BERITA NEGARA REPUBLIK INDONESIA

No.590, 2018 KPK. Sistem Manajemen Keamanan Informasi.

PERATURAN
KOMISI PEMBERANTASAN KORUPSI REPUBLIK INDONESIA
NOMOR 04 TAHUN 2018
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN KOMISI PEMBERANTASAN KORUPSI

DENGAN RAHMAT TUHAN YANG MAHA ESA

PIMPINAN K0MISI PEMBERANTASAN K0RUPSI REPUBLIK INDONESIA,

Menimbang : a. bahwa Komisi Pemberantasan Korupsi memiliki sistem elektronik yang berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara (kategori strategis);

b. bahwa dalam rangka melindungi serta menjaga kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) Aset Informasi Komisi Pemberantasan Korupsi, diperlukan Sistem Manajemen Keamanan Informasi yang menerapkan standar Keamanan Informasi sesuai dengan ketentuan peraturan perundang-undangan;

c. bahwa Keputusan Pimpinan Komisi Pemberantasan Korupsi Nomor KEP-166B/PKPK/11/2006 tentang Kebijakan dan Struktur Organisasi Keamanan Informasi pada Komisi Pemberantasan Korupsi sudah tidak sesuai lagi dengan kebutuhan dan perkembangan Sistem Manajemen Keamanan Informasi;

d. berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu ditetapkan Peraturan Komisi Pemberantasan Korupsi tentang Sistem Manajemen Keamanan Informasi di Lingkungan Komisi Pemberantasan Korupsi;

Mengingat : 1. Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 137, Tambahan Lembaran Negara Republik Indonesia Nomor 4250) sebagaimana diubah dengan Undang-Undang Nomor 10 Tahun 2015 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2015 tentang Perubahan atas Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 107, Tambahan Lembaran Negara Republik Indonesia Nomor 5698);

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);
3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
4. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 152, Tambahan Lembaran Negara Republik Indonesia Nomor 5071);
5. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
6. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan

Informasi (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 551);

7. Peraturan Komisi Pemberantasan Korupsi Nomor 08 Tahun 2013 tentang Pedoman Penyusunan Prosedur Operasi Baku (*Standard Operating Procedures*);
8. Peraturan Komisi Pemberantasan Korupsi Nomor 07 Tahun 2013 tentang Nilai-Nilai Dasar Pribadi, Kode Etik dan Pedoman Perilaku Komisi Pemberantasan Korupsi;
9. Peraturan Komisi Pemberantasan Korupsi Nomor PER-02 Tahun 2015 tentang Pedoman Umum Pengawasan Internal;
10. Peraturan Komisi Pemberantasan Korupsi Nomor 10 Tahun 2016 tentang Disiplin Pegawai dan Penasihat di Lingkungan Komisi Pemberantasan Korupsi (Berita Negara Republik Indonesia Tahun 2016 Nomor 1579);
11. Peraturan Komisi Pemberantasan Korupsi Nomor 03 Tahun 2017 tentang Pedoman Kearsipan di Lingkungan Komisi Pemberantasan Korupsi (Berita Negara Republik Indonesia Tahun 2017 Nomor 598);
12. Peraturan Komisi Pemberantasan Korupsi Nomor 07 Tahun 2017 tentang Pedoman Klasifikasi Keamanan dan Akses Arsip Dinamis di Lingkungan Komisi Pemberantasan Korupsi (Berita Negara Republik Indonesia Tahun 2017 Nomor 1073);
13. Peraturan Komisi Pemberantasan Korupsi Nomor 03 Tahun 2018 tentang Organisasi dan Tata Kerja Komisi Pemberantasan Korupsi (Berita Negara Republik Indonesia Tahun 2018 Nomor 286);

MEMUTUSKAN:

Menetapkan : PERATURAN KOMISI PEMBERANTASAN KORUPSI REPUBLIK INDONESIA TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN KOMISI PEMBERANTASAN KORUPSI.

BAB I

KETENTUAN UMUM

Bagian Kesatu

Definisi

Pasal 1

Dalam Peraturan Komisi ini yang dimaksud dengan:

1. Akses adalah tindakan untuk memperoleh Aset Informasi.
2. Arsip adalah rekaman kegiatan atau peristiwa dalam berbagai bentuk dan media sesuai dengan perkembangan teknologi Informasi dan komunikasi yang dibuat dan diterima oleh lembaga negara, pemerintah daerah, lembaga pendidikan, perusahaan, organisasi politik, organisasi kemasyarakatan, dan perseorangan dalam pelaksanaan kehidupan bermasyarakat, berbangsa, dan bernegara.
3. Aset adalah segala sesuatu yang memiliki nilai untuk Komisi dan karenanya membutuhkan suatu bentuk perlindungan.
4. Aset Informasi adalah Informasi yang memiliki nilai untuk Komisi dan karenanya membutuhkan suatu bentuk perlindungan.
5. *Back Up* adalah salinan duplikasi dari data atau keseluruhan data dari tempat penyimpanan data ke dalam tempat penyimpanan yang terpisah.
6. *Business Continuity Management* adalah mekanisme yang mengatur dan memastikan adanya tindakan yang dilakukan ketika aktivitas teknologi Informasi mengalami gangguan/hambatan (bencana) serta memastikan bahwa proses bisnis Komisi masih dapat berjalan dan pelayanan tidak terhenti.
7. *Business Continuity Plan* adalah strategi pemulihan bencana yang dirancang oleh Komisi.

8. *Contingency Planning Process* adalah pernyataan secara komprehensif mengenai tindakan yang akan diambil sebelum, selama, dan setelah terjadinya bencana.
9. *Document Management System* adalah Sistem Informasi yang digunakan untuk mengelola dokumen pada setiap *life cycle* dokumen tersebut.
10. Enkripsi adalah metode pengodean data agar komputer tidak dapat membaca atau menggunakan data.
11. *Event Log* adalah objek yang memungkinkan pengguna komputer untuk melihat status dari aplikasi keamanan dan proses dari suatu sistem dan melihat keterkaitannya.
12. Fasilitas Pengolahan Informasi adalah sebuah sistem, layanan, infrastruktur, atau suatu lokasi fisik yang melakukan pengolahan Informasi.
13. Hak Akses adalah izin yang diberikan untuk memperoleh Aset Informasi.
14. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non elektronik.
15. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, telecopy, atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
16. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) Aset Informasi untuk pencapaian visi dan misi Komisi.
17. Komisi Pemberantasan Korupsi yang selanjutnya disebut Komisi adalah lembaga negara yang dalam melaksanakan

tugas dan wewenangnya bersifat independen dan bebas dari pengaruh kekuasaan manapun sebagaimana dimaksud dalam Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi sebagaimana diubah dengan Undang-Undang Nomor 10 Tahun 2015 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2015 tentang Perubahan Perubahan atas Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi menjadi Undang-Undang.

18. Kriptografi adalah teknik yang mengubah data menjadi berbeda dari aslinya dengan menggunakan algoritma matematika sehingga orang yang tidak mengetahui kuncinya tidak akan dapat membongkar data tersebut.
19. *Malicious Software* yang selanjutnya disebut *Malware* adalah suatu program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer.
20. Media Informasi adalah segala bentuk atau alat yang dapat digunakan untuk menyalurkan dan/atau menyimpan Informasi dari pengirim kepada penerima Informasi.
21. *Patch* adalah perangkat lunak sederhana yang digunakan untuk memperbaiki kelemahan perangkat lunak utama.
22. Pegawai Komisi Pemberantasan Korupsi yang selanjutnya disebut Pegawai adalah Pegawai Komisi sebagaimana dimaksud dalam Peraturan Pemerintah Nomor 63 Tahun 2005 tentang Sistem Manajemen Sumber Daya Manusia Komisi Pemberantasan Korupsi sebagaiman telah diubah dengan Peraturan Pemerintah Nomor 14 Tahun 2017 tentang Perubahan Kedua atas Peraturan Pemerintah Nomor 63 Tahun 2005 tentang Sistem Manajemen Sumber Daya Manusia Komisi Pemberantasan Korupsi.
23. Penasihat Komisi Pemberantasan Korupsi yang selanjutnya disebut Penasihat adalah Tim Penasihat sebagaimana dimaksud dalam Peraturan Pemerintah Nomor 63 Tahun 2005 tentang Sistem Manajemen Sumber Daya Manusia Komisi Pemberantasan Korupsi

sebagaiman telah diubah dengan Peraturan Pemerintah Nomor 14 Tahun 2017 tentang Perubahan Kedua atas Peraturan Pemerintah Nomor 63 Tahun 2005 tentang Sistem Manajemen Sumber Daya Manusia Komisi Pemberantasan Korupsi.

24. Peran Pengendalian adalah tindakan pengendalian atau penerapan kontrol oleh seseorang dalam suatu peristiwa.
25. Perangkat Penunjang adalah peralatan dan suku cadang yang diperlukan untuk menjaga agar sistem tetap beroperasi.
26. Personil Komisi adalah Pimpinan, Penasihat, dan Pegawai Komisi.
27. Peta Pengendalian adalah pengelompokan kontrol dalam Peran Pengendalian.
28. Pihak Eksternal adalah pihak selain Personil Komisi.
29. Pimpinan Komisi Pemberantasan Korupsi yang selanjutnya disebut Pimpinan adalah Pimpinan Komisi sebagaimana dimaksud dalam Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi sebagaimana diubah dengan Undang-Undang Nomor 10 Tahun 2015 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2015 tentang Perubahan Perubahan atas Undang-Undang Nomor 30 Tahun 2002 tentang Komisi Pemberantasan Tindak Pidana Korupsi menjadi Undang-Undang.
30. *Platform Middleware* adalah perangkat lunak yang menyediakan layanan bagi aplikasi perangkat lunak yang tersedia di luar sistem operasi.
31. Risiko adalah kejadian atau kondisi yang dapat menimbulkan dampak negatif atau positif terhadap pencapaian sasaran kinerja Komisi.
32. Risiko Keamanan Informasi adalah kejadian atau kondisi yang dapat menimbulkan dampak negatif atau positif terhadap terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) Aset Informasi untuk pencapaian visi dan misi Komisi.

33. *Removable Media* adalah media penyimpanan data yang dapat dipindahkan (*portable*) dan dapat dihubungkan ke perangkat komputer serta dapat dilepas kembali tanpa membahayakan data di dalamnya.
34. *Restore* adalah memulihkan salinan data cadangan.
35. *Routing* adalah pengaturan lintasan komunikasi/data secara otomatis.
36. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
37. Sistem Informasi adalah kesatuan komponen yang terdiri dari lembaga, sumber daya manusia, perangkat keras, perangkat lunak, substansi data, dan Informasi yang terkait satu sama lain dalam satu mekanisme kerja untuk mengelola data dan Informasi.
38. Sistem Manajemen Keamanan Informasi adalah bagian dari keseluruhan sistem manajemen organisasi untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan Keamanan Informasi yang dibangun dengan pendekatan Risiko untuk mencapai visi dan misi Komisi.
39. *System Administrator* adalah seseorang yang mengelola sistem komputer dalam suatu organisasi.
40. *System Image* adalah isi dari cakram keras yang didalamnya terdapat sistem operasi dan aplikasi yang terinstal.
41. *System Operator* adalah seseorang yang mengelola pengoperasian sistem komputer atau layanan komunikasi elektronik tertentu.
42. *Technical Vulnerability* adalah sesuatu teknik yang bertalian dengan sistem komputer yang memungkinkan seseorang mengoperasikan dan menjalankannya dengan benar atau memungkinkan pihak yang tidak berwenang mengambil alih.

43. *Teleworking* adalah suatu aktivitas yang dilakukan oleh Personil Komisi untuk melakukan pekerjaan dari suatu tempat di luar gedung Komisi dan tidak terhubung ke jaringan internal dengan memanfaatkan teknologi komunikasi sehingga mendapatkan tingkatan Akses yang sama seperti saat bekerja di gedung Komisi.
44. *User Acceptance Test* adalah suatu proses pengujian oleh pengguna untuk menghasilkan dokumen yang dijadikan bukti bahwa *software* yang dikembangkan telah diterima oleh pengguna, apabila hasil pengujian sudah bisa dianggap memenuhi kebutuhan dari pengguna.

Bagian Kedua
Tujuan

Pasal 2

Sistem Manajemen Keamanan Informasi bertujuan:

a. mengendalikan Risiko dan manfaat Informasi untuk pencapaian sasaran Komisi melalui perlindungan kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) Aset Informasi;
b. meningkatkan komitmen terhadap pelaksanaan Sistem Manajemen Keamanan Informasi untuk mewujudkan Sistem Manajemen Keamanan Informasi sesuai dengan ketentuan peraturan perundang-undangan;
c. memperoleh sertifikasi Keamanan Informasi berdasarkan Standar Nasional Indonesia (SNI) ISO/IEC 27001:2013 Teknologi Informasi, Teknik Keamanan, Sistem Manajemen Keamanan Informasi, Persyaratan *(Information Technology, Security Techniques, Information Security Management Systems, Requirements*) dan ISO/IEC 27002:2013 *Information Technology, Security Techniques, Code of Practice for Information Security Controls;* dan
d. menerapkan Keamanan Informasi berdasarkan Standar Nasional Indonesia (SNI) ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 di lingkungan Komisi.

Bagian Ketiga
Ruang Lingkup

Pasal 3

Lingkup Peraturan Komisi ini mencakup:

a. komitmen Pimpinan dan kebijakan Sistem Manajemen Keamanan Informasi;
b. susunan organisasi Keamanan Informasi;
c. sasaran, Peran Pengendalian, dan Peta Pengendalian Sistem Manajemen Keamanan Informasi; dan
d. kerangka kerja Sistem Manajemen Keamanan Informasi.

BAB II
KOMITMEN PIMPINAN DAN KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 4

(1) Komitmen Pimpinan Komisi dalam Sistem Manajemen Keamanan Informasi diwujudkan dengan:
    a. memastikan Sistem Manajemen Keamanan Informasi dilaksanakan sesuai dengan Rencana Strategis Komisi;
    b. memastikan integrasi ketentuan Sistem Manajemen Keamanan Informasi terdapat dalam proses bisnis dan prosedur operasi baku Direktorat, Biro, dan unit kerja terkait;
    c. memastikan ketersediaan sumber daya yang dibutuhkan untuk Sistem Manajemen Keamanan Informasi;
    d. mengomunikasikan pentingnya Sistem Manajemen Keamanan Informasi yang efektif dan sesuai dengan ketentuan Sistem Manajemen Keamanan Informasi;
    e. memastikan Sistem Manajemen Keamanan Informasi sesuai tujuan Komisi;
    f. mengarahkan dan memberi dukungan terhadap Direktur/Kepala Biro dalam implementasi Sistem Manajemen Keamanan Informasi;

g. mendorong perbaikan Sistem Manajemen Keamanan Informasi secara berkelanjutan;
h. mendukung peran kepemimpinan kepala unit kerja di Komisi dalam melaksanakan tugas dan fungsi unit kerja; dan
i. memastikan tersedianya regulasi untuk mendukung pelaksanaan Sistem Manajemen Keamanan Informasi.

(2) Regulasi sebagaimana dimaksud pada ayat (1) huruf i, harus memenuhi unsur sebagai berikut:
a. sesuai dengan tujuan Komisi;
b. sesuai dengan tujuan dari Keamanan Informasi;
c. adanya komitmen untuk menetapkan ketentuan yang terukur terkait dengan Keamanan Informasi; dan
d. adanya komitmen untuk perbaikan yang berkelanjutan dari Sistem Manajemen Keamanan Informasi.

BAB III
SUSUNAN ORGANISASI KEAMANAN INFORMASI

Pasal 5

Susunan organisasi keamanan informasi dalam Sistem Manajemen Keamanan Informasi di lingkungan Komisi, sebagai berikut:

a. Komite Keamanan Informasi (*Information Security Committee/*ISC) yaitu Sekretaris Jenderal sebagai Ketua dan beranggotakan Deputi Bidang Informasi dan Data, Deputi Bidang Pencegahan, Deputi Bidang Penindakan, Deputi Bidang Pengawasan Internal dan Pengaduan Masyarakat, dan Direktur/Kepala Biro;
b. *Chief Security Officer* (CSO) yaitu Deputi Bidang Informasi dan Data;
c. *Chief Information Security Officer* (CISO) yaitu Direktur/Kepala Biro; dan

d. Sekretariat Keamanan Informasi *(Information Security Secretariat)* yaitu terdiri atas Pegawai pada Direktorat Pengolahan Informasi dan Data, Biro Sumber Daya Manusia, dan Biro Umum yang ditunjuk berdasarkan surat tugas.

Pasal 6

(1) Susunan keanggotaan organisasi keamanan informasi sebagaimana dimaksud dalam Pasal 5 berlaku secara *ex officio*.

(2) Apabila pejabat yang menduduki jabatan sedang berhalangan dan/atau tidak ada yang memegang jabatan maka secara *ex officio* digantikan oleh pelaksana tugas atau pelaksana harian yang ditunjuk berdasarkan Peraturan Komisi.

(3) Peranan, tugas, dan hubungan kerja pada organisasi keamanan informasi di lingkungan Komisi tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Komisi ini.

BAB IV

SASARAN, PERAN, DAN PETA PENGENDALIAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 7

(1) Sasaran pengendalian dalam Sistem Manajemen Keamanan Informasi di lingkungan Komisi, meliputi 14 (empat belas) area, yaitu:
   a. umum;
   b. organisasi Keamanan Informasi;
   c. sumber daya manusia;
   d. manajemen Media Informasi;
   e. pengendalian Akses;
   f. Kriptografi;
   g. keamanan fisik dan lingkungan;
   h. keamanan operasional;
   i. keamanan komunikasi;

j. sistem akuisisi, pengembangan, dan pemeliharaan;
k. hubungan dengan penyedia barang dan jasa;
l. manajemen insiden Keamanan Informasi;
m. *Business Continuity Management*; dan
n. kepatuhan.

(2) Pengendalian dalam Sistem Manajemen Keamanan Informasi dilaksanakan sesuai dengan peran, wewenang, dan tanggung jawab masing-masing pengendali sebagaimana tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Komisi ini.

BAB V
KERANGKA KERJA SISTEM MANAJEMEN KEAMANAN INFORMASI

Bagian Kesatu
Dukungan terhadap Sistem Manajemen Keamanan Informasi

Pasal 8

Untuk mendukung keberhasilan Sistem Manajemen Keamanan Informasi, ditentukan sebagai berikut:

a. Sekretaris Jenderal menetapkan dan menyediakan sumber daya yang diperlukan untuk pengembangan, pelaksanaan, pemeliharaan, dan perbaikan yang berkesinambungan dalam Sistem Manajemen Keamanan Informasi;
b. Kepala Biro Sumber Daya Manusia yang selanjutnya disebut Kepala Biro SDM dan Komite Keamanan Informasi menjamin terbentuknya pemahaman dan pelaksanaan tanggung jawab Keamanan Informasi sesuai dengan peran masing-masing;
c. Direktur dan Kepala Biro memastikan Personil Komisi dan Pihak Eksternal menyadari dan memenuhi tanggung jawabnya terhadap Keamanan Informasi;
d. Kepala Biro SDM memastikan tersedianya sumber daya manusia yang kompeten dalam pengelolaan Keamanan

Informasi;

e. Kepala Biro Hubungan Masyarakat yang selanjutnya disebut Kepala Biro Humas bekerja sama dengan Komite Keamanan Informasi memastikan berjalannya komunikasi yang diperlukan dalam pelaksanaan Sistem Manajemen Keamanan Informasi;

f. Direktur dan Kepala Biro bekerja sama dengan Kepala Biro Umum untuk mendokumentasikan Informasi sesuai dengan ketentuan kearsipan Komisi;

g. Direktur dan Kepala Biro bekerja sama dengan Kepala Biro Umum dalam menetapkan Aset Informasi berupa dokumentasi Informasi yang meliputi:
   1. Informasi yang diarsipkan;
   2. penentuan klasifikasi Informasi yang diperlukan oleh Komisi untuk efektivitas Sistem Manajemen Keamanan Informasi; dan
   3. klasifikasi Informasi sesuai dengan ketentuan kearsipan Komisi.

h. Direktur dan Kepala Biro bekerja sama dengan Kepala Biro Umum untuk menetapkan pembuatan dan perubahan dokumentasi informasi, harus memastikan:
   1. identifikasi dan deskripsi;
   2. format; dan
   3. pengendalian dokumen.

i. Direktur dan Kepala Biro bekerja sama dengan Kepala Biro Umum mendokumentasikan informasi yang diperlukan oleh Sistem Manajemen Keamanan Informasi untuk memastikan:
   1. ketersediaan dan kesesuaian waktu serta lokasi penggunaannya; dan
   2. terlindungi sesuai dengan standar yang berlaku.

j. Direktur dan Kepala Biro bekerja sama dengan Kepala Biro Umum untuk mengendalikan dokumentasi Informasi dengan penanganan terhadap aktivitas, meliputi:
   1. distribusi, Akses, pengambilan, dan penggunaan;
   2. penyimpanan dan pemeliharaannya;
   3. pengendalian terhadap perubahan; dan

4. retensi serta relokasi Informasi.

Bagian Kedua
Tahapan Proses

Pasal 9

Sistem Manajemen Keamanan Informasi dilaksanakan dengan 4 (empat) tahapan sebagai berikut:

a. perencanaan;
b. implementasi;
c. evaluasi; dan
d. perbaikan.

Pasal 10

(1) Perencanaan sebagaimana dimaksud dalam Pasal 9 huruf a mencakup, proses penetapan peraturan, tujuan, proses, dan prosedur Sistem Manajemen Keamanan Informasi dalam rangka mengelola Risiko Keamanan Informasi sesuai dengan ketentuan peraturan perundang-undangan.
(2) Dalam menentukan tujuan sebagaimana dimaksud pada ayat (1) harus memenuhi kriteria sebagai berikut:
    a. selaras dan terukur dengan Sistem Manajemen Keamanan Informasi;
    b. memperhitungkan ketentuan Keamanan Informasi, hasil identifikasi, evaluasi, analisis, serta penanganan Risiko; dan
    c. mempertimbangkan isu eksternal dan internal, serta isu yang mempengaruhi kemampuan untuk mencapai sasaran Komisi berdasarkan Manajemen Risiko Komisi.
(3) Tujuan sebagaimana dimaksud pada ayat (2) harus dikomunikasikan kepada Personil Komisi dan diperbarui oleh Komite Keamanan Informasi.
(4) Dalam rangka mengelola Risiko Keamanan Informasi dalam tahap perencanaan sebagaimana dimaksud pada ayat (1), Komite Keamanan Informasi berwenang:

a. menentukan kegiatan untuk mengatasi Risiko Keamanan Informasi;
b. mengintegrasikan dan menerapkan kegiatan yang diperlukan dalam proses Sistem Manajemen Keamanan Informasi;
c. mengevaluasi efektivitas kegiatan yang dimaksud dalam huruf a dan huruf b; dan
d. menetapkan dan menerapkan penilaian serta perlakuan Risiko Keamanan Informasi berdasarkan Manajemen Risiko Komisi.

(5) Implementasi sebagaimana dimaksud dalam Pasal 9 huruf b mencakup pelaksanaan proses, prosedur, dan pengendalian terkait Sistem Manajemen Keamanan Informasi.

(6) Evaluasi sebagaimana dimaksud dalam Pasal 9 huruf c mencakup proses penilaian dan pengukuran kinerja pelaksanaan Sistem Manajemen Keamanan Informasi untuk dilaporkan kepada Pimpinan.

(7) Perbaikan sebagaimana dimaksud dalam Pasal 9 huruf d merupakan kegiatan perbaikan yang berkesinambungan sebagai tindak lanjut hasil audit atau evaluasi terhadap Sistem Manajemen Keamanan Informasi.

Pasal 11

Implementasi Sistem Manajemen Keamanan Informasi dilakukan oleh Komisi sebagai berikut:

a. unit kerja wajib menyusun dan melaksanakan rencana kegiatan serta melakukan pengendalian kegiatan untuk memenuhi ketentuan Sistem Manajemen Keamanan Informasi;
b. unit kerja wajib menjaga Arsip yang diperlukan untuk memastikan pelaksanaan kegiatan telah sesuai dengan yang direncanakan;
c. unit kerja wajib mengendalikan perubahan yang telah direncanakan dan mereviu konsekuensi dari perubahan serta mengambil tindakan mitigasi yang diperlukan;

d. unit kerja wajib mengendalikan dan bertanggung jawab atas Keamanan Informasi sehubungan dengan kegiatan Pihak Eksternal yang berhubungan dengan Komisi; dan
e. unit kerja wajib melaksanakan penilaian Risiko Keamanan Informasi secara berkala maupun apabila terjadi perubahan yang berdampak signifikan.

Pasal 12

Direktorat Pengawasan Internal melakukan evaluasi kinerja Keamanan Informasi dengan menetapkan hal-hal sebagai berikut:

a. objek dan ruang lingkup yang perlu dipantau dan diukur, termasuk proses dan kendali Keamanan Informasi;
b. metode pemantauan, pengukuran, analisis, dan evaluasi untuk memastikan hasil yang valid;
c. waktu pemantauan dan pengukuran;
d. pihak yang melakukan pemantauan dan pengukuran;
e. waktu hasil dari pemantauan dan pengukuran untuk dianalisis serta dievaluasi;
f. pihak yang melakukan analisis dan evaluasi hasil pemantauan serta pengukuran;
g. pengendalian Keamanan Informasi terhadap Informasi disesuaikan dengan klasifikasi Informasi; dan
h. mengidentifikasi Informasi dan mendefinisikan penanggung jawab pengendali Keamanan Informasi;

Pasal 13

Hasil evaluasi yang dilakukan Direktorat Pengawasan Internal sebagaimana dimaksud dalam Pasal 12, menjadi bahan pertimbangan bagi Pimpinan untuk menentukan arah dan kebijakan Sistem Manajemen Keamanan Informasi selanjutnya.

Pasal 14

(1) Direktorat Pengawasan Internal melakukan audit internal terhadap unit kerja lain secara berkala untuk memastikan Sistem Manajemen Keamanan Informasi

dilaksanakan dan dikelola secara efektif sesuai dengan ketentuan peraturan perundang-undangan dan ketentuan internal mengenai Keamanan Informasi Komisi.

(2) Pimpinan menetapkan tim audit untuk melakukan audit terhadap Sistem Manajemen Keamanan Informasi yang dilaksanakan di lingkungan Direktorat Pengawasan Internal yang anggotanya terdiri atas Personil Komisi yang memiliki kompetensi dalam bidang audit selain yang berasal dari Direktorat Pengawasan Internal.

(3) Tim audit sebagaimana dimaksud pada ayat (2) dibantu dan didampingi oleh tim teknis yang terdiri atas Personil Komisi yang memiliki kompetensi dalam bidang hukum serta Personil Komisi yang memiliki kompetensi dalam bidang teknologi Informasi.

Pasal 15

Audit internal Sistem Manajemen Keamanan Informasi berdasarkan ketentuan dalam Pedoman Umum Pengawasan Internal yang mencakup:

a. perencanaan, penetapan, penerapan pengelolaan, periode pelaksanaan audit, metode, tanggung jawab, dan pelaporan;
b. pertimbangan objek pemeriksaan yang penting dan hasil audit sebelumnya;
c. penentuan kriteria dan ruang lingkup audit;
d. penentuan tim auditor internal untuk memastikan pelaksanaan audit dilakukan secara objektif dan tidak berpihak;
e. pelaporan hasil audit kepada Pimpinan dan unit kerja terkait; dan
f. pengarsipan kegiatan dan hasil audit.

Pasal 16

Dalam hal terjadi ketidaksesuaian terhadap Sistem Manajemen Keamanan Informasi maka Komisi:

a. mengambil tindakan untuk menghilangkan penyebab

ketidaksesuaian dengan Sistem Manajemen Keamanan Informasi untuk mencegah terulangnya kembali ketidaksesuaian tersebut dengan mempertimbangkan konsekuensinya;

b. melakukan evaluasi tindakan yang diperlukan untuk menghilangkan penyebab ketidaksesuaian Sistem Manajemen Keamanan Informasi agar hal tersebut tidak berulang melalui:
   1. reviu;
   2. menentukan penyebab ketidaksesuaian; dan
   3. menentukan ketidaksesuaian yang serupa atau dapat terjadi lagi;
c. mengimplementasikan semua tindakan yang diperlukan;
d. mereviu efektivitas semua tindakan perbaikan yang dilakukan; dan
e. membuat perubahan Sistem Manajemen Keamanan Informasi jika diperlukan.

Pasal 17

(1) Komite Keamanan Informasi secara efektif wajib melakukan perbaikan terhadap penyimpangan dalam pelaksanaan Sistem Manajemen Keamanan Informasi.
(2) Dalam rangka perbaikan sebagaimana dimaksud pada ayat (1), Sekretariat Keamanan Informasi mendokumentasikan Informasi yang membuktikan:
   a. penyebab dari penyimpangan Sistem Manajemen Keamanan Informasi dan tindak lanjut yang dilakukan; dan
   b. hasil dari setiap upaya perbaikan.

BAB VI
LAIN-LAIN

Pasal 18

(1) Teknis pelaksanaan Sistem Manajemen Keamanan Informasi dituangkan dalam bentuk pedoman dan/atau prosedur.

(2) Ketentuan lebih lanjut mengenai bentuk pelanggaran dan sanksi yang berkaitan dengan Sistem Manajemen Keamanan Informasi diatur dengan Peraturan Komisi.

BAB VII
KETENTUAN PENUTUP

Pasal 19

Peraturan Komisi ini mulai berlaku sejak tanggal diundangkan.

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

Ditetapkan di Jakarta
pada tanggal 17 April 2018

PIMPINAN KOMISI PEMBERANTASAN KORUPSI
REPUBLIK INDONESIA,

ttd.

AGUS RAHARDJO

Diundangkan di Jakarta
pada tanggal 3 Mei 2018

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

ttd.

WIDODO EKATJAHJANA

LAMPIRAN I
PERATURAN
KOMISI PEMBERANTASAN KORUPSI
REPUBLIK INDONESIA
NOMOR 04 TAHUN 2018
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI

PERANAN, TUGAS, DAN HUBUNGAN KERJA
ORGANISASI KEAMANAN INFORMASI

I. Peranan dan Tugas

A. Komite Keamanan Informasi/*Information Security Committee* (ISC) berperan dalam melakukan evaluasi terhadap penerapan kebijakan dan efektivitas Keamanan Informasi dan memiliki tugas:

1. melaksanakan evaluasi atas pelaksanaan pengamanan Informasi termasuk menilai kepatuhan seluruh unit kerja terhadap kebijakan pengamanan Informasi dan merekomendasikan pengendalian yang perlu dilakukan;
2. melakukan koordinasi dan sinkronisasi perumusan dan penerapan kebijakan dan standar Keamanan Informasi;
3. melakukan koordinasi dan komunikasi dengan pihak terkait;
4. melakukan penyerapan dan penanganan aspirasi terkait Keamanan Informasi di lingkungan Komisi sebagai bahan evaluasi; dan
5. menyampaikan hasil evaluasi atas penerapan kebijakan Keamanan Informasi dan memberikan rekomendasi kepada Pimpinan untuk menjadi bahan pertimbangan dalam merumuskan kebijakan Keamanan Informasi sebagai bagian dari Rencana Strategis Komisi, efektivitas implementasi kebijakan pengamanan Informasi, dan efektivitas langkah-langkah mitigasi Risiko yang dilakukan untuk meningkatkan pengamanan Informasi bagi Personil Komisi yang dituangkan lebih lanjut dalam peraturan perundang-undangan.

B. *Chief Security Officer* (CSO) berperan sebagai penanggung jawab atas pelaksanaan Keamanan Informasi di lingkungan Komisi dan memiliki tugas:

1. menyampaikan usulan rumusan kebijakan, standar, dan pelaksanaan Keamanan Informasi kepada Komite Keamanan Informasi/*Information Security Committee* (ISC) berdasarkan masukan dari CISO;
2. melakukan pengelolaan fungsi pengamanan Informasi agar sesuai dengan kebijakan dan ketentuan serta standar yang berlaku;
3. memelihara dan mengendalikan penerapan kebijakan dan standar Keamanan Informasi di seluruh area yang menjadi tujuan/sasaran pengendalian;
4. memastikan efektivitas dan konsistensi penerapan kebijakan dan standar Keamanan Informasi dan mengukur kinerja keseluruhan;
5. pemantauan pelaksanaan pengamanan Informasi di setiap unit kerja dan memastikan pengamanan Informasi yang diterapkan sesuai dengan standar;
6. mengomunikasikan program pengamanan Informasi termasuk melakukan upaya peningkatan kesadaran pengamanan (*security awareness program*) dan memberikan arahan serta konsultasi atas penerapan kebijakan Keamanan Informasi; dan
7. melaporkan hasil kinerja kepada Komite Keamanan Informasi/*Information Security Committee* (ISC) dan Pimpinan.

C. *Chief Information Security Officer* (CISO) berperan sebagai penanggung jawab atas seluruh pelaksanaan Keamanan Informasi di masing-masing unit kerja dan memiliki tugas:

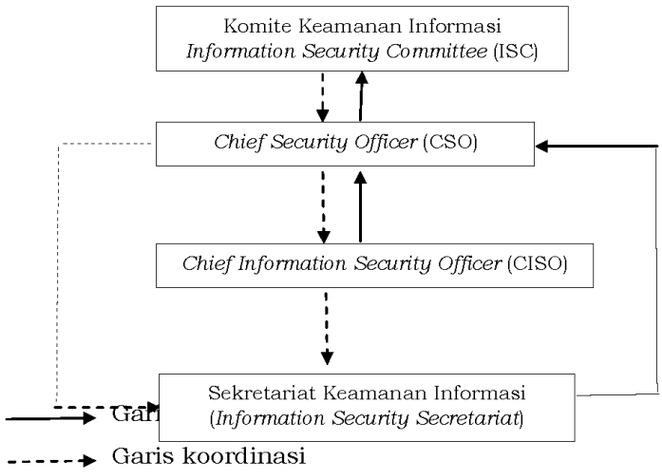
1. memastikan pelaksanaan kebijakan dan standar Keamanan Informasi secara efektif di unit kerja masing-masing;
2. mengidentifikasikan dan mengkaji secara berkala pelaksanaan Keamanan Informasi di unit kerja masing-masing;

3. memberikan arahan dan konsultasi atas penerapan kebijakan Keamanan Informasi di unit kerja masing-masing;
4. melakukan sosialisasi dan pelatihan tentang Keamanan Informasi di unit kerja masing-masing;
5. menentukan jenis dan klasifikasi Informasi di unit kerja masing-masing sesuai ketentuan Keamanan Informasi;
6. mengelola dan mengendalikan Aset Informasi di unit kerja masing-masing;
7. mengoordinasikan penanganan gangguan Keamanan Informasi pada unit kerja masing-masing;
8. memberikan masukan atas rumusan kebijakan, standar Keamanan Informasi, dan pelaksanaan Keamanan Informasi kepada CSO;
9. memastikan terlaksananya evaluasi terhadap penerapan kebijakan dan standar Keamanan Informasi di unit kerja masing-masing;
10. melakukan koordinasi dengan CSO dan pihak-pihak terkait dalam pengelolaan Informasi di unit masing-masing; dan
11. melaporkan penerapan kebijakan dan pelaksanaan Keamanan Informasi di unit kerja masing-masing kepada CSO.

D. Sekretariat Keamanan Informasi/*Information Security Secretariat* (ISS)
1. berperan sebagai administrator dalam pelaksanaan Keamanan Informasi;
2. mengumpulkan dan mengelola data, materi, dan laporan kegiatan Keamanan Informasi dari masing-masing unit kerja melalui CISO;
3. membantu pelaksanaan sosialisasi dan pelatihan Keamanan Informasi yang dilakukan CISO;
4. melaporkan hasil kegiatan kepada CSO;
5. menyiapkan dan mendistribusikan data dan materi untuk dibahas dalam rapat Komite Keamanan Informasi/*Information Security Committee* (ISC); dan
6. mengadministrasikan dan mendistribusikan hasil rapat Komite Keamanan Informasi/*Information Security Committee*

(ISC) kepada CISO dan membuat laporan hasil rapat Komite Keamanan Informasi/*Information Security Committee* (ISC) dan CSO.

II. Hubungan Kerja



LAMPIRAN II

PERATURAN
KOMISI PEMBERANTASAN KORUPSI REPUBLIK INDONESIA
NOMOR 04 TAHUN 2018
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI

PERAN PENGENDALI DAN PETA PENGENDALIAN
SISTEM MANAJEMEN KEAMANAN INFORMASI KOMISI

I. UMUM

A. Tujuan

Memberikan arah dan dukungan terhadap pengelolaan Keamanan Informasi sesuai dengan kepentingan Komisi dan ketentuan hukum yang berlaku.

B. Kebijakan

1. Dokumen terkait ketentuan Sistem Manajemen Keamanan Informasi harus terdefinisi, disetujui oleh Komite Keamanan Informasi, diterbitkan, dan dikomunikasikan kepada Personil Komisi dan Pihak Eksternal, sebagai berikut:
   a. Komite Keamanan Informasi menyusun ketentuan-ketentuan terkait keamanan Aset Informasi termasuk Fasilitas Pengolahan Informasi; dan
   b. Unit Kerja Pusat Edukasi Antikorupsi atau *Anti-Corruption Learning Center* yang selanjutnya disingkat ACLC membuat program pendidikan dan pelatihan tentang ketentuan Sistem Manajemen Keamanan Informasi kepada Personil Komisi misalnya induksi, program peningkatan kesadaran (*awareness*), atau pendidikan dan pelatihan.
2. Dokumen terkait Sistem Manajemen Keamanan Informasi harus direviu baik secara berkala atau sewaktu-waktu jika terjadi perubahan yang signifikan untuk memastikan kesesuaian, kecukupan, dan efektivitasnya.

II. ORGANISASI KEAMANAN INFORMASI

A. Tujuan

Membentuk kerangka kerja dalam Sistem Manajemen Keamanan Informasi.

B. Kebijakan

1. Pembuatan kerangka kerja Sistem Manajemen Keamanan Informasi dalam rangka menjalankan dan mengendalikan pelaksanaan Sistem Manajemen Keamanan Informasi agar peran, tanggung jawab, dan wewenang masing-masing unit kerja dapat didefinisikan dan dialokasikan sebagai berikut:
   a. unit kerja bertanggung jawab terhadap Keamanan Informasi di unit kerjanya masing-masing; dan
   b. unit kerja harus membuat panduan perlindungan Aset Informasi dalam melaksanakan Sistem Manajemen Keamanan Informasi di unit kerjanya.
2. Pemisahan area kerja Personil Komisi sesuai tugas dan tanggung jawabnya untuk mengurangi peluang terjadinya pemodifikasian yang tidak sah atau tidak disengaja atau terjadinya penyalahgunaan terhadap Aset Informasi sebagai berikut:
   a. unit kerja menerapkan pemisahan tugas (*segregation of duties);* dan
   b. unit kerja melakukan pengawasan terkait otorisasi Akses Personil Komisi di unit kerjanya.
3. Menjalin dan membina kontak dengan pihak yang memiliki otoritas (*authorities)* yang relevan dilakukan dengan:
   a. Komite Keamanan Informasi membuat dan menjalankan *Business Continuity Plan* dan *Contingency Planning Process;*
   b. Komite Keamanan Informasi membentuk dan menetapkan *Business Continuity Management*; dan
   c. Komite Keamanan Informasi membuat daftar pihak yang memiliki otoritas terkait penanganan keamanan informasi dan diperbarui secara berkala.

4. Menjalin dan membina kontak dengan kelompok/komunitas yang berkepentingan khusus atau forum spesialis Keamanan Informasi lain, sebagai berikut:
   a. Komite Keamanan Informasi dapat mengikuti forum, kegiatan, atau menjadi anggota kelompok/komunitas khusus terkait teknologi dan Keamanan Informasi; dan
   b. Komite Keamanan Informasi dapat merekomendasikan substansi (klausul) perlindungan Informasi rahasia pada perjanjian pertukaran Informasi dalam rangka peningkatan kerja sama dan koordinasi terkait masalah Keamanan Informasi.
5. Keamanan Informasi harus tercantum dan dilaksanakan dalam pengelolaan kegiatan yang dilaksanakan oleh unit kerja, sebagai berikut:
   a. setiap unit kerja mengidentifikasi Risiko Keamanan Informasi sebagai bagian dari pengelolaan kegiatan;
   b. setiap unit kerja melakukan mitigasi Risiko Keamanan Informasi dalam pengelolaan kegiatan dengan beserta penanggungjawabnya; dan
   c. setiap unit kerja mereviu kegiatan identifikasi dan mitigasi Risiko Keamanan Informasi secara berkala.
6. Dalam hal dilakukan *Teleworking*, dilakukan pengamanan sebagai berikut:
   a. Direktorat Pengolahan Informasi dan Data yang selanjutnya disebut Direktorat PINDA memberikan perlindungan khusus pada perangkat bergerak dengan memperhitungkan Risiko apabila bekerja dengan perangkat bergerak di lingkungan yang tidak terlindungi; dan
   b. ACLC melaksanakan sosialisasi dan pendidikan serta pelatihan untuk Personil Komisi yang menggunakan perangkat bergerak untuk meningkatkan kesadaran atas Keamanan Informasi.
7. Pedoman dan dukungan Keamanan Informasi yang terukur dijalankan untuk melindungi Aset Informasi yang diakses, diproses, atau disimpan di lokasi *Teleworking,* sebagai berikut:

a. Direktorat PINDA membuat pedoman untuk melindungi Aset Informasi yang diakses, diproses, atau disimpan di dalam area *Teleworking* termasuk mendefinisikan kondisi dan pembatasan penggunaan *Teleworking*;
b. Direktorat PINDA menerapkan pedoman *Teleworking;* dan
c. Direktorat PINDA menyediakan dukungan keamanan terkait *Teleworking*.

III. SUMBER DAYA MANUSIA

A. Tujuan

Memberikan pedoman bagi Personil Komisi untuk memahami tanggung jawab dalam pelaksanaan Sistem Manajemen Keamanan Informasi sesuai dengan peran masing-masing.

B. Kebijakan

1. Pemeriksaan dan verifikasi latar belakang calon Personil Komisi dan Pihak Eksternal sesuai dengan ketentuan hukum sebagai berikut:
   a. Biro SDM membuat prosedur rekrutmen dan seleksi Personil Komisi;
   b. Biro SDM melakukan verifikasi terhadap latar belakang semua Personil Komisi atau Pihak Eksternal sesuai dengan ketentuan Komisi;
   c. Biro SDM memberikan perlindungan terhadap Keamanan Informasi pribadi;
   d. Biro SDM membantu memberikan Informasi data pribadi dalam proses verifikasi akses Personil Komisi ke Fasilitas Pengolahan Informasi apabila Personil Komisi ditempatkan ke bagian lain atau berhenti sebagai Personil Komisi; dan
   e. Direktorat PINDA dan Biro SDM melakukan verifikasi terhadap latar belakang Pihak Eksternal sesuai dengan ketentuan Komisi.
2. Personil Komisi dan Pihak Eksternal membuat pernyataan terkait tanggung jawab atas Keamanan Informasi mengenai

Akses ke Informasi Rahasia yang diberikan dan Akses ke Fasilitas Pengolahan Informasi sesuai izin yang diberikan pihak berwenang dilakukan:

a. Biro SDM dan Direktorat Pengawasan Internal mengomunikasikan peran dan tanggung jawab terhadap Keamanan Informasi kepada calon Personil Komisi selama proses rekrutmen dan seleksi;
b. Biro SDM, Direktorat Pengawasan Internal, atau unit terkait meminta Personil Komisi untuk menandatangani perjanjian kerahasiaan *(non-disclosure agreement*) sebelum memberi Akses ke Fasilitas Pengolahan Informasi dan Informasi rahasia; dan
c. Biro SDM dan Direktorat Pengawasan Internal menyusun pedoman kode etik (*code of conduct*) terkait tanggung jawab Keamanan Informasi oleh Personil Komisi yang terkait kerahasiaan, perlindungan Aset Informasi, etika, dan penggunaan yang tepat dari peralatan dan fasilitas Komisi.

3. Personil Komisi dan Pihak Eksternal harus menyadari dan memenuhi tanggung jawab terhadap Keamanan Informasi dan menerapkan Keamanan Informasi sesuai dengan ketentuan Sistem Manajemen Keamanan Informasi, dilakukan:
   a. Direktorat Pengawasan Internal menyediakan saluran pelaporan anonim untuk melaporkan adanya pelanggaran (*whistle blowing*);
   b. Direktorat Pengawas Internal dan Direktorat PINDA memberikan sosialisasi terkait peran, tanggungjawab, kesadaran, ekspektasi, syarat kondisi kerja, dan motivasi terkait Keamanan Informasi sebelum Personil Komisi dan Pihak Eksternal diberikan Akses ke Fasilitas Pengolahan Informasi atau Sistem Informasi rahasia; dan
   c. ACLC memberikan pendidikan dan pelatihan untuk mengembangkan keahlian yang sesuai dengan kualifikasi terkait Keamanan Informasi.
4. Personil Komisi dan Pihak Eksternal yang relevan menerima pendidikan dan pelatihan yang tepat dan mendapatkan

Informasi terkini atas prosedur dan pedoman Keamanan Informasi secara berkala, sesuai dengan tugas dan fungsi masing-masing, sebagai berikut:

a. Direktorat PINDA memberikan materi terkait prosedur Keamanan Informasi tingkat dasar dan keamanan kata sandi (*password*), kontrol *Malware* dan meja kerja *(clean desk)*, pelatihan teknologi Informasi, atau pelatihan keamanan secara umum;
b. ACLC memberikan pendidikan dan pelatihan untuk meningkatkan kesadaran atas Keamanan Informasi, diantaranya menggunakan metode seperti pertemuan dalam kelas, pembelajaran jarak jauh, berbasis web, belajar mandiri, dan lain-lain; dan
c. unit kerja memberikan informasi terkini atas prosedur Keamanan Informasi yang relevan dengan fungsi pekerjaan mereka kepada Pihak Eksternal yang relevan.

5. Pimpinan Komisi memberikan tindakan indisipliner terhadap Personil Komisi dan peringatan kepada Pihak Eksternal yang telah melakukan pelanggaran Keamanan Informasi, dilakukan:
   a. Direktorat Pengawasan Internal melakukan proses pendisiplinan terhadap Personil Komisi dan memberikan peringatan kepada Pihak Eksternal yang telah melakukan pelanggaran Keamanan Informasi; dan
   b. Direktorat Pengawasan Internal mengomunikasikan kejadian pelanggaran Keamanan Informasi serta proses pengendalian yang dilakukan oleh Komisi melalui cara dan saluran komunikasi yang tepat kepada Personil Komisi sebagai upaya pencegahan terjadinya pelanggaran yang sama.
6. Apabila terjadi proses perubahan atau terminasi hubungan kerja maka dilakukan langkah-langkah untuk melindungi kepentingan Komisi dengan mendefinisikan, mengomunikasikan, dan tetap memberlakukan tanggung jawab serta tugas Keamanan Informasi kepada Personil Komisi dan Pihak Eksternal, sebagai berikut:

a. Direktur atau Kepala Biro (selaku CISO) bertanggung jawab terhadap proses perubahan atau terminasi hubungan kerja, dengan memberikan informasi kepada Personil Komisi dan berkoordinasi dengan Deputi Bidang Informasi dan Data (selaku CSO) dalam upaya mengawasi Personil Komisi yang ditentukan untuk mengelola aspek Keamanan Informasi sesuai dengan prosedur; dan

b. Direktur atau Kepala Biro (selaku CISO) bertanggung jawab terhadap proses perubahan atau terminasi hubungan kerja dengan memberikan informasi kepada Pihak Eksternal dan berkoordinasi dengan Deputi Bidang Informasi dan Data (selaku CSO) dalam upaya mengawasi Pihak Eksternal yang terlibat pada kegiatan yang terkait Keamanan Informasi.

IV. MANAJEMEN MEDIA INFORMASI

A. Tujuan

Mengidentifikasi Media Informasi Komisi dan menentukan tanggung jawab perlindungan yang tepat.

B. Kebijakan

1. Perlindungan dan pertanggungjawaban terhadap Media Informasi disusun dan dipelihara melalui identifikasi dan inventarisasi Media Informasi, sebagai berikut:
   a. Biro Umum mengidentifikasi dan menginventarisasi Media Informasi; dan
   b. Biro Umum mengklasifikasikan dan menetapkan Media Informasi secara akurat, terkini (*up to date)*, konsisten, serta harus sesuai dalam siklus Media Informasi (pembuatan, pengolahan, penyimpanan, transmisi, penghapusan, dan penghancuran).
2. Penetapan kepemilikan Media Informasi harus ditetapkan sebagai berikut:
   a. unit kerja menetapkan penanggung jawab pengelolaan dan pemilik Media Informasi;

b. unit kerja mengelola Media Informasi (inventarisasi, klasifikasi, proteksi, penghapusan, dan pembatasan Akses sesuai pedoman dan prosedur kontrol Akses) milik unit kerja masing-masing;
c. semua unit kerja yang mengelola Media Informasi bekerja sama dengan unit pelaksana pengelolaan Media Informasi Komisi;
d. Direktorat PINDA menyediakan layanan Sistem Informasi yang mengelola Media Informasi dari Unit/Biro/ Direktorat; dan
e. Biro Umum menyediakan layanan pengelolaan Media Informasi dalam bentuk fisik yang terkait dengan Informasi di antaranya penyimpanan, pengantaran, penghancuran, dan lain-lain.

3. Pengidentifikasian, pendokumentasian, dan penerapan pedoman tentang persetujuan penggunaan Aset Informasi dan Media Informasi, dilakukan sebagai berikut:
a. unit kerja mengidentifikasi dan mendokumentasi penggunaan Aset Informasi dan Media Informasi;
b. unit kerja membuat dan menerapkan prosedur terkait pemberian persetujuan penggunaan Aset Informasi dan Media Informasi; dan
c. unit kerja mengawasi penggunaan Aset Informasi dan Media Informasi Personil Komisi yang telah disetujui.

4. Personil Komisi dan Pihak Eksternal wajib mengembalikan semua Media Informasi Komisi yang dipinjampakaikan apabila terjadi pemutusan hubungan kerja atau kontrak/perjanjian, sebagai berikut:
a. unit kerja memastikan semua Informasi harus dipindahkan ke Media Informasi Komisi dan dipastikan secara aman telah dihapus dari peralatan milik pribadi;
b. unit kerja Komisi harus memastikan dan mengontrol Personil Komisi atau Pihak Eksternal selama periode pemberitahuan pemutusan hubungan kerja dan kontrak/perjanjian terhadap penyalinan Informasi milik Komisi secara tidak sah, di antaranya kekayaan intelektual;

c. Biro SDM menetapkan pedoman pengembalian semua Media Informasi fisik dan elektronik milik Komisi dalam hal terjadi perubahan atau terminasi hubungan kerja; dan

d. Biro SDM mengoordinasikan terminasi hubungan kerja Personil Komisi dengan Direktorat PINDA dan Biro Umum;

e. Direktorat PINDA dan Biro Umum menerima Informasi dari Biro SDM dan menjalankan prosedur/pedoman pengembalian Media Informasi.

5. Pengelolaan perlindungan Informasi sesuai dengan tingkat kepentingan Informasi bagi Komisi melalui klasifikasi Keamanan Informasi dalam hal terkait ketentuan hukum, nilai, kritikalitas, dan kepekaan terhadap pengungkapan yang tidak sah atau adanya modifikasi, dilakukan sebagai berikut:

a. unit kerja harus bertanggung jawab dan membuat klasifikasi Keamanan Informasi sesuai ketentuan klasifikasi Keamanan Informasi;

b. unit kerja membuat klasifikasi Informasi yang disesuaikan dengan klasifikasi Keamanan Informasi, yang mana pada Aset tersebut diproses, dilindungi, dan terdapat Informasi;

c. unit kerja mereviu klasifikasi Keamanan Informasi secara berkala berdasarkan kerahasiaan, integritas, dan ketersediaan serta pedoman lain sesuai pedoman kontrol Akses;

d. unit kerja memasukkan ketentuan Keamanan Informasi ke dalam proses bisnis masing-masing unit kerja secara konsisten dan terintegrasi; dan

e. Biro Humas mengelola Informasi publik sesuai dengan peraturan perundang-undangan.

6. Prosedur pelabelan Informasi dikembangkan dan dilaksanakan sesuai dengan ketentuan klasifikasi Keamanan Informasi yang berlaku di Komisi, sebagai berikut:

a. Direktorat PINDA bertanggung jawab terhadap adanya Sistem Elektronik yang menunjang pengelolaan pelabelan Informasi dan Media Informasi; dan

b. Biro Umum membuat prosedur pelabelan Informasi dan Aset yang terkait dengan pengolahan Informasi dalam format fisik dan elektronik serta sesuai dengan ketentuan klasifikasi Keamanan Informasi.

7. Prosedur untuk penanganan Media Informasi (tingkat pengamanan dan retensi) dikembangkan dan dilaksanakan sesuai dengan ketentuan klasifikasi Keamanan Informasi Komisi sebagai berikut:
   a. Direktorat PINDA membuat prosedur penanganan, pengolahan, penyimpanan, dan pengomunikasian Informasi Elektronik sesuai dengan klasifikasi Keamanan Informasi;
   b. Biro Umum membuat prosedur penanganan, pengolahan, penyimpanan, dan pengkomunikasian Media Informasi yang sesuai dengan klasifikasi Keamanan Informasi; dan
   c. Direktorat Pembinaan Jaringan Kerja Antar Komisi dan Instansi yang selanjutnya disebut Direktorat PJKAKI berkoordinasi dengan Biro Umum dan unit kerja terkait memastikan pertukaran Aset Informasi antara Komisi dengan Pihak Eksternal sesuai dengan ketentuan klasifikasi Keamanan Informasi serta dengan persetujuan Kepala Biro Humas (selaku Pejabat Pengelola Informasi dan Data).
8. Pencegahan atas insiden tidak sahnya pengungkapan, modifikasi, penghapusan, atau perusakan Informasi yang tersimpan dilakukan oleh Komisi dengan memastikan ketentuan pengelolaan *Removable Media* telah dijalankan sesuai dengan klasifikasi Keamanan Informasi Komisi sebagai berikut:
   a. Direktorat PINDA membuat pedoman pengelolaan *Removable Media* sesuai dengan klasifikasi Keamanan Informasi dan pedoman pengelolaan *Removable Media*;
   b. Direktorat PINDA wajib menggunakan teknik Kriptografi untuk melindungi data pada *Removable Media*; dan
   c. Direktorat PINDA mengarsipkan prosedur dan tingkat otorisasi pengelolaan *Removable Media*.

9. Pemusnahan Media Informasi yang tidak diperlukan dengan menggunakan prosedur yang resmi secara aman, sebagai berikut:
   a. Biro Umum membuat prosedur pemusnahan Media Informasi yang proporsional dengan memperhatikan sensitivitas Informasi untuk meminimalisir Risiko kebocoran Informasi; dan
   b. unit kerja mengidentifikasi dan memberikan penilaian Risiko untuk menentukan tingkat sensitivitas Informasi yang ada di dalam Media Informasi sebelum dibuang atau diperbaiki.
10. Perlindungan Media Informasi terhadap Akses yang tidak sah, penyalahgunaan atau kecurangan selama pengangkutan/ transportasi, sebagai berikut:
   a. Biro Umum membuat pedoman tentang pemindahan Media Informasi fisik sesuai klasifikasi Keamanan Informasi serta ketentuan lain yang berlaku; dan
   b. Direktorat PINDA memberikan konsultasi apabila ada Media Informasi fisik elektronik yang memerlukan perlindungan tambahan, misalnya Enkripsi.

V. PENGENDALIAN AKSES

A. Tujuan

Membatasi Akses atas Aset Informasi ke Media Informasi.

B. Kebijakan

1. Pembatasan Akses ke Informasi ke Media Informasi melalui penetapan, pendokumentasian, dan pengkajian pada ketentuan yang terkait dengan pengendalian Akses berdasarkan Keamanan Informasi, sebagai berikut:
   a. Direktorat PINDA menetapkan, mengkaji, dan mengarsipkan pengendalian Akses, hak, dan pembatasan Akses bagi Pihak Eksternal terhadap Informasi dan Media Informasi secara tepat, ketat, dan detail yang mencerminkan Risiko Keamanan Informasi sesuai dengan pedoman kontrol Akses; dan

b. unit kerja melaksanakan pengendalian Akses di unit kerja sesuai dengan pedoman kontrol Akses.

2. Penyediaan Akses Personil Komisi sesuai dengan kebutuhan dan hak Personil Komisi masing-masing oleh Direktorat PINDA dengan menyediakan dan mengelola infrastruktur, jaringan, serta Akses ke layanan jaringan sesuai dengan pedoman kontrol Akses.

3. Pengaturan Akses Personil Komisi dan Pihak Eksternal ke sistem dan layanan untuk pencegahan terhadap pengguna yang tidak sah dipastikan secara formal melalui pelaksanaan proses pendaftaran dan pencabutan untuk mengatur dan mengalihkan Hak Akses, sebagai berikut:
   a. Biro SDM memberikan Informasi kepada Direktorat PINDA dan Biro Umum terkait Hak Akses Personil Komisi yang diberikan atau dicabut;
   b. Direktorat PINDA dan Biro Umum menerima Informasi dari Biro SDM dan selanjutnya melaksanakan proses pendaftaran dan pencabutan serta mengelola Hak Akses Personil Komisi sesuai dengan pedoman kontrol Akses; dan
   c. Biro Umum dan Direktorat PINDA memastikan hanya Pihak Eksternal yang berwenang yang dapat mengakses sistem dan layanan di Komisi.

4. Pengelolaan Hak Akses untuk Personil Komisi dan Pihak Eksternal sebagai pengguna (*user*) di semua level pada sistem dan layanan Komisi, sebagai berikut:
   a. semua unit kerja menentukan perubahan Hak Akses dari pengguna apabila terjadi perubahan dan menginformasikannya kepada Direktorat PINDA;
   b. Direktorat PINDA menyediakan dan mengelola Akses pengguna sesuai dengan pedoman kontrol Akses;
   c. Direktorat PINDA mereviu Hak Akses bersama pemilik Sistem Informasi secara berkala; dan
   d. Direktorat Pengawasan Internal menerima laporan dan memproses sanksi jika ada Akses yang tidak sah dilakukan oleh Personil Komisi atau Pihak Eksternal;

5. Pengendalian alokasi dan penggunaan Hak Akses khusus (*Privileged Access Rights*) oleh Direktorat PINDA dilakukan dengan mengontrol dan mereviu pemberian Hak Akses khusus melalui proses pengesahan yang sesuai dengan pedoman kontrol Akses.
6. Pengendalian terhadap alokasi Informasi otentik rahasia (*secret authentication information*), nama pengguna (*user name*), kata sandi, dan biometrik (*biometric*), sebagai berikut:
   a. Direktorat PINDA menetapkan prosedur untuk melakukan verifikasi identitas pengguna yang terkait dengan otentikasi rahasia (*secret authentication*) dan perubahannya (kata sandi ke Sistem Informasi) harus sesuai dengan pedoman penggunaan kata sandi; dan
   b. Direktorat Pengawasan Internal menetapkan prosedur untuk melakukan verifikasi identitas pengguna yang terkait dengan otentikasi rahasia (*secret authentication*) dan perubahannya harus sesuai dengan pedoman penggunaan perangkat Akses (*token hardware/smart card/Building Automation System).*
7. Reviu terhadap kepemilikan Hak Akses pengguna secara berkala dilakukan oleh unit kerja masing-masing.
8. Penghapusan Hak Akses pengguna atas Informasi dan Media Informasi dalam penguasaan Personil Komisi dan Pihak Eksternal dalam hal terjadi pengajuan pemutusan hubungan kerja, kontrak/perjanjian, atau disesuaikan pada perubahan yang terjadi, sebagai berikut:
   a. Biro SDM memberikan Informasi perubahan atau terminasi hubungan kerja Personil Komisi atau Pihak Eksternal kepada Direktorat PINDA dan Biro Umum untuk penghapusan atau penyesuaian Hak Akses; dan
   b. Direktorat PINDA dan Biro Umum mengelola penghapusan dan penyesuaian Hak Akses Personil Komisi atau Pihak Eksternal pada Sistem Informasi Komisi setelah mendapatkan Informasi dari Biro SDM.
9. Pengelolaan Hak Akses yang bertanggung jawab dalam penggunaan Informasi otentikasi rahasia (*secret authentication information*) sesuai dengan ketentuan, yaitu:

a. Direktorat PINDA membuat pedoman kata sandi pada Sistem Informasi Komisi;
b. Biro Umum membuat pedoman terkait Informasi otentikasi rahasia (*secret authentication information*) pada *Building Automation System*;
c. Biro SDM membuat pedoman terkait Informasi otentikasi rahasia (*secret authentication information*) pada sistem pencatatan kehadiran Personil Komisi;
d. Direktorat PINDA menyediakan otentikasi akses terintegrasi (*single sign on*) terhadap Akses data dan Informasi Elektronik;
e. Biro Umum menyediakan token perangkat keras atau kode otentikasi *Building Automation System*, perangkat biometrik (*biometric*), dan kode otentikasi kehadiran yang memadai dan sesuai dengan perkembangan teknologi; dan
f. Biro SDM menentukan spesifikasi perangkat biometrik (*biometric*) dan kode otentikasi kehadiran.

10. Pencegahan Akses yang tidak sah ke sistem dan aplikasi melalui pembatasan Akses ke fungsi Sistem Informasi dan aplikasi oleh Direktorat PINDA dengan mengelola pembatasan Akses ke Sistem Informasi Komisi sesuai dengan kebutuhan aplikasi bisnis dan pedoman kontrol Akses.
11. Penerapan pengendalian Akses ke sistem dan aplikasi melalui prosedur log masuk (*log-on*) yang aman oleh Direktorat PINDA dengan menyediakan prosedur log masuk (*log-on*) yang aman ke Sistem Informasi Komisi.
12. Penerapan sistem manajemen kata sandi yang interaktif dan memastikan kualitas dari kata sandi oleh Direktorat PINDA dengan menetapkan dan mengelola sistem manajemen kata sandi.
13. Pembatasan dan pengendalian penggunaan program utilitas yang mampu menimpa dan mengambil alih (*overwrite*) sistem dan aplikasi oleh Direktorat PINDA dengan membuat pedoman penggunaan dan pengelolaan program utilitas khusus.

14. Pembatasan Akses ke program kode sumber (*source code program*) oleh Direktorat Pinda dengan mengelola manajemen dan mengontrol ketat Akses ke program kode sumber (*source code program*).

VI. KRIPTOGRAFI

A. Tujuan

Memastikan penggunaan Kriptografi yang tepat dan efektif agar Informasi terlindungi kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaannya (*availability).*

B. Kebijakan

1. Penggunaan Kriptografi yang tepat dan efektif dalam upaya menjaga Informasi tetap terlindungi kerahasiaan, keaslian, dan integritasnya dilakukan oleh Direktorat PINDA dengan menetapkan, mengembangkan, dan mengimplementasikan pedoman tentang pengendalian Enkripsi dalam Kriptografi yang melindungi Informasi.
2. Pengendalian Enkripsi dalam Kriptografi yang memuat pedoman tentang penggunaan, perlindungan, dan masa pakai kunci Kriptografi yang dikembangkan dan dilaksanakan seluruh siklusnya dilakukan oleh Direktorat PINDA dengan mengelola kunci Kriptografi dari seluruh siklusnya yakni menghasilkan (*generating*), menyimpan (*storing*), mengarsipkan (*archiving*), menerima (*retrieving*), mendistribusikan (*distributing*), menyingkirkan (*retiring*), dan memusnahkan kunci (*destroying keys*).

VII. KEAMANAN FISIK DAN LINGKUNGAN

A. Tujuan

Mencegah Akses fisik yang tidak sah, termasuk kerusakan dan gangguan terhadap Informasi dan Fasilitas Pengolahan Informasi milik Komisi.

B. Kebijakan

1. Pencegahan Akses fisik yang tidak sah, yang berpotensi menyebabkan terjadinya kerusakan dan gangguan terhadap Informasi dan Media Informasi milik Komisi dilakukan oleh Biro Umum dengan menetapkan dan menerapkan batasan keamanan untuk melindungi area Media Informasi dan area yang terdapat Informasi sensitif atau kritis.
2. Perlindungan terhadap area aman (*secure area*) dengan menggunakan sistem kontrol keluar masuk untuk menjamin hanya personil yang berwenang yang diperbolehkan mengakses dilakukan sebagai berikut:
   a. Direktorat PINDA memantau mekanisme Akses ke Media Informasi Komisi; dan
   b. Biro Umum mengelola dan mereviu implementasi *Building Automation System*, dan mengontrol sistem keluar masuk Personil Komisi ke area fisik dan menerapkan mekanisme otentikasi Akses fisik yang sesuai.
3. Perancangan dan penerapan keamanan fisik untuk lingkungan kantor, ruangan, dan fasilitas lainnya dilakukan oleh Biro Umum dengan merancang, mempertimbangkan, dan menerapkan pengamanan fisik untuk kantor, ruangan, dan fasilititas Komisi sesuai dengan batasan Akses yang ditetapkan.
4. Perancangan dan penerapan perlindungan fisik terhadap bencana alam, gangguan keamanan, atau kecelakaan dilakukan oleh Biro Umum dengan merancang dan mengimplementasikan perlindungan terhadap ancaman dari luar (bencana, huru-hara, dan lain-lain).
5. Perancangan dan penerapan prosedur untuk bekerja di area aman (*secure area*) dilakukan oleh Biro Umum dengan membuat prosedur untuk bekerja di area aman (*secure area*) dan merancang serta menetapkan area aman (*secure area*).
6. Pengendalian Media Informasi untuk menghindari Akses personil yang tidak berwenang, sebagai berikut:
   a. Biro Umum membuat dan menjalankan prosedur pembatasan Akses personil pada area bongkar muat; dan

b. Biro Umum membuat dan menjalankan prosedur manajemen Aset.

7. Pencegahan terhadap kehilangan, kerusakan, pencurian yang membahayakan Aset Informasi dan Media Informasi serta munculnya potensi gangguan terhadap operasional, sebagai berikut:
   a. Direktorat PINDA menempatkan dan melindungi peralatan untuk mengurangi Risiko dari ancaman dan bahaya lingkungan, serta peluang dari Akses yang tidak berwenang;
   b. Direktorat PINDA menyusun *Business Continuity Plan* terkait sistem, teknologi Informasi, dan Media Informasi; dan
   c. Biro Umum membuat pedoman dan menentukan lokasi penempatan dan perlindungan peralatan dari ancaman dan bahaya.
8. Perlindungan peralatan dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan berfungsinya Perangkat Penunjang, sebagai berikut:
   a. Biro Umum membuat pedoman/prosedur terkait pemeliharaan, pengoperasian, dan respon tindakan darurat terhadap dukungan keberlangsungan fungsi Perangkat Penunjang; dan
   b. Biro Umum menyusun dan melaksanakan *Business Continuity Management* terkait dukungan fungsi Perangkat Penunjang;
9. Perlindungan kabel listrik dan kabel telekomunikasi yang mentransmisikan data atau yang mendukung layanan Informasi dari penyadapan, gangguan, atau kerusakan dilakukan oleh Biro Umum dan Direktorat PINDA dengan memastikan dan bertanggung jawab terhadap seluruh infrastruktur atau Perangkat Penunjang dan komunikasi dari penyadapan, gangguan, dan kerusakan.
10. Pemeliharaan peralatan dengan benar untuk memastikan kontinuitas ketersediaan dan keutuhan peralatan dilakukan oleh Biro Umum dengan membuat prosedur pemeliharaan

dan perbaikan serta pemeliharaan sesuai dengan spesifikasi peralatan.

11. Penggunaan peralatan, Informasi, atau perangkat lunak di luar area Komisi wajib mendapat izin yang sah, sebagai berikut:
    a. Biro Umum melaksanakan dan bertanggung jawab terhadap pemindahan Media Informasi; dan
    b. Biro Umum membuat prosedur pemindahan Media Informasi.
12. Penerapan keamanan untuk Aset di luar area Komisi dengan memperhitungkan perbedaan Risiko ketika pekerjaan dilakukan di luar area kantor dilakukan semua unit kerja dengan melakukan identifikasi, reviu, penyimpanan, dan penggunaan terhadap Media Informasi termasuk semua Media Informasi yang diadakan untuk menunjang *Teleworking* atau diangkut/dipindah dari lokasi kerja normal seperti: komputer pribadi, ponsel, kartu pintar (*smart card*), kertas, atau bentuk lain.
13. Verifikasi atas semua peralatan yang mengandung *Removable Media* untuk memastikan setiap data sensitif dan perangkat lunak yang berlisensi telah dihapus atau ditimpa dan diambil alih (*overwrite*) dengan aman sebelum dibuang atau digunakan kembali, sebagai berikut:
    a. Biro Umum memastikan keamanan pembuangan atau penghancuran media yang berisikan Aset Informasi yang sensitif dari kebocoran Informasi; dan
    b. Direktorat PINDA menerapkan teknik yang aman dan sesuai dengan teknologi media penyimpanan dalam melakukan proses menimpa dan mengambil alih (*overwritting*), penggunaan kembali dari media penyimpanan yang berbeda, dan teknologi dari media penyimpanan harus direviu untuk memastikan proses menimpa dan mengambil alih (*overwritting*) dapat diberlakukan.

14. Pengawasan dan perlindungan terhadap peralatan kerja sebagai berikut:
    a. Direktorat PINDA melakukan pengaturan pengamanan komputer dan perangkat komunikasi bergerak dari pengguna yang tidak sah melalui kontrol yang setara (*key lock)*; dan
    b. Personil Komisi wajib mengikuti pedoman yang terkait keamanan terhadap perlindungan penggunaan peralatan.
15. Pengembangan pedoman tentang meja kerja (*clean desk*) terhadap kertas dan *Removable Media* dan pedoman penguncian yang dikendalikan oleh kata sandi, token, atau yang serupa (*clear screen*) terhadap Media Informasi sebagai berikut:
    a. Personil Komisi wajib mengikuti pedoman meja kerja (*clean desk)* dan pedoman penguncian yang dikendalikan oleh kata sandi (*password*), token, atau yang serupa *(clear screen);*
    b. Direktorat PINDA melakukan pengaturan komputer dan perangkat komunikasi melalui penguncian yang dikendalikan oleh kata sandi, token, atau yang serupa;
    c. Direktorat PINDA mencari teknologi yang memenuhi pedoman meja kerja (*clean desk)* dan pedoman penguncian yang dikendalikan oleh kata sandi, token, atau yang serupa *(clear screen)*; dan
    d. Biro Umum memastikan Keamanan Informasi pada fasilitas penyimpanan (misalnya brankas) terhadap bencana.

VIII. KEAMANAN OPERASIONAL

A. Tujuan

Memastikan operasional yang tepat dan aman terhadap Fasilitas Pengolahan Informasi.

B. Kebijakan

1. Prosedur operasi didokumentasikan dan tersedia untuk Personil Komisi yang membutuhkannya sehingga Fasilitas Pengolahan Informasi dapat dioperasikan dengan tepat dan aman, sebagai berikut:
   a. Direktorat PINDA membuat prosedur operasional yang terkait dengan Fasilitas Pengolahan Informasi dan komunikasi; dan
   b. Direktorat PINDA menyediakan sarana pengelolaan *Document Management System*.
2. Pengendalian perubahan organisasi, proses bisnis, Fasilitas Pengolahan Informasi, dan sistem yang mempengaruhi Keamanan Informasi, sebagai berikut:
   a. unit kerja mengidentifikasi dan mendokumentasikan perubahan organisasi, proses bisnis, Fasilitas Pengolahan Informasi, dan sistem yang mempengaruhi Keamanan Informasi;
   b. unit kerja melaporkan kepada Biro Perencanaan dan Keuangan apabila terjadi perubahan organisasi, proses bisnis, Fasilitas Pengolahan Informasi, dan sistem lainnya yang mempengaruhi Keamanan Informasi; dan
   c. Biro Perencanaan dan Keuangan memastikan pengendalian perubahan organisasi, proses bisnis, Fasilitas Pengolahan Informasi, dan sistem lainnya yang mempengaruhi Keamanan Informasi sudah memenuhi ketentuan.
3. Pemantauan dan penyesuaian penggunaan sumber daya, serta proyeksi kebutuhan dan kepentingan Komisi di masa yang akan datang dilakukan oleh Direktorat PINDA dengan memantau dan memproyeksikan kebutuhan kapasitas dari sistem milik Komisi di masa yang akan datang.
4. Pemisahan antara area pengembangan, pengujian, dan operasional untuk mengurangi Risiko akibat Akses yang tidak berwenang atau perubahan area operasional sebagai berikut:
   a. Direktorat PINDA membuat pedoman pengembangan aplikasi; dan

b. Direktorat PINDA menyiapkan dan membuat pemisahan fasilitas pengembangan, pengujian, dan operasional.

5. Pengendalian deteksi, pencegahan, dan pemulihan yang dikombinasikan dengan kepedulian pengguna secara tepat untuk melindungi sarana Informasi dan pengolahan Informasi dari *Malware* sebagai berikut:
   a. Direktorat PINDA membuat ketentuan terkait virus dan *Malware;* dan
   b. Direktorat PINDA menerapkan dan menangani perlindungan terhadap virus dan *Malware* pada sistem.
6. Pengendalian berupa *Back Up* terhadap Informasi, perangkat lunak, *System Image* yang diuji secara berkala sesuai dengan ketentuan untuk perlindungan terhadap kehilangan data sebagai berikut:
   a. Direktorat PINDA menerapkan prosedur *Back Up* dan *Restore*; dan
   b. Direktorat PINDA membuat ketentuan *Back Up* dan *Restore*.
7. Pengelolaan *Event Log* yang mencatat atau merekam dan mereviu aktivitas pengguna, pengecualian khusus (*exception*), kesalahan, dan peristiwa Keamanan Informasi secara berkala dilakukan oleh Direktorat PINDA dengan mengelola *Event Log* sesuai dengan pedoman Keamanan Informasi log.
8. Perlindungan terhadap fasilitas log dan Informasi log dari gangguan dan Akses yang tidak berwenang dilakukan oleh Direktorat PINDA dengan membuat pedoman perlindungan terhadap fasilitas log dan Sistem Informasi log.
9. Pencatatan log terhadap kegiatan *System Administrator* dan *System Operator* serta log yang dihasilkannya harus dilindungi dan direviu secara berkala, sebagai berikut:
   a. Direktorat PINDA membuat pedoman pencatatan log; dan
   b. Direktorat PINDA melakukan reviu secara berkala pada kegiatan *System Administrator* dan *System Operator*.
10. Penerapan standar sinkronisasi waktu pada seluruh Fasilitas Pengolahan Informasi yang relevan pada Komisi atau area keamanan Komisi sesuai dengan referensi yang bersumber pada satu penunjukan waktu yang sama oleh Direktorat

PINDA dengan mengimplementasikan dan mereviu secara berkala penerapan standar sinkronisasi waktu.

11. Pengendalian instalasi perangkat lunak melalui penerapan prosedur pada sistem operasional, sebagai berikut:
    a. Direktorat PINDA membuat instruksi kerja untuk mengendalikan perubahan atau pengembangan perangkat lunak pada Sistem Informasi sesuai dengan pedoman pengembangan aplikasi;
    b. Direktorat PINDA memastikan dan memonitor Pihak Eksternal yang menyediakan perangkat lunak pada sistem operasional memenuhi kewajiban sesuai kontrak/perjanjian;
    c. Direktorat PINDA mempertimbangkan Risiko untuk perangkat lunak yang suatu saat tidak lagi didukung oleh Pihak Eksternal; dan
    d. Direktorat PINDA memonitor dan mengendalikan perangkat lunak dari Risiko kelemahan terhadap Keamanan Informasi.
12. Pengelolaan Informasi tentang kerawanan teknis terkait Sistem Informasi yang digunakan dan diperoleh secara tepat waktu, serta evaluasi dan tindak lanjut untuk mengatasi Risiko terhadap kerawanan teknis sebagai berikut:
    a. Direktorat PINDA melakukan manajemen kerawanan teknis terkait Sistem Informasi yang digunakan dan melakukan reviu;
    b. Direktorat PINDA membuat instruksi kerja tentang pengelolaan *Technical Vulnerability* yang efektif sesuai dengan pedoman umum keamanan teknologi Informasi; dan
    c. Direktorat PINDA memastikan dan memonitor Pihak Eksternal sebagai penyedia perangkat lunak dalam memenuhi dukungan terkait ketersediaan *Patch*.
13. Instalasi perangkat lunak yang dilakukan pengguna diatur oleh Direktorat PINDA melalui pedoman umum penggunaan sarana teknologi Informasi tentang pembatasan instalasi perangkat lunak, dilakukan dengan perencanaan pedoman kegiatan audit atas sistem operasional untuk meminimalisir

Risiko dari gangguan terhadap proses bisnis yang dilakukan oleh Direktorat Pengawasan Internal dan tim audit.

IX. KEAMANAN KOMUNIKASI

A. Tujuan

Menjamin perlindungan terhadap Aset Informasi yang ada di dalam jaringan dan yang mendukung Fasilitas Pengolahan Informasi.

B. Kebijakan

1. Pengelolaan jaringan untuk melindungi Informasi pada sistem dan aplikasi oleh Direktorat PINDA dengan mengelola dan memonitor jaringan pada sistem, aplikasi, dan Fasilitas Pengolahan Informasi.
2. Identifikasi mekanisme keamanan, tingkat layanan, dan pedoman pengelolaan dari semua layanan jaringan dan dimuat ke dalam perjanjian layanan jaringan (*network services agreements*), sebagai layanan internal (*in-house*) atau melalui Pihak Eksternal dilakukan oleh Direktorat PINDA dengan mengidentifikasi mekanisme keamanan, tingkat layanan, dan pedoman pengelolaan dari semua layanan jaringan dan dimuat ke dalam perjanjian layanan jaringan (*network services agreements*) serta mengelola dan menyepakati tingkat keamanan jaringan bersama-sama penyedia jasa (*provider*) untuk menjaga ketersediaannya.
3. Pemisahan layanan jaringan berdasarkan jenis layanan Informasi, pengguna, dan Sistem Informasi oleh Direktorat PINDA dengan merancang dan mengelola pemisahan domain jaringan pada sistem jaringan internal.
4. Pengelolaan prosedur dan pengendalian terkait pertukaran Informasi yang memuat perlindungan terhadap pertukaran Informasi pada semua jenis media komunikasi untuk menjaga keamanan pertukaran Informasi internal maupun Pihak Eksternal sebagai berikut:

a. Direktorat PINDA membuat dan menerapkan pedoman dan prosedur pengendalian transfer Informasi Elektronik dan komunikasi; dan
b. unit kerja mematuhi pedoman transfer Informasi Elektronik dan komunikasi.

5. Perlindungan Informasi rahasia dalam aktivitas pertukaran Informasi dilakukan oleh Direktorat PJKAKI dan Biro Umum dengan memastikan dicantumkannya substansi (klausul) kerahasiaan dalam setiap perjanjian kerja sama antara Komisi dengan Pihak Eksternal.
6. Perlindungan Informasi yang memanfaatkan pesan elektronik, oleh Direktorat PINDA dengan mengelola dan melindungi penggunaan pesan elektronik untuk komunikasi.
7. Reviu atas substansi (klausul) kerahasiaan dalam perjanjian kerja sama pertukaran Informasi yang mencerminkan kebutuhan Komisi dan pengarsipan perjanjian sebagai berikut:
   a. Direktorat PJKAKI melakukan reviu secara berkala terhadap implementasi perjanjian kerja sama pertukaran data dan Inforamsi yang di dalamnya memuat substansi (klausul) kerahasiaan serta mengarsipkan hasil implementasi kerja sama; dan
   b. Biro Hukum merancang, membuat, mereviu, dan mengarsipkan perjanjian kerja sama yang didalamnya memuat substansi (klausul) kerahasiaan.

X. SISTEM AKUISISI, PENGEMBANGAN, DAN PEMELIHARAAN

A. Tujuan

Memastikan Keamanan Informasi sebagai bagian yang terintegrasi dari Sistem Informasi di seluruh siklus Komisi, termasuk juga pedoman untuk Sistem Informasi yang menyediakan layanan melalui jaringan publik.

B. Kebijakan

1. Pengembangan Sistem Informasi yang baru atau pembaruan Sistem Informasi untuk mengintegrasikan seluruh siklus

Sistem Informasi termasuk juga Sistem Informasi yang menyediakan layanan melalui jaringan publik sebagai bagian dari Keamanan Informasi sebagai berikut:

a. Direktorat PINDA mengimplementasikan pengelolaan pedoman Keamanan Informasi secara terintegrasi dalam tahap awal proyek Sistem Informasi (khususnya proyek Sistem Informasi yang menggunakan jaringan publik atau transaksional);
b. Biro Umum dalam melaksanakan pengujian dan akuisisi terkait pengadaan harus mempertimbangkan Risiko Keamanan Informasi dan pengendaliannya sebelum pengadaan barang dan jasa; dan
c. Pejabat Pembuat Komitmen memastikan isi kontrak/ perjanjian memuat hal-hal terkait Keamanan Informasi sesuai dengan objek yang diperjanjikan.

2. Perlindungan atas Informasi yang berada di dalam layanan aplikasi pada jaringan publik dari aktivitas penipuan, perbedaan atau perselisihan kontrak/perjanjian dan kegiatan modifikasi atau pengungkapan Informasi yang tidak sah oleh Direktorat PINDA dengan menjamin keamanan layanan aplikasi yang dapat diakses dijaringan publik dengan menggunakan metode otentifikasi yang aman.
3. Perlindungan Informasi transaksi pada layanan aplikasi untuk mencegah terjadinya transmisi tidak lengkap, kesalahan *Routing*, serta kegiatan tidak sah, berupa perubahan pesan, pengungkapan data, duplikasi, atau pembalasan pesan dilakukan oleh Direktorat PINDA dengan menjamin perlindungan transaksi yang menggunakan layanan aplikasi.
4. Penetapan dan penerapan pedoman dalam pengembangan aplikasi dan sistem untuk memastikan Keamanan Informasi telah dirancang dan diimplementasikan pada siklus pengembangan Sistem Informasi oleh Direktorat PINDA dengan membuat pedoman pengembangan aplikasi yang aman serta menerapkan pedoman pengembangan aplikasi.
5. Pengendalian perubahan yang sah terhadap perubahan sistem dalam siklus pengembangan Sistem Informasi

ditentukan oleh Direktorat PINDA dengan membuat pedoman pengendalian dan pengelolaan perubahan.

6. Platform sistem teknologi Informasi yang mengalami perubahan terhadap aplikasi pendukung kegiatan utama untuk memastikan tidak ada dampak buruk pada keamanan dan operasional Komisi dilakukan oleh Direktorat PINDA dengan mereviu perubahan pada platform sistem teknologi Informasi (sistem operasi, basis data, dan *Platform Middleware*) dan mengontrol perubahan pada aplikasi.
7. Penetapan pembatasan modifikasi pada perangkat lunak, terbatas pada perubahan yang diperlukan dan semua perubahan dikontrol secara ketat dilakukan oleh Direktorat PINDA dengan mengendalikan perubahan/modifikasi pada paket perangkat lunak.
8. Penetapan, pendokumentasian, pemeliharaan, dan penerapan prinsip dalam rekayasa keamanan sistem untuk setiap implementasi Sistem Informasi dilakukan oleh Direktorat PINDA dengan membuat, menerapkan dan mereviu prosedur rekayasa Sistem Informasi berdasarkan prinsip keamanan.
9. Penetapan dan perlindungan keamanan area pengembangan untuk pembangunan sistem dan penggabungan yang mencakup seluruh siklus pengembangan sistem dilakukan oleh Direktorat PINDA memonitor pengembangan sistem oleh Pihak Eksternal, melakukan penilaian Risiko terkait pengembangan sistem, serta melakukan penilaian Risiko terkait pembangunan keamanan area pengembangan (sumber daya manusia, proses, teknologi, dan integrasi).
10. Pengawasan dan pemantauan aktivitas pengembangan sistem yang dilakukan oleh Pihak Eksternal dilakukan oleh Direktorat PINDA.
11. Pengujian fungsi Keamanan Informasi dilakukan selama pengembangan wajib dilakukan oleh Direktorat PINDA dengan melakukan pengujian fungsi keamanan secara menyeluruh dan melakukan verifikasi hasil pengujian selama proses pengembangan.
12. Menetapkan *User Acceptance Test* dan kriterianya untuk Sistem Informasi baru, peningkatan versi (*upgrade*), dan versi

baru oleh Direktorat PINDA dengan melakukan pengujian kehandalan sistem (uji coba) lingkungan sebenarnya yang nyata.

13. Jaminan pengendalian dan perlindungan data yang digunakan untuk pengujian dalam pengembangan Sistem Informasi oleh Direktorat PINDA dengan memastikan tidak menggunakan data operasional yang berisikan Informasi pribadi/rahasia untuk tujuan pengujian serta membuat catatan/laporan pengujian yang dilaporkan kepada Direktur PINDA.

XI. HUBUNGAN DENGAN PENYEDIA BARANG DAN JASA

A. Tujuan

Memastikan perlindungan Aset Komisi yang dapat diakses oleh Pihak Eksternal selaku penyedia barang dan jasa.

B. Kebijakan

1. Perlindungan Aset Komisi yang dapat diakses oleh penyedia barang dan jasa memerlukan kesepakatan dan pendokumentasian kebutuhan Keamanan Informasi untuk mengurangi Risiko yang terkait dengan Akses penyedia barang dan jasa ke Aset Komisi sebagai berikut :
   a. unit kerja memastikan penerapan ketentuan Keamanan Informasi terkait hubungan dengan penyedia barang dan jasa; dan
   b. unit kerja mengendalikan dan memonitor hubungan dengan penyedia barang dan jasa sesuai perjanjian.
2. Penetapan dan pemberian persetujuan seluruh kebutuhan Keamanan Informasi oleh setiap penyedia barang dan jasa yang dapat mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur teknologi dan Informasi Komisi dilakukan oleh Biro Umum dengan menetapkan, menyetujui, mengelola, dan mereviu perjanjian kerja dengan penyedia barang dan jasa terkait Keamanan Informasi.

3. Perjanjian dengan penyedia barang dan jasa wajib memuat klausul yang mengikat kepada penyedia barang dan jasa untuk mengatasi Risiko Keamanan Informasi terkait dengan layanan teknologi Informasi dan komunikasi sebagai berikut:
   a. Pejabat Pembuat Komitmen dan Direktorat PINDA membuat klausul yang mengikat terhadap penyedia barang dan jasa terkait Risiko Keamanan Informasi; dan
   b. Pejabat Pembuat Komitmen dan Direktorat PINDA mengontrol pelaksanaan perjanjian dengan penyedia barang dan jasa terkait pemenuhan rantai pasok (*supply chain*) Informasi dan komunikasi.
4. Pemantauan, reviu, dan audit layanan penyedia barang dan jasa secara berkala oleh Pejabat Pembuat Komitmen dengan memonitor dan mereviu berjalannya layanan penyedia barang dan jasa.
5. Pengelolaan perubahan perjanjian dan penilaian ulang Risiko terhadap perubahan layanan oleh penyedia barang dan jasa, termasuk pemeliharaan dan pembaruan ketentuan, prosedur serta kontrol Keamanan Informasi, dengan mempertimbangkan tingkat kekritisan Informasi utama, perubahan sistem, dan proses di Komisi sebagai berikut:
   a. unit kerja memberikan Informasi perubahan terhadap ketersediaan layanan pihak penyedia barang dan jasa kepada Biro Umum; dan
   b. Biro Umum memonitor dan memproses perubahan yang terjadi pada layanan pihak penyedia barang dan jasa sesuai dengan peraturan perundang-undangan.

XII. MANAJEMEN INSIDEN KEAMANAN INFORMASI

A. Tujuan

Memastikan pendekatan yang konsisten dan efektif untuk pengelolaan insiden Keamanan Informasi, termasuk komunikasi pada peristiwa keamanan dan kelemahan.

B. Kebijakan

1. Pendekatan yang konsisten dan efektif untuk pengelolaan insiden Keamanan Informasi, termasuk komunikasi pada insiden dan kelemahan Keamanan Informasi melalui penetapan tanggung jawab dan prosedur pengelolaan Keamanan Informasi untuk memastikan respon yang cepat, efektif, dan terorganisir terhadap insiden Keamanan Informasi oleh Komite Keamanan Informasi dengan membuat prosedur terhadap respon dan penanganan insiden Keamanan Informasi.
2. Pelaporan kejadian terhadap Keamanan Informasi menggunakan saluran manajemen yang tepat dan cepat oleh unit kerja dengan melaporkan kejadian Keamanan Informasi secepat mungkin kepada Komite Keamanan Informasi.
3. Pencatatan dan pelaporan penggunaan sistem dan layanan Informasi oleh Personil Komisi dan Pihak Eksternal pada setiap kelemahan Keamanan Informasi yang diamati atau dicurigai berada dalam sistem atau layanan sebagai berikut:
   a. unit kerja wajib melakukan pencegahan insiden Keamanan Informasi; dan
   b. unit kerja melaporkan apabila menemukan kelemahan Keamanan Informasi dalam sistem dan layanan kepada Komite Keamanan Informasi.
4. Penetapan penilaian dan pengambilan keputusan dalam insiden Keamanan Informasi sebagai berikut:
   a. Komite Keamanan Informasi membuat skala klasifikasi insiden dan kejadian Keamanan Informasi berdasarkan dampak yang dihasilkan;
   b. Komite Keamanan Informasi menyepakati dan memutuskan tingkat kejadian Keamanan Informasi sesuai skala klasifikasi insiden dan kejadian Keamanan Informasi; dan
   c. Komite Keamanan Informasi melakukan pencatatan secara rinci insiden dan kejadian Keamanan Informasi dan melaksanakan asesmen Keamanan Informasi.

5. Pengelolaan respon atas insiden Keamanan Informasi sesuai dengan prosedur yang berlaku oleh Komite Keamanan Informasi sesuai dengan prosedurnya.
6. Penggunaan hasil analisa dari penyelesaian insiden Keamanan Informasi untuk mengurangi kemungkinan atau dampak dari insiden di masa yang akan datang oleh Komite Keamanan Informasi dengan menganalisa laporan penyelesaian insiden Keamanan Informasi untuk mengidentifikasi dampak yang berulang/tinggi.
7. Penetapan dan penerapan prosedur untuk kegiatan identifikasi, pengumpulan, perolehan, dan pemeliharaan Informasi, yang dapat berfungsi sebagai bukti, sebagai berikut:
   a. Komite Keamanan Informasi membuat dan menerapkan prosedur untuk mengidentifkasi, mengumpulkan, memperoleh, dan memelihara bukti; dan
   b. Komite Keamanan Informasi meningkatkan kualifikasi personil sehingga dapat memperkuat nilai dari pemeliharaan bukti.

XIII. *BUSINESS CONTINUITY MANAGEMENT*

A. Tujuan

Memastikan pendekatan yang konsisten dan efektif untuk pengelolaan insiden Keamanan Informasi, termasuk komunikasi pada peristiwa keamanan dan kelemahan.

B. Kebijakan

1. Penentuan kebutuhan Keamanan Informasi dan keberlangsungan manajemen Keamanan Informasi dalam keadaan kahar, misalnya selama krisis atau bencana untuk memastikan keberlangsungan Keamanan Informasi melekat pada *Business Continuity Management* sebagai berikut:
   a. Komite Keamanan Informasi melakukan dan memperbarui penilaian Risiko analisis dampak bisnis, rencana strategi pemulihan, dan rencana keberlangsungan bisnis; dan

b. Komite Keamanan Informasi membuat dan menetapkan *Business Continuity Management* yang terintegrasi dengan Manajemen Risiko Komisi.

2. Penetapan, pendokumentasian, penerapan, pemeliharaan proses, prosedur, dan kontrol untuk memastikan tingkat keberlangsungan yang diperlukan dalam Keamanan Informasi selama kondisi kahar:
   a. *Business Continuity Management* merespon insiden yang dikategorikan mengganggu sesuai skala klasifikasi insiden dan kejadian Keamanan Informasi; dan
   b. Direktur dan Kepala Biro (selaku CISO) menjadi bagian dari struktur *Business Continuity Management* yang bertanggungjawab untuk merespon dan mengelola insiden serta menjaga Keamanan Informasi di Direktorat/Biro masing-masing.
   c. *Business Continuity Management* mengendalikan keberlangsungan Keamanan Informasi dalam bentuk:
      1) rencana proses keberlangsungan bisnis/pemulihan bisnis;
      2) prosedur implementasi dan perubahan kontrol Keamanan Informasi;
      3) prosedur respon dan pemulihan;
      4) ketetapan dukungan sistem dan peralatan;
      5) pemeliharaan kontrol Keamanan Informasi; dan
      6) dokumentasi kejadian/peristiwa.
   d. *Business Continuity Management* menguji coba keberlangsungan bisnis/pemulihan bisnis pada Komisi.
3. Verifikasi secara berkala atas pengendalian dari keberlangsungan Keamanan Informasi yang telah diterapkan untuk memastikan bahwa pengendalian tersebut sah dan efektif dijalankan dalam keadaan kahar oleh *Business Continuity Management* dengan melakukan verifikasi secara berkala terhadap kendali keberlangsungan Keamanan Informasi.
4. Penyediaan Fasilitas Pengolahan Informasi yang penerapannya secara cukup efisien untuk memenuhi kebutuhan atas ketersediaan Informasi ditetapkan oleh

Direktorat PINDA dengan mengidentifikasi kebutuhan Komisi terkait ketersediaan Sistem Informasi yang akan dibutuhkan serta menyiapkan fasilitas pusat pemulihan bencana.

XIV. KEPATUHAN

A. Tujuan

Memastikan pelaksanaan Sistem Manajemen Keamanan Informasi sesuai dengan ketentuan hukum yang berlaku.

B. Kebijakan

1. Ketentuan hukum terkait Keamanan Informasi harus secara eksplisit diidentifikasi, didokumentasikan dan dijaga pembaruannya sebagai berikut:
   a. Komite Keamanan Informasi membuat ketentuan pertukaran Aset Informasi antara Komisi dengan Pihak Eksternal;
   b. unit kerja menerapkan ketentuan pertukaran Aset Informasi dengan Pihak Eksternal; dan
   c. Direktorat PINDA menentukan persyaratan Keamanan Informasi terkait kontrak/perjanjian pengadaan Sistem Informasi atau perjanjian kerja sama pertukaran data dan Informasi serta Sistem Informasi antara Komisi dengan Pihak Eksternal.
2. Penerapan prosedur untuk memastikan kesesuaian dengan hukum, peraturan perundang-undangan dan kewajiban kontrak/perjanjian tentang penggunaan materi memiliki hak kekayaan intelektual dan tentang penggunaan produk perangkat lunak yang memiliki hak paten, sebagai berikut:
   a. Direktorat PINDA memastikan pemakaian dan pembuatan perangkat lunak telah sesuai dengan hak kekayaan intelektual; dan
   b. Direktorat PINDA wajib mengikuti pedoman lisensi teknologi Informasi dan komunikasi untuk melindungi materi apapun yang dapat dianggap hak kekayaan intelektual.

3. Perlindungan Arsip dari kehilangan, penghancuran, dan pemalsuan sesuai dengan ketentuan hukum, peraturan perundang-undangan, kewajiban kontrak/perjanjian, dan kebutuhan Komisi, sebagai berikut:
   a. Direktorat PINDA bertanggung jawab melindungi penyimpanan dan penanganan Arsip dalam bentuk elektronik sesuai ketentuan dan rekomendasi teknis; dan
   b. Biro Umum bertanggung jawab melindungi penyimpanan dan penanganan Arsip dalam bentuk dokumen fisik sesuai prosedur dan rekomendasi.
4. Perlindungan data dan kerahasiaan seperti yang dipersyaratkan dalam proses registrasi, sesuai regulasi dan klausul kontrak/perjanjian, sebagai berikut:
   a. unit kerja memastikan kepatuhan terhadap peraturan perundang-undangan yang terkait pengumpulan, pengolahan, dan penyebaran Informasi pribadi dalam sistem teknologi Informasi dan komunikasi;
   b. unit kerja melindungi Informasi pribadi dalam bentuk pengamanan, penerapan, dan pengelolaan yang sesuai kebutuhan masing-masing;
   c. Biro Umum menyediakan dan mengembangkan sarana pengelolaan dan penyimpanan dokumentasi fisik; dan
   d. semua unit kerja menggunakan sarana pengelolaan *Documet Management System* dan sarana pengelolaan dokumen fisik yang telah ditetapkan dan disediakan.
5. Penggunaan Kriptografi sesuai dengan ketentuan dilakukan oleh Direktorat PINDA dengan memastikan pengembangan dan penerapan Kriptografi telah sesuai dengan peraturan perundang-undangan.
6. Reviu secara independen dan berkala atau ketika terjadi perubahan yang signifikan terhadap pengelolaan dan implementasi Keamanan Informasi untuk memastikan Keamanan Informasi diimplementasikan dan dioperasikan sesuai dengan ketentuan dan prosedur, yang meliputi tujuan pengendalian, kendali, ketentuan, proses, dan prosedur Keamanan Informasi dilakukan oleh Komite Keamanan

Informasi dengan melakukan reviu ketika terjadi perubahan yang signifikan terhadap pengelolaan Keamanan Informasi.

7. Reviu dilakukan untuk memastikan kepatuhan terhadap pengolahan Informasi dan prosedur dalam lingkup tanggung jawabnya yang dilakukan secara benar untuk memenuhi ketentuan keamanan, standar, dan ketentuan keamanan lainnya oleh unit kerja masing-masing dengan memastikan kepatuhan pengolahan Informasi sesuai pedoman umum keamanan teknologi Informasi.
8. Reviu secara berkala atas Sistem Informasi untuk memenuhi kepatuhan terhadap ketentuan dan standar teknis Keamanan Informasi dilakukan oleh Komite Keamanan Informasi, Direktorat Pengawasan Internal, dan Direktorat PINDA.