KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
PERATURAN DIREKTUR JENDERAL PERBENDAHARAAN

NOMOR PER- 1 /PB/2021

TENTANG

KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN DIREKTORAT JENDERAL PERBENDAHARAAN

DIREKTUR JENDERAL PERBENDAHARAAN,

Menimbang : a. bahwa ketentuan mengenai sistem manajemen keamanan informasi di lingkungan Direktorat Jenderal Perbendaharaan telah ditetapkan dalam Peraturan Direktur Jenderal Perbendaharaan Nomor PER-17/PB/2019 tentang Kebijakan Sistem Manajemen Keamanan Informasi di Lingkungan Direktorat Jenderal Perbendaharaan;

b. bahwa guna meningkatkan efektivitas dan efisiensi dalam pengelolaan keamanan informasi sesuai dengan perkembangan Teknologi Informasi dan Komunikasi (TIK), telah ditetapkan Keputusan Menteri Keuangan Nomor 942/KMK.01/2019 tentang Pengelolaan Keamanan Informasi di Lingkungan Kementerian Keuangan;

c. bahwa guna menyesuaikan ketentuan sistem manajemen keamanan informasi di lingkungan Direktorat Jenderal Perbendaharaan sesuai Keputusan Menteri Keuangan Nomor 942/KMK.01/2019 tentang Pengelolaan Keamanan Informasi di Lingkungan Kementerian Keuangan, perlu mengatur kembali kebijakan sistem manajemen keamanan informasi di lingkungan Direktorat Jenderal Perbendaharaan;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Direktur Jenderal Perbendaharaan tentang Kebijakan Sistem Manajemen Keamanan Informasi di Lingkungan Direktorat Jenderal Perbendaharaan;

Mengingat : 1. Peraturan Menteri Keuangan Nomor 97/PMK.01/2017 tentang Tata Kelola Teknologi Informasi dan Komunikasi di Lingkungan Kementerian Keuangan (Berita Negara Republik Indonesia Tahun 2017 Nomor 988);

2. Peraturan Menteri Keuangan Nomor 217/PMK.01/2018 tentang Organisasi dan Tata Kerja Kementerian Keuangan (Berita Negara Republik Indonesia Tahun 2018 Nomor 1862) sebagaimana telah beberapa kali diubah, terakhir dengan Peraturan Menteri Keuangan Nomor 229/PMK.01/2019 tentang Perubahan Kedua atas Peraturan Menteri Keuangan Nomor 217/PMK.01/2018 tentang Organisasi dan Tata Kerja Kementerian Keuangan (Berita Negara Republik Indonesia Tahun 2019 Nomor 1745);

3. Keputusan Menteri Keuangan Nomor 350/KMK.01/2010 tentang Kebijakan dan Standar Pengelolaan Data Elektronik di Lingkungan Kementerian Keuangan sebagaimana telah diubah dengan Keputusan Menteri Keuangan Nomor 38/KMK.01/2014 tentang Perubahan atas Keputusan Menteri Keuangan Nomor 350/KMK.01/2010 tentang Kebijakan dan Standar Pengelolaan Data Elektronik di Lingkungan Kementerian Keuangan;

4. Keputusan Menteri Keuangan Nomor 552/KMK.01/2018 tentang Penggunaan Akun dan Kata Sandi, Surat Elektronik, Intranet dan Internet di Lingkungan Kementerian Keuangan;

5. Keputusan Menteri Keuangan Nomor 577/KMK.01/2019 tentang Manajemen Risiko di Lingkungan Kementerian Keuangan;

6. Keputusan Menteri Keuangan Nomor 878/KMK.01/2019 tentang Tata Kelola Data di Lingkungan Kementerian Keuangan;

7. Keputusan Menteri Keuangan Nomor 942/KMK.01/2019 tentang Pengelolaan Keamanan Informasi di Lingkungan Kementerian Keuangan;

MEMUTUSKAN:

Menetapkan : PERATURAN DIREKTUR JENDERAL PERBENDAHARAAN TENTANG KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN DIREKTORAT JENDERAL PERBENDAHARAAN.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Direktur Jenderal ini, yang dimaksud dengan:

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. Aset Informasi Direktorat Jenderal Perbendaharaan adalah aset dalam bentuk data/dokumen, perangkat lunak, aset berwujud (*tangible*), dan aset tak berwujud (*intangible*).
3. Dokumen Sistem Manajemen Keamanan Informasi (SMKI) Direktorat Jenderal Perbendaharaan adalah dokumen terkait pelaksanaan SMKI yang meliputi antara lain dokumen rencana, kebijakan, standar, prosedur, dan catatan penerapan SMKI.
4. Fasilitas Pengolah Informasi adalah perangkat pengolah informasi dan perangkat pendukung.
5. Hak Akses Khusus adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan (*storage devices*), *file server,* dan aplikasi-aplikasi sensitif, hanya diberikan kepada pengguna yang membutuhkan dan pemakaiannya terbatas dan dikontrol.
6. Instansi adalah seluruh satuan kerja di lingkup Direktorat Jenderal Perbendaharaan yang meliputi kantor pusat dan kantor vertikal di lingkungan Direktorat Jenderal Perbendaharaan.

7. Kebijakan Keamanan Informasi adalah serangkaian aturan terkait keamanan informasi di lingkungan Direktorat Jenderal Perbendaharaan dalam rangka melindungi Aset Informasi milik Direktorat Jenderal Perbendaharaan meliputi kebijakan SMKI, pedoman pelaksanaan SMKI, dan kebijakan *baseline* konfigurasi keamanan perangkat TIK di lingkungan Direktorat Jenderal Perbendaharaan.
8. Kejadian Kemanan Informasi adalah peristiwa yang berpotensi mengakibatkan tidak tercapainya aspek kerahasiaan, keutuhan, dan ketersediaan Aset Informasi milik Direktorat Jenderal Perbendaharaan.
9. Kelemahan Kemanan Informasi adalah kondisi yang berpotensi mengakibatkan tidak tercapainya aspek kerahasiaan, keutuhan, dan ketersediaan Aset Informasi milik Direktorat Jenderal Perbendaharaan.
10. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan keamanan informasi. Dalam Kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi.
11. *Mobile Device* adalah penggunaan perangkat komputasi yang dapat dipindah (portabel) misalnya *notebook* dan *Personal Data Assistant* (PDA) untuk melakukan akses, pengolahan data dan penyimpanan.
12. Pengguna adalah pegawai Direktorat Jenderal Perbendaharaan dan/atau pihak ketiga yang diberikan hak mengakses sistem TIK di lingkungan Direktorat Jenderal Perbendaharaan.
13. Pemasok adalah penyedia layanan (barang dan/atau jasa) kepada Instansi di lingkungan Direktorat Jenderal Perbendaharaan.
14. Pemilik Aset Informasi adalah satuan kerja yang memiliki kewenangan terhadap Aset Informasi.
15. Perangkat Jaringan adalah peralatan jaringan komunikasi data seperti: *modem, hub, switch, router,* dan lain-lain.

16. Perangkat Lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.
17. Perangkat Pendukung adalah peralatan yang berfungsi untuk menjamin beroperasinya Perangkat Pengolah Informasi serta untuk melindunginya dari kerusakan, seperti *Uninterruptible Power Supply* (UPS), pembangkit tenaga listrik, *fire suppression* dan kabel.
18. Perangkat Pengolah Informasi adalah perangkat yang digunakan untuk memproses informasi, seperti komputer, faksimili, telepon, mesin *fotocopy*.
19. 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.
20. Pihak Ketiga adalah Kementerian/Lembaga, penyedia barang dan/atau jasa yang menjadi mitra kerja Direktorat Jenderal Perbendaharaan.
21. *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.
22. Sertifikat Sistem Manajemen Pengamanan Informasi adalah bukti tertulis yang diberikan oleh Lembaga Sertifikasi kepada Penyelenggara Sistem Elektronik yang telah memenuhi persyaratan.
23. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
24. Sistem Elektronik Strategis adalah Sistem Elektronik yang berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.

25. Sistem Elektronik Tinggi adalah Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu.
26. Sistem Elektronik Rendah adalah Sistem Elektronik lainnya yang tidak termasuk pada Sistem Elektronik Strategis dan Sistem Elektronik Tinggi.
27. 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.
28. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penangung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.
29. *Teleworking* adalah aktivitas bekerja di luar kantor dan berkomunikasi dengan kantor melalui telepon, email atau menggunakan internet.
30. Unit TIK Direktorat Jenderal Perbendaharaan, yang selanjutnya disebut Unit, adalah unit eselon II pada Kantor Pusat Direktorat Jenderal Perbendaharaan yang berada di bawah dan bertanggung jawab kepada Direktur Jenderal Perbendaharaan, yang melaksanakan tugas dan fungsi terkait TIK di lingkungan Direktorat Jenderal Perbendaharaan, dalam hal ini Direktorat Sistem Informasi dan Teknologi Perbendaharaan (SITP).
31. Unit TIK Pusat Kementerian Keuangan, yang selanjutnya disebut Unit TIK Pusat, adalah unit eselon II pada Sekretariat Jenderal Kementerian Keuangan yang berada di bawah dan bertanggung jawab kepada Sekretaris Jenderal Kementerian Keuangan, yang melaksanakan tugas dan fungsi terkait TIK di lingkungan Kementerian Keuangan, dalam hal ini Pusat Sistem Informasi dan Teknologi Keuangan (PUSINTEK).

BAB II

RUANG LINGKUP

Pasal 2

(1) Ruang lingkup pengaturan dalam Peraturan Direktur Jenderal ini meliputi:
   a. Ketentuan pokok SMKI di lingkungan Direktorat Jenderal Perbendaharaan;
   b. Pengendalian SMKI di lingkungan Direktorat Jenderal Perbendaharaan;
   c. Organisasi Keamanan Informasi di lingkungan Direktorat Jenderal Perbendaharaan; dan
   d. Sertifikasi Pelaksanaan SMKI di lingkungan Direktorat Jenderal Perbendaharaan.

(2) SMKI di lingkungan Direktorat Jenderal Perbendaharaan dilaksanakan sesuai dengan SNI ISO/IEC 27001:2013.

(3) Pengelolaan keamanan informasi yang diatur dalam Peraturan Direktur Jenderal ini, dilaksanakan oleh seluruh Instansi dan pegawai di lingkungan Direktorat Jenderal Perbendaharaan serta Pihak Ketiga.

BAB III

KETENTUAN POKOK SMKI

Pasal 3

(1) Unit harus membangun, menerapkan, memelihara, dan meningkatkan kebijakan SMKI secara berkelanjutan.

(2) Kebijakan SMKI sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan pedoman teknis penerapan kebijakan SMKI.

(3) Unit menyusun pedoman teknis penerapan kebijakan SMKI sebagaimana dimaksud pada ayat (2) dengan berbasis risiko.

(4) Pedoman teknis penerapan kebijakan SMKI sebagaimana dimaksud pada ayat (2) disusun dengan mempertimbangkan:

4

a. isu eksternal dan internal Direktorat Jenderal Perbendaharaan dalam keamanan informasi;
b. kebutuhan pihak yang berkepentingan dalam penerapan kebijakan SMKI; dan
c. hubungan dan ketergantungan antara kegiatan yang dilakukan oleh internal Direktorat Jenderal Perbendaharaan dan kegiatan yang dilakukan oleh pihak yang berkepentingan dalam penerapan kebijakan SMKI.

(5) Pimpinan Unit dan pimpinan Instansi di lingkungan DJPb harus berkomitmen dalam penerapan kebijakan SMKI sebagaimana dimaksud pada ayat (1).

(6) Komitmen dalam penerapan kebijakan SMKI sebagaimana dimaksud pada ayat (5) dilaksanakan dengan langkah-langkah antara lain:
a. memastikan kebijakan dan sasaran keamanan informasi ditetapkan dan selaras dengan arah strategis Direktorat Jenderal Perbendaharaan;
b. memastikan penerapan ketentuan SMKI ke dalam proses bisnis Direktorat Jenderal Perbendaharaan;
c. memastikan ketersediaan sumber daya yang digunakan untuk penerapan SMKI;
d. mengkomunikasikan pentingnya pengelolaan keamanan informasi yang efektif dan kesesuaiannya dengan ketentuan SMKI;
e. memastikan penerapan SMKI mencapai sasaran yang telah ditentukan;
f. memberi arahan dan dukungan kepada pegawai untuk berkontribusi terhadap penerapan SMKI yang efektif;
g. memastikan peningkatan berkelanjutan atas penerapan SMKI; dan
h. mendukung peran Direktorat Jenderal Perbendaharaan untuk memberikan kontribusi sesuai dengan tanggung jawabnya.

(7) Unit menerapkan manajemen risiko dengan memperhatikan ketentuan yang diatur dalam Keputusan Menteri Keuangan mengenai manajemen risiko di lingkungan Kementerian Keuangan.

(8) Penerapan manajemen risiko sebagaimana dimaksud pada ayat (7) dilaksanakan dengan mempertimbangkan kerahasiaan, keutuhan, dan ketersediaan Aset Informasi Direktorat Jenderal Perbendaharaan.

(9) Unit menentukan sasaran keamanan informasi dan menyusun perencanaan untuk mencapai sasaran keamanan informasi.

(10) Unit dan Instansi menetapkan dan menyediakan sumber daya yang dibutuhkan untuk membangun, menerapkan, memelihara, dan meningkatkan SMKI secara berkelanjutan.

(11) Unit bertanggung jawab untuk meningkatkan pengetahuan, keterampilan, dan kepedulian seluruh pegawai terhadap keamanan informasi.

(12) Unit menetapkan rencana komunikasi internal dan eksternal yang terkait dengan SMKI.

(13) Unit mengelola dokumen SMKI Direktorat Jenderal Perbendaharaan untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan, dan mencegah akses oleh pihak yang tidak berwenang.

(14) Unit dan Instansi melaksanakan pengendalian SMKI.

(15) Unit melakukan evaluasi terhadap pelaksanaan SMKI paling sedikit sekali dalam setahun untuk menjamin efektivitas dan meningkatkan keamanan informasi.

(16) Evaluasi sebagaimana dimaksud pada ayat (15) dilakukan melalui:

a. pemantauan, pengukuran, analisis, dan evaluasi penerapan SMKI;

b. audit internal SMKI, yaitu audit yang dilakukan oleh unit kepatuhan internal Direktorat Jenderal Perbendaharaan dan/atau oleh unit yang

mengkoordinasikan fungsi pengawasan internal di lingkungan Kementerian Keuangan; dan

c. rapat tinjauan manajemen, yaitu rapat pembahasan yang dilaksanakan secara berkala untuk meninjau penerapan SMKI.

(17) Berdasarkan evaluasi sebagaimana dimaksud pada ayat (15), Unit melaksanakan tindak lanjut hasil evaluasi pelaksanaan SMKI serta melakukan peningkatan berkelanjutan.

Pasal 4

Dalam membangun, menerapkan, memelihara, dan meningkatkan kebijakan SMKI sebagaimana dimaksud dalam Pasal 3 ayat (1), Unit menghasilkan *output* paling sedikit berupa:

a. Pakta pernyataan penerapan SMKI;
b. Dokumen rencana SMKI yang memuat:
   1) ruang lingkup penerapan SMKI, termasuk dokumen pertimbangan penentuan ruang lingkup;
   2) sasaran keamanan informasi dan rencana pencapaian sasaran keamanan informasi; dan
   3) rencana komunikasi internal dan eksternal;
c. Dokumen pernyataan pemberlakuan (*Statement of Applicability*/SoA), berisi tentang pengendalian yang diadopsi/tidak diadopsi beserta pertimbangannya;
d. Daftar inventaris Aset Informasi Direktorat Jenderal Perbendaharaan;
e. Profil risiko keamanan informasi;
f. Laporan pemantauan, pengukuran, analisis, dan evaluasi penerapan SMKI;
g. Laporan audit internal;
h. Laporan rapat tinjauan manajemen;
i. Dokumen tindak lanjut hasil evaluasi terhadap pelaksanaan SMKI; dan
j. Pedoman pengendalian dokumen.

BAB IV

PENGENDALIAN SMKI

Bagian Kesatu

Umum

Pasal 5

Pengendalian keamanan informasi di lingkungan Direktorat Jenderal Perbendaharaan terdiri dari 14 (empat belas) pengendalian, yaitu:

1. Pengendalian Kebijakan Keamanan Informasi;
2. Pengendalian Organisasi Keamanan Informasi;
3. Pengendalian Keamanan Sumber Daya Manusia (SDM);
4. Pengendalian Pengelolaan Aset Informasi;
5. Pengendalian Akses;
6. Pengendalian Terhadap Penerapan Kriptografi;
7. Pengendalian Keamanan Fisik dan Lingkungan;
8. Pengendalian Pengelolaan Keamanan Operasional;
9. Pengendalian Keamanan Komunikasi;
10. Pengendalian Keamanan Informasi dalam Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi;
11. Pengendalian Hubungan dengan Pemasok;
12. Pengendalian Pengelolaan Gangguan Keamanan Informasi
13. Pengendalian Aspek Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan; dan
14. Pengendalian Kepatuhan.

Bagian Kedua

Pengendalian Kebijakan Keamanan Informasi

Pasal 6

(1) Unit menetapkan, mempublikasikan, dan mengkomunikasikan Kebijakan Keamanan Informasi kepada seluruh pegawai di lingkungan Direktorat Jenderal Perbendaharaan dan Pihak Ketiga.

(2) Unit melakukan evaluasi dan reviu atas Kebijakan Keamanan Informasi di lingkungan Direktorat Jenderal Perbendaharaan secara berkala paling singkat 2 (dua) tahun sekali.

(3) Dalam hal terjadi perubahan yang signifikan, Unit dapat melakukan evaluasi dan reviu atas Kebijakan Keamanan Informasi di lingkungan Direktorat Jenderal Perbendaharaan sebagaimana dimaksud pada ayat (2) kurang dari jangka waktu 2 (dua) tahun.

Bagian Ketiga

Pengendalian Organisasi Keamanan Informasi

Pasal 7

(1) Pengendalian Organisasi Keamanan Informasi terdiri dari:
   a. Organisasi Keamanan Informasi Direktorat Jenderal Perbendaharaan; dan
   b. *Mobile Device* dan *Teleworking.*

(2) Organisasi Keamanan Informasi Direktorat Jenderal Perbendaharaan sebagaimana dimaksud pada ayat (1) huruf a dilaksanakan dengan ketentuan:
   a. Organisasi Keamanan Informasi Direktorat Jenderal Perbendaharaan bertanggung jawab mengelola keamanan informasi di lingkungan Direktorat Jenderal Perbendaharaan;
   b. peran dan tanggung jawab pengelolaan keamanan informasi harus didefinisikan dan dipetakan, termasuk mengenai pemisahan tugas dan area tanggung jawab;
   c. Organisasi Keamanan Informasi Direktorat Jenderal Perbendaharaan menjalin kerjasama dengan Kementerian/Lembaga yang mengoordinasikan pelaksanaan keamanan informasi nasional dan pihak-pihak berwenang terkait dengan keamanan informasi serta menjalin kerjasama dengan komunitas keamanan informasi di luar Direktorat Jenderal Perbendaharaan; dan
   d. keamanan informasi harus diterapkan dalam manajemen proyek untuk seluruh tipe proyek.

(3) Penggunaan *Mobile Device* dan *Teleworking* sebagaimana dimaksud pada ayat (1) huruf b dilaksanakan dengan ketentuan:

a. Unit menerapkan aturan untuk mengelola risiko terkait penggunaan *mobile device*; dan

b. Unit menerapkan aturan untuk melindungi informasi yang diakses, diproses, atau disimpan pada lokasi *teleworking*.

Bagian Keempat

Pengendalian Keamanan Sumber Daya Manusia (SDM)

Pasal 8

(1) Unit dan Instansi melaksanakan pengendalian keamanan informasi kepada seluruh pegawai dan Pemasok.

(2) Pengendalian keamanan informasi sebagaimana dimaksud pada ayat (1) meliputi:

a. pengendalian sebelum bertugas/bekerja di unit kerja masing-masing;

b. pengendalian selama bertugas/bekerja di unit kerja masing-masing, dan

c. pengendalian setelah bertugas/bekerja di unit kerja masing-masing;

untuk memastikan pegawai dan Pemasok memahami tanggung jawab terkait keamanan informasi.

(3) Pengendalian sebelum pegawai dan Pemasok bertugas di unit kerja masing-masing sebagaimana dimaksud pada ayat (2) huruf a, paling sedikit meliputi:

a. Unit dan Instansi melaksanakan pemeriksaan (*screening*) data pribadi; dan

b. Unit dan Instansi memastikan:

1) Pemasok menandatangani perjanjian untuk menjaga keamanan informasi Direktorat Jenderal Perbendaharaan; dan

2) pegawai menandatangani dokumen yang memuat tanggung jawab menjaga kerahasiaan informasi Direktorat Jenderal Perbendaharaan.

(4) Pengendalian selama pegawai dan Pemasok bertugas di unit kerja masing-masing sebagaimana dimaksud pada ayat (2) huruf b, paling sedikit meliputi:

a. Unit dan Instansi harus memastikan pegawai dan Pemasok menerapkan semua kebijakan dan prosedur keamanan informasi, dan menindaklanjuti semua pelanggaran terhadap keamanan informasi;

b. Unit dan Instansi melaksanakan peningkatan pendidikan, pelatihan, dan kepedulian keamanan informasi kepada pegawai secara berkala sesuai tanggung jawabnya; dan

c. pelaksanaan peningkatan kepedulian terkait keamanan informasi untuk Pemasok.

(5) Pengendalian sesudah pegawai dan Pemasok bertugas di unit kerja masing-masing sebagaimana dimaksud pada ayat (2) huruf c, paling sedikit meliputi:

a. Unit dan Instansi memastikan pegawai yang telah menyelesaikan masa kerja atau mutasi tetap bertanggung jawab atas keamanan informasi di lingkungan Direktorat Jenderal Perbendaharaan; dan

b. Unit dan Instansi memastikan Pemasok yang telah menyelesaikan hubungan kerja tetap bertanggung jawab atas keamanan informasi di lingkungan Direktorat Jenderal Perbendaharaan.

Bagian Kelima

Pengendalian Pengelolaan Aset Informasi

Pasal 9

(1) Aset Informasi terdiri dari aset dalam bentuk:

a. data/dokumen, meliputi data ekonomi dan keuangan, data gaji, data kepegawaian, dokumen penawaran dan kontrak, dokumen perjanjian kerahasiaan, kebijakan kementerian, hasil penelitian, bahan penelitian, prosedur operasional, rencana kelangsungan bisnis (*business continuity plan*), dan hasil audit;

b. Perangkat Lunak, meliputi perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat bantu pengembangan sistem;

c. aset berwujud (*tangible*), meliputi sumber daya manusia, perangkat komputer, perangkat jaringan dan komunikasi, *removable* media, dan perangkat pendukung; dan

d. aset tak berwujud (*intangible*), meliputi pengetahuan, pengalaman, keahlian, citra, dan reputasi.

(2) Pengendalian Pengelolaan Aset Informasi terdiri dari:

a. Tanggung jawab terhadap Aset Informasi;

b. Klasifikasi Aset Informasi; dan

c. Penanganan Media Penyimpanan Informasi.

(3) Tanggung jawab terhadap Aset Informasi sebagaimana dimaksud pada ayat (2) huruf a dilaksanakan dengan ketentuan:

a. Unit dan Instansi melaksanakan identifikasi Aset Informasi dan mendokumentasikannya dalam daftar inventaris Aset Informasi serta menentukan pemilik dan penanggung jawab aset;

b. Pemilik Aset Informasi menetapkan aturan penggunaan Aset Informasi; dan

c. pegawai dan Pemasok/Pihak Ketiga yang telah menyelesaikan masa kerja atau mutasi harus mengembalikan Aset Informasi Direktorat Jenderal Perbendaharaan yang berupa data/dokumen dan perangkat TIK.

(4) Klasifikasi Aset Informasi sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan dengan ketentuan:

a. Unit melaksanakan klasifikasi Aset Informasi sesuai tingkat kerahasiaan, nilai, tingkat kritikalitas, serta aspek hukumnya;

b. klasifikasi informasi berdasarkan tingkat kerahasiaan sesuai dengan ketentuan klasifikasi data pada peraturan mengenai tata kelola TIK di lingkungan Kementerian Keuangan;

c. pemberian label klasifikasi Aset Informasi Direktorat Jenderal Perbendaharaan dilakukan secara konsisten terhadap seluruh Aset Informasi; dan

d. Unit mengembangkan dan mengimplementasikan prosedur penanganan Aset Informasi Direktorat Jenderal Perbendaharaan sesuai dengan klasifikasi informasinya.

(5) Penanganan Media Penyimpanan Informasi sebagaimana dimaksud pada ayat (2) huruf c dilaksanakan dengan ketentuan:

a. Unit melaksanakan pengelolaan media penyimpanan informasi untuk mencegah pengungkapan, modifikasi, pemindahan, dan penghapusan informasi secara tidak sah; dan

b. pengelolaan media penyimpanan informasi sebagaimana dimaksud dalam huruf a, antara lain dilakukan dengan:

1) Unit harus mengimplementasikan prosedur penanganan media yang dapat dipindahkan (*removable media*);

2) media yang memuat informasi harus dilindungi terhadap akses, penyalahgunaan, atau perubahan yang tidak sah pada saat dipindahkan; dan

3) media yang tidak lagi dibutuhkan harus dihancurkan dengan aman menggunakan prosedur yang berlaku.

Bagian Keenam

Pengendalian Akses

Pasal 10

(1) Unit menyusun, mendokumentasikan, dan mengkaji ketentuan akses terhadap Aset Informasi berdasarkan kebutuhan organisasi dan ketentuan keamanan informasi.

(2) Unit menyediakan akses ke jaringan dan layanan jaringan untuk Pengguna sesuai dengan tingkat wewenangnya.

(3) Unit harus mengelola akses seperti pendaftaran, penyediaan, peninjauan, penghapusan, dan penyesuaian hak akses Pengguna.

(4) Penghapusan hak akses Pengguna, sebagaimana dimaksud pada ayat (3), harus dilakukan pada saat terjadi penghentian pegawai, penghentian kontrak/perjanjian atau disesuaikan dengan perubahan yang terjadi.

(5) Unit harus membatasi dan mengendalikan penggunaan hak akses khusus yaitu hak akses terhadap Sistem TIK yang bersifat sensitif, termasuk di dalamnya namun tidak terbatas pada sistem operasi, perangkat penyimpanan (*storage devices*), *file server*, dan aplikasi-aplikasi yang bersifat sensitif.

(6) Unit harus memastikan bahwa akses terhadap Sistem TIK dilaksanakan dengan aman.

(7) Pengguna sebagaimana dimaksud pada ayat (3), bertanggung jawab menjaga kerahasiaan dalam menggunakan akun dan kata sandi, sesuai dengan ketentuan mengenai penggunaan akun dan kata sandi, surat elektronik, intranet dan internet di lingkungan Kementerian Keuangan.

(8) Pembatasan akses ke informasi dan Sistem TIK harus diterapkan sesuai dengan kendali akses (matrik akses).

(9) Unit harus memastikan Sistem TIK memiliki fitur pengelolaan kata sandi yang interaktif dan berkualitas.

(10) Unit harus membatasi dan mengendalikan dengan ketat penggunaan program utilitas yang dapat membatalkan kendali keamanan sistem informasi.

(11) Unit harus membatasi akses ke kode sumber program.

Bagian Ketujuh

Pengendalian Terhadap Penerapan Kriptografi

Pasal 11

Unit menerapkan Kriptografi yang tepat dan efektif untuk melindungi kerahasiaan, keabsahan, dan integritas informasi.

Bagian Kedelapan

Pengendalian Keamanan Fisik dan Lingkungan

Pasal 12

(1) Pengendalian Keamanan Fisik dan Lingkungan terdiri dari:
   a. Area yang aman; dan
   b. Pengamanan Fasilitas Pengolah Informasi.

(2) Area yang aman sebagaimana dimaksud pada ayat (1) huruf a dilaksanakan dengan ketentuan:
   a. Unit dan Instansi menerapkan pengamanan fisik kantor, ruangan, serta fasilitasnya untuk melindungi area yang berisi informasi yang bersifat rahasia dan sangat rahasia, dengan cara:
      1) membuat parameter;
      2) membatasi akses masuk;
      3) mendesain pengamanan dan penempatan fasilitas, ruangan, dan kantor; dan
      4) membangun perlindungan terhadap ancaman bencana alam, serangan berbahaya, dan kecelakaan;
   b. Unit dan Instansi merancang dan menerapkan prosedur untuk bekerja di area yang aman; dan
   c. Unit dan Instansi menjaga, mengawasi, dan mengendalikan area keluar masuk barang untuk menghindari akses ke Perangkat TIK oleh pihak yang tidak berwenang.

(3) Pengamanan Fasilitas Pengolah Informasi sebagaimana dimaksud pada ayat (1) huruf b dilaksanakan dengan ketentuan:

a. Unit dan Instansi harus menempatkan dan melindungi Fasilitas Pengolah Informasi dari ancaman dan bahaya lingkungan, serta akses tidak sah;
b. Unit dan Instansi harus melindungi Perangkat Pengolah Informasi dari kegagalan catu daya (*power supply*) dan gangguan lain yang disebabkan oleh kegagalan perangkat pendukung;
c. kabel daya dan telekomunikasi yang membawa data dan informasi harus dilindungi dari intersepsi, interferensi dan/atau kerusakan;
d. Unit dan Instansi harus melakukan pemeliharaan yang tepat terhadap Fasilitas Pengolah Informasi untuk menjamin keutuhan dan ketersediaan Fasilitas Pengolah Informasi;
e. perangkat penyimpan data yang sudah tidak digunakan lagi harus dilakukan penghapusan data secara permanen sebelum digunakan kembali atau dihapuskan/dimusnahkan;
f. penggunaan Aset Informasi Direktorat Jenderal Perbendaharaan yang dibawa ke luar dari lingkungan kantor Unit dan Instansi harus disetujui oleh Pejabat yang berwenang.
g. Pengguna harus memastikan Aset Informasi Direktorat Jenderal Perbendaharaan yang tidak berada dalam pengawasan atau yang digunakan di luar lingkungan kantor memiliki perlindungan keamanan yang tepat; dan
h. Unit dan Instansi menerapkan aturan bagi pegawai yang meninggalkan area kerja agar membersihkan media yang menampilkan informasi rahasia dan sangat rahasia.

9

Bagian Kesembilan

Pengendalian Pengelolaan Keamanan Operasional

Pasal 13

(1) Pengendalian Pengelolaan Keamanan Operasional terdiri dari:
   a. prosedur operasional dan tanggung jawab;
   b. perlindungan terhadap ancaman program yang membahayakan (*malware*);
   c. pengelolaan *backup;*
   d. pengelolaan data aktivitas *(log)* dan pemantauan;
   e. pengendalian perangkat lunak operasional;
   f. pengelolaan kerentanan teknis; dan
   g. pelaksanaan Audit Sistem Informasi.

(2) Prosedur operasional dan tanggung jawab sebagaimana dimaksud pada ayat (1) huruf a dilaksanakan dengan ketentuan:
   a. Unit mendokumentasikan, memelihara, dan menyediakan seluruh prosedur operasional yang terkait dengan penggunaan Perangkat TIK bagi pengguna sesuai dengan peruntukannya;
   b. Unit harus mengelola perubahan organisasi, proses bisnis, dan Fasilitas Pengolah Informasi yang berdampak terhadap keamanan informasi;
   c. Unit harus melakukan pemisahan lingkungan pengembangan, pengujian, dan operasional Sistem TIK untuk mengurangi risiko perubahan atau akses tidak sah terhadap sistem operasional;
   d. Unit harus melakukan pemantauan penggunaan sumber daya dan membuat perkiraan kebutuhan untuk memastikan kecukupan kapasitas sumber daya yang akan datang; dan
   e. Unit harus melakukan pemantauan terhadap ketersediaan Fasilitas Pengolah Informasi dan memastikan Fasilitas Pengolah Informasi berfungsi sebagaimana mestinya.

(3) Perlindungan terhadap ancaman program yang membahayakan *(malware)* sebagaimana dimaksud pada ayat (1) huruf b dilaksanakan dengan ketentuan Unit harus menerapkan sistem yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap *malware*, disertai dengan pemberian *awareness* atas ancaman *malware* kepada Pengguna, melalui:

a. implementasi perangkat lunak anti *malware* yang dilaksanakan sesuai dengan ketentuan mengenai anti *malicious code* dan perangkat lunak antivirus di lingkungan Direktorat Jenderal Perbendaharaan; dan

b. implementasi *join domain* Kementerian Keuangan yang dilaksanakan sesuai dengan ketentuan mengenai manajemen perangkat TIK di lingkungan Direktorat Jenderal Perbendaharaan.

(4) Pengelolaan *Backup* sebagaimana dimaksud pada ayat (1) huruf c dilaksanakan dengan ketentuan Unit harus melakukan *backup* terhadap informasi dan Perangkat Lunak yang berada di Pusat Data (*Data Center*) secara berkala, dengan ketentuan sebagai berikut:

a. *backup* dilaksanakan terhadap:
   1) sistem operasi;
   2) aplikasi;
   3) data dan/atau informasi; dan
   4) konfigurasi;

b. Unit melaksanakan *backup* sesuai dengan tanggung jawab dan kewenangannya;

c. tanggung jawab sebagaimana dimaksud dalam huruf b, dituangkan dalam *Service Level Agreement* (SLA) antara Unit dengan Unit TIK Pusat, dengan mengacu kepada tingkat kritikalitas layanan TIK berdasarkan *business impact analysis*; dan

d. Unit melaksanakan *restore* secara berkala untuk memverifikasi hasil *backup*.

(5) Pengelolaan data aktivitas *(log)* dan pemantauan sebagaimana dimaksud pada ayat (1) huruf d dilaksanakan dengan ketentuan:

a. Unit harus mencatat, menyimpan, dan meninjau secara berkala data aktivitas yang terdiri dari aktivitas Pengguna/administrator/operator, pengecualian (*exception*), kegagalan, dan Kejadian Keamanan lnformasi pada sistem;

b. fasilitas pencatat *log* dan informasi *log* harus dilindungi terhadap pemalsuan dan akses yang tidak sah; dan

c. Unit harus memastikan semua Perangkat TIK yang tersambung dengan jaringan Kementerian Keuangan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.

(6) Pengendalian perangkat lunak operasional sebagaimana dimaksud pada ayat (1) huruf e dilaksanakan dengan ketentuan Unit harus menerapkan prosedur untuk mengendalikan instalasi Perangkat Lunak pada sistem operasional.

(7) Pengelolaan kerentanan teknis sebagaimana dimaksud pada ayat (1) huruf f dilaksanakan dengan ketentuan:

a. Unit harus melakukan evaluasi dan penilaian risiko secara berkala terhadap kerentanan teknis yang ditemukan dalam Sistem Informasi serta menetapkan pengendalian yang tepat terhadap risiko terkait;

b. pengendalian terhadap risiko kerentanan teknis dapat dilakukan dengan mengimplementasikan *baseline* konfigurasi keamanan sesuai dengan ketentuan mengenai *baseline* konfigurasi keamanan di lingkungan Kementerian Keuangan; dan

c. Unit membatasi Pengguna dalam melakukan instalasi Perangkat Lunak.

(8) Pelaksanaan Audit Sistem Informasi sebagaimana dimaksud pada ayat (1) huruf g dilaksanakan dengan ketentuan Audit Sistem Informasi yang melibatkan verifikasi sistem operasional harus direncanakan secara hati-hati dan disepakati para pihak yang terlibat dalam proses audit untuk memperkecil gangguan terhadap proses bisnis.

Bagian Kesepuluh

Pengendalian Keamanan Komunikasi

Pasal 14

(1) Pengendalian Keamanan Komunikasi terdiri dari:
   a. pengelolaan keamanan jaringan; dan
   b. keamanan dalam transfer informasi.

(2) Pengelolaan keamanan jaringan sebagaimana dimaksud pada ayat (1) huruf a dilaksanakan dengan ketentuan:
   a. Unit bekerja sama dengan Unit TIK Pusat dalam mengelola dan mengendalikan jaringan, termasuk memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi; dan
   b. Unit memastikan Unit TIK Pusat dapat memberikan jaminan layanan jaringan yang tertuang dalam kesepakatan penyediaan layanan, termasuk layanan yang disediakan oleh Pemasok.

(3) Keamanan dalam transfer informasi sebagaimana dimaksud pada ayat (1) huruf b dilaksanakan dengan ketentuan:
   a. Unit harus menetapkan kebijakan, prosedur, dan pengendalian transfer informasi yang dikirimkan melalui semua jenis fasilitas komunikasi;
   b. Unit menyusun kesepakatan yang mengatur transfer informasi yang aman dengan Pihak Ketiga;
   c. Unit harus menerapkan pengamanan informasi yang terdapat dalam surat elektronik, sebagaimana diatur dalam ketentuan mengenai penggunaan akun dan kata sandi, surat elektronik, intranet dan internet di lingkungan Kementerian Keuangan; dan

d. Unit memastikan persyaratan kerahasiaan terkait kegiatan transfer informasi dengan Pihak Ketiga melalui Perjanjian Kerahasiaan atau *Non Disclosure Agreement*.

Bagian Kesebelas

Pengendalian Keamanan Informasi dalam

Akuisisi, Pengembangan, dan Pemeliharaan Sistem Informasi

Pasal 15

(1) Pengendalian keamanan Informasi dalam akuisisi, pengembangan, dan pemeliharaan sistem informasi terdiri dari:
   a. persyaratan keamanan pada Sistem Informasi;
   b. keamanan dalam proses pengembangan dan pendukung; dan
   c. data pengujian.

(2) Persyaratan keamanan pada Sistem Informasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui:
   a. analisis dan spesifikasi persyaratan keamanan Sistem Informasi yang dilaksanakan dengan ketentuan:
      1) Unit menetapkan dan mendokumentasikan persyaratan keamanan informasi yang relevan sebelum pengembangan Sistem Informasi;
      2) persyaratan keamanan informasi yang harus disusun juga termasuk *vulnerability point* atas Sistem Informasi yang akan dikembangkan; dan
      3) Unit harus mengindentifikasi risiko dari setiap *vulnerability point* dan menentukan mitigasi yang harus diterapkan dalam pengembangan Sistem Informasi.
   b. Pengamanan layanan aplikasi pada jaringan publik yang dilaksanakan dengan ketentuan:

1) Unit harus melindungi informasi dalam layanan aplikasi yang melewati jaringan publik dari kegiatan penipuan, perselisihan, dan pengungkapan informasi serta kegiatan modifikasi yang tidak sah; dan
2) Unit harus melakukan penilaian risiko terkait potensi serangan siber terhadap Sistem Informasi yang dapat diakses melalui jaringan publik, serta menetapkan pengendalian yang tepat terhadap risiko terkait.

c. Perlindungan transaksi layanan aplikasi yang dilaksanakan dengan ketentuan Unit harus melindungi informasi dalam transaksi pada layanan aplikasi untuk mencegah transmisi informasi yang tidak lengkap, kesalahan *Routing* dan perubahan, serta pengungkapan dan duplikasi pesan yang tidak sah.

(3) Keamanan dalam proses pengembangan dan pendukung sebagaimana dimaksud pada ayat (1) huruf b dilaksanakan dengan ketentuan:

a. Unit harus menerapkan ketentuan pengembangan Sistem Informasi yang aman;
b. Unit harus mengelola perubahan pada sistem dalam setiap tahapan pengembangan Sistem Informasi dengan menerapkan prosedur pengelolaan perubahan;
c. Unit harus melakukan *review* teknis dan uji coba setelah adanya perubahan *platform*;
d. perubahan terhadap paket program (*software package*) harus dibatasi;
e. prinsip untuk rekayasa sistem yang aman harus ditetapkan, didokumentasikan, dipelihara dan diterapkan pada setiap upaya implementasi sistem informasi;
f. Unit harus melakukan perlindungan terhadap lingkungan pengembangan pada seluruh tahapan pengembangan Sistem Informasi dan melakukan

pengawasan dalam hal pengembangan dilakukan oleh Pihak Ketiga;

g. pengujian fungsi keamanan harus dilakukan selama pengembangan; dan

h. program pengujian penerimaan dan kriteria lain harus ditetapkan untuk Sistem Informasi baru, peningkatan dan versi baru.

(4) Data pengujian sebagaimana dimaksud pada ayat (1) huruf c harus dipilih dengan hati-hati, dilindungi, dan dikendalikan.

Bagian Keduabelas

Pengendalian Hubungan dengan Pemasok

Pasal 16

(1) Unit dan Instansi memastikan Pemasok menyetujui seluruh persyaratan keamanan informasi yang ditetapkan dalam perjanjian, termasuk mitigasi risiko terkait rantai pasok layanan dan produk TIK.

(2) Unit dan Instansi melakukan pemantauan, *review*, dan audit secara berkala layanan Pemasok.

(3) Unit dan Instansi melakukan pengelolaan perubahan ketentuan layanan Pemasok, dengan mempertimbangkan kritikalitas informasi, sistem dan proses bisnis serta perlu adanya asesmen ulang risiko.

Bagian Ketigabelas

Pengendalian Pengelolaan Gangguan Keamanan Informasi

Pasal 17

(1) Unit menyusun dan menetapkan prosedur dan tanggung jawab pegawai untuk memastikan tanggapan yang cepat, efektif, dan tepat untuk gangguan keamanan informasi.

(2) Setiap pegawai dan Pemasok wajib melaporkan adanya kejadian dan/atau kelemahan keamanan informasi kepada petugas keamanan informasi dan/atau melalui Layanan Pengguna HAI-DJPb.

(3) Unit menilai dan memutuskan bahwa Kejadian Keamanan Informasi merupakan gangguan keamanan informasi.

(4) Unit memastikan tanggapan dan penanganan gangguan keamanan informasi dilakukan sesuai dengan prosedur yang berlaku.

(5) Unit mendokumentasikan seluruh gangguan keamanan informasi yang terjadi beserta tindakan perbaikannya untuk digunakan sebagai basis pengetahuan agar dapat mengurangi peluang atau dampak gangguan di masa mendatang.

(6) Unit mendefinisikan dan menerapkan prosedur untuk melakukan identifikasi, pengumpulan, akuisisi, dan preservasi informasi yang dapat berguna sebagai bukti gangguan keamanan informasi.

(7) Unit bersama dengan Unit TIK Pusat berkoordinasi dengan Pusat Operasi Keamanan Siber Nasional Badan Siber dan Sandi Negara (BSSN) dalam hal penanganan gangguan siber.

Bagian Keempatbelas
Pengendalian Aspek Keamanan Informasi
dalam Pengelolaan Kelangsungan Kegiatan

Pasal 18

(1) Unit harus melakukan perencanaan dan penerapan kelangsungan keamanan informasi jika terjadi keadaan kahar yang merugikan, seperti selama keadaan krisis atau bencana.

(2) Unit harus melakukan evaluasi pengendalian kelangsungan keamanan informasi dalam keadaan kahar untuk memastikan pengendalian dimaksud valid dan efektif.

(3) Unit harus mengelola Infrastruktur TIK dengan *redundancy* yang memadai untuk memenuhi persyaratan ketersediaan.

(4) *Redundancy* Sistem Informasi harus diuji secara berkala untuk memastikan kelangsungan kegiatan.

Bagian Kelimabelas
Pengendalian Kepatuhan

Pasal 19

(1) Pengendalian Kepatuhan terdiri dari:
   a. kepatuhan terhadap persyaratan peraturan perundang-undangan dan perjanjian; dan
   b. *review* keamanan informasi.

(2) Kepatuhan terhadap persyaratan peraturan perundang-undangan dan perjanjian sebagaimana dimaksud pada ayat (1) huruf a dilakukan dengan ketentuan:
   a. Unit harus mengidentifikasi, mendokumentasikan, dan memelihara kemutakhiran semua persyaratan peraturan perundang-undangan dan kontrak yang terkait dengan keamanan informasi;
   b. Unit harus menerapkan prosedur untuk memastikan kepatuhan terhadap peraturan perundang-undangan dan persyaratan kontrak terkait dengan hak atas kekayaan intelektual dan penggunaan Perangkat Lunak berlisensi;
   c. Unit harus melindungi arsip milik Direktorat Jenderal Perbendaharaan dari kehilangan, kerusakan, pemalsuan, akses yang tidak sah dan rilis yang tidak sah;
   d. Unit harus melindungi privasi dan data pribadi sesuai ketentuan perundang-undangan yang berlaku; dan
   e. Unit melaksanakan pengendalian Kriptografi dalam rangka kepatuhan terhadap perjanjian dan peraturan perundang-undangan.

(3) *Review* keamanan informasi sebagaimana dimaksud pada ayat (1) huruf b dilakukan dengan ketentuan:
   a. Unit melakukan *review* secara independen terhadap pengelolaan dan penerapan keamanan informasi secara berkala dalam selang waktu yang direncanakan atau ketika terjadi perubahan yang signifikan;

b. Unit melakukan *review* kepatuhan proses dan prosedur pada area tanggung jawab Unit sesuai dengan kebijakan, standar dan persyaratan keamanan lainnya; dan

c. Unit harus melakukan *review* aspek keamanan pada Sistem Informasi secara berkala agar tetap sesuai dengan kebijakan dan standar keamanan informasi.

BAB V
ORGANISASI KEAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 20

Ketentuan Organisasi Keamanan Informasi Direktorat Jenderal Perbendaharaan terdiri dari:

a. Struktur Organisasi; dan

b. Tugas dan Tanggung Jawab.

Bagian Kedua
Struktur Organisasi

Pasal 21

Struktur Organisasi Keamanan Informasi Direktorat Jenderal Perbendaharaan sebagaimana dimaksud dalam Pasal 20 huruf a terdiri dari:

a. Organisasi Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan; dan

b. Organisasi Keamanan Informasi Instansi Vertikal Direktorat Jenderal Perbendaharaan.

Pasal 22

(1) Organisasi Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan sebagaimana dimaksud dalam Pasal 21 huruf a mengelola keamanan informasi di lingkup Direktorat Jenderal Perbendaharaan.

(2) Struktur Organisasi Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan sekurang-kurangnya terdiri dari:
   a. Ketua Keamanan Informasi;
   b. Koordinator Keamanan Informasi; dan
   c. Petugas Keamanan Informasi.

(3) Ketua Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan sebagaimana dimaksud pada ayat (2) huruf a dijabat oleh Pejabat Eselon II yang membawahi Unit TIK Direktorat Jenderal Perbendaharaan.

(4) Koordinator Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan sebagaimana dimaksud pada ayat (2) huruf b dijabat oleh Pejabat setingkat eselon III pada Unit TIK Direktorat Jenderal Perbendaharaan.

(5) Petugas Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan sebagaimana dimaksud pada ayat (2) huruf c dijabat oleh Pejabat/Pelaksana pada Unit TIK Direktorat Jenderal Perbendaharaan dan Unit Eselon II di lingkup Kantor Pusat Direktorat Jenderal Perbendaharaan yang diusulkan oleh Pimpinan Unit Eselon II di lingkup Kantor Pusat Direktorat Jenderal Perbendaharaan.

(6) Organisasi Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan ditetapkan melalui Keputusan Direktur Jenderal Perbendaharaan.

Pasal 23

(1) Organisasi Keamanan Informasi Instansi Vertikal Direktorat Jenderal Perbendaharaan sebagaimana dimaksud dalam Pasal 21 huruf b mengelola keamanan informasi di lingkup Kantor Wilayah Direktorat Jenderal Perbendaharaan, termasuk KPPN di wilayah kerjanya.

(2) Struktur Organisasi Keamanan Informasi Instansi Vertikal Direktorat Jenderal Perbendaharaan terdiri dari:

4

a. Koordinator Keamanan Informasi Instansi Vertikal, dijabat oleh Pejabat setingkat eselon III yang ditunjuk oleh Kepala Kantor Wilayah Direktorat Jenderal Perbendaharaan; dan

b. Petugas Keamanan Informasi Instansi Vertikal, dijabat oleh Pejabat/Pelaksana pada Kantor Wilayah Direktorat Jenderal Perbendaharaan dan perwakilan Pejabat/Pelaksana dari KPPN di lingkup wilayah kerja Kantor Wilayah Direktorat Jenderal Perbendaharaan, yang ditunjuk oleh Kepala Kantor Wilayah Direktorat Jenderal Perbendaharaan.

(3) Organisasi Keamanan Informasi Instansi Vertikal Direktorat Jenderal Perbendaharaan ditetapkan melalui Keputusan Kepala Kantor Wilayah Direktorat Jenderal Perbendaharaan sesuai wilayah kerjanya masing-masing.

Bagian Ketiga

Tugas dan Tanggung Jawab

Pasal 24

(1) Ketua Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan sebagaimana dimaksud dalam Pasal 22 ayat (2) huruf a bertanggung jawab untuk:

a. mengoordinasikan perumusan dan penyempurnaan Kebijakan Keamanan Informasi di Direktorat Jenderal Perbendaharaan;

b. menetapkan target dan rencana kerja keamanan informasi setiap tahunnya di Direktorat Jenderal Perbendaharaan;

c. berkoordinasi dengan Unit Pemilik Risiko Direktorat Jenderal Perbendaharaan dalam pelaksanaan manajemen risiko keamanan informasi di Direktorat Jenderal Perbendaharaan;

d. memastikan pelaksanaan audit internal secara berkala untuk memeriksa kepatuhan terhadap kebijakan, persyaratan, standar, dan prosedur keamanan informasi, minimal sekali dalam setahun;

e. memastikan efektivitas penerapan Kebijakan Keamanan Informasi di Lingkungan Direktorat Jenderal Perbendaharaan; dan

f. melaporkan kinerja penerapan kebijakan serta pencapaian target keamanan informasi di Direktorat Jenderal Perbendaharaan kepada Ketua Keamanan Informasi Kementerian Keuangan dan tembusan kepada Direktur Jenderal Perbendaharaan.

(2) Koordinator Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan sebagaimana dimaksud dalam Pasal 22 ayat (2) huruf b bertanggung jawab untuk:

a. mengoordinasikan penerapan Kebijakan Keamanan Informasi di Direktorat Jenderal Perbendaharaan;

b. memastikan langkah-langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan dalam pelaksanaan evaluasi dan/atau audit penerapan Kebijakan Keamanan Informasi di Direktorat Jenderal Perbendaharaan;

c. mengoordinasikan penanganan gangguan keamanan informasi pada Direktorat Jenderal Perbendaharaan;

d. mengoordinasikan pelaksanaan evaluasi efektivitas Kebijakan Keamanan Informasi dan penerapannya pada Direktorat Jenderal Perbendaharaan;

e. mengoordinasikan dengan pihak terkait dalam rangka peningkatan pengetahuan dan keterampilan terkait keamanan informasi;

f. mengoordinasikan kepedulian seluruh pegawai terhadap Kebijakan Keamanan Informasi pada Direktorat Jenderal Perbendaharaan;

g. melaporkan kinerja penerapan Kebijakan Keamanan Informasi pada Direktorat Jenderal Perbendaharaan sesuai ruang lingkup tanggung jawabnya kepada Ketua Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan; dan

h. menjalankan tugas lain terkait penerapan keamanan informasi.

(3) Petugas Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan sebagaimana dimaksud dalam Pasal 22 ayat (2) huruf c bertanggung jawab untuk:

a. melaksanakan dan memantau penerapan Kebijakan Keamanan Informasi di Direktorat Jenderal Perbendaharaan;
b. memberi masukan dalam rangka penyempurnaan Kebijakan Keamanan Informasi di Direktorat Jenderal Perbendaharaan;
c. mengusulkan kebutuhan pendidikan dan pelatihan terkait keamanan informasi bagi pegawai di Direktorat Jenderal Perbendaharaan;
d. memantau, mencatat, menguraikan adanya gangguan keamanan informasi dan menindaklanjuti sesuai prosedur penanganan gangguan keamanan informasi di Direktorat Jenderal Perbendaharaan;
e. memberikan panduan dan/atau bantuan penyelesaian masalah-masalah keamanan informasi di Direktorat Jenderal Perbendaharaan;
f. menyampaikan *progress* pelaksanaan Kebijakan Keamanan Informasi di Direktorat Jenderal Perbendaharaan kepada Koordinator Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan;
g. menjalankan tugas lain terkait penerapan keamanan informasi; dan
h. melaporkan kinerja penerapan Kebijakan Keamanan Informasi pada Direktorat Jenderal Perbendaharaan sesuai ruang lingkup tanggung jawabnya kepada Koordinator Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan.

Pasal 25

(1) Koordinator Keamanan Informasi Instansi Vertikal sebagaimana dimaksud dalam Pasal 23 ayat (2) huruf a bertanggung jawab untuk:

a. mengoordinasikan penerapan Kebijakan Keamanan Informasi di lingkungan instansi vertikal masing-masing;
b. memastikan langkah-langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi hasil evaluasi dan/atau audit penerapan Kebijakan Keamanan Informasi di lingkungan instansi vertikal masing-masing;
c. mengoordinasikan penanganan gangguan keamanan informasi di lingkungan instansi vertikal masing-masing;
d. mengoordinasikan dengan pihak terkait dalam rangka peningkatan pengetahuan dan keterampilan terkait keamanan informasi;
e. mengoordinasikan kepedulian seluruh pegawai terhadap Kebijakan Keamanan Informasi di lingkungan instansi vertikal masing-masing; dan
f. melaporkan kinerja penerapan Kebijakan Keamanan Informasi di lingkungan instansi vertikal masing-masing sesuai ruang lingkup tanggung jawabnya kepada Ketua Keamanan Informasi Kantor Pusat Direktorat Jenderal Perbendaharaan dan tembusan kepada Kepala Kantor Wilayah Direktorat Jenderal Perbendaharaan.

(2) Petugas Keamanan Informasi Instansi Vertikal sebagaimana dimaksud dalam Pasal 23 ayat (2) huruf b bertanggung jawab untuk:
a. melaksanakan dan memantau penerapan Kebijakan Keamanan Informasi di lingkungan instansi vertikal masing-masing;
b. memberi masukan untuk meningkatkan penerapan Kebijakan Keamanan Informasi di lingkungan instansi vertikal masing-masing;
c. mengusulkan kebutuhan pendidikan dan pelatihan terkait keamanan informasi bagi pegawai di lingkungan instansi vertikal masing-masing;

d. memantau, mencatat, dan menguraikan adanya gangguan keamanan informasi dan menindaklanjuti sesuai dengan prosedur penanganan gangguan keamanan informasi di lingkungan instansi vertikal masing-masing;

e. memberikan panduan dan/atau bantuan penyelesaian masalah-masalah keamanan informasi di lingkungan instansi vertikal masing-masing; dan

f. melaporkan pelaksanaan dan pemantauan penerapan Kebijakan Keamanan Informasi di lingkungan instansi vertikal masing-masing kepada Koordinator Keamanan Informasi instansi vertikal.

BAB VI
SERTIFIKASI PELAKSANAAN SMKI

Pasal 26

(1) Dalam pelaksanaan SMKI di lingkungan Direktorat Jenderal Perbendaharaan, Unit harus membuat kategori atas setiap Sistem Elektronik yang diselenggarakan di lingkungan Direktorat Jenderal Perbendaharaan.

(2) Kategori Sistem Elektronik di lingkungan Direktorat Jenderal Perbendaharaan sebagaimana dimaksud pada ayat (1), terdiri atas:
   a. Sistem Elektronik Strategis;
   b. Sistem Elektronik Tinggi; dan
   c. Sistem Elektronik Rendah.

(3) Untuk menjamin efektivitas pelaksanaan SMKI, Unit selaku penyelenggara Sistem Elektronik di lingkungan Direktorat Jenderal Perbendaharaan:
   a. harus memiliki Sertifikat Sistem Manajemen Pengamanan Informasi untuk Sistem Elektronik dengan kategori Strategis dan Sistem Elektronik Tinggi; dan
   b. dapat memiliki Sertifikat Sistem Manajemen Pengamanan Informasi untuk Sistem Elektronik dengan kategori Sistem Elektronik Rendah.

(4) Sertifikat Sistem Manajemen Pengamanan Informasi sebagaimana dimaksud pada ayat (3) huruf a dan huruf b, diperoleh setelah Unit yang menyelenggarakan Sistem Elektronik melaksanakan sertifikasi SNI ISO/IEC 27001:2013.

(5) Unit yang menyelenggarakan Sistem Elektronik harus memiliki Sertifikat Sistem Manajemen Pengamanan Informasi untuk Sistem Elektronik dengan kategori Sistem Elektronik Strategis dan Sistem Elektronik Tinggi sebagaimana dimaksud pada ayat (3) huruf a paling lambat 2 (dua) tahun sejak Keputusan Menteri Keuangan mengenai pengelolaan keamanan informasi di lingkungan Kementerian Keuangan ditetapkan.

BAB VII
KETENTUAN LAIN-LAIN

Pasal 27

Pedoman teknis yang diperlukan dalam rangka pelaksanaan Peraturan Direktur Jenderal ini diatur lebih lanjut oleh *Chief Information Officer* (CIO) Direktorat Jenderal Perbendaharaan.

BAB VIII
KETENTUAN PENUTUP

Pasal 28

Pada saat Peraturan Direktur Jenderal ini berlaku, Peraturan Direktur Jenderal Perbendaharaan Nomor PER-17/PB/2019 tentang Kebijakan Sistem Manajemen Keamanan Informasi di Lingkungan Direktorat Jenderal Perbendaharaan dicabut dan dinyatakan tidak berlaku.

Pasal 29

Peraturan Direktur Jenderal Perbendaharaan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 15 Januari 2021

DIREKTUR JENDERAL PERBENDAHARAAN,

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTUR JENDERAL
DIREKTORAT JENDERAL PERBENDAHARAAN

ANDIN HADIYANTO