik dari dalam maupun dari luar, dengan tujuan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.

Hal-hal yang sifatnya terlalu teknis dan spesifik yang belum diatur dalam Peraturan Badan ini, secara khusus akan diatur dalam pedoman, atau dapat dilaksanakan langsung sesuai dengan Standar Operasional Prosedur.

KEPALA BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA

ttd

JAZI EKO ISTIYANTO