SALINAN

PERATURAN SEKRETARIS JENDERAL
KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI
NOMOR 11 TAHUN 2022
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI PADA
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK
KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI

DENGAN RAHMAT TUHAN YANG MAHA ESA

SEKRETARIS JENDERAL
KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI,

Menimbang : a. bahwa untuk menjamin kerahasiaan, integritas, dan ketersediaan aset informasi Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi, perlu mengatur manajemen keamanan informasi di lingkungan Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Sekretaris Jenderal Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi tentang Sistem Manajemen Keamanan Informasi pada Sistem Pemerintahan Berbasis Elektronik Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi;

Mengingat : 1. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916);

2. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
3. Peraturan Presiden Nomor 62 Tahun 2021 tentang Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 156);
4. Peraturan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi Nomor 28 Tahun 2021 tentang Organisasi dan Tata Kerja Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Berita Negara Republik Indonesia Tahun 2021 Nomor 963);
5. Peraturan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi Nomor 8 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi (Berita Negara Republik Indonesia Tahun 2022 Nomor 192);
6. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik;

MEMUTUSKAN:

Menetapkan : PERATURAN SEKRETARIS JENDERAL KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI PADA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET, DAN TEKNOLOGI.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Sekretaris Jenderal ini yang dimaksud dengan:

1. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penanggung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk merencanakan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengendalikan, dan meningkatkan keamanan informasi.
2. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
3. Keamanan Informasi adalah perlindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.
4. Koordinator SPBE Kementerian adalah Sekretaris Jenderal Kementerian.
5. Pengelola SPBE Kementerian adalah unit kerja pada Kementerian yang mempunyai tugas melaksanakan penyiapan perumusan kebijakan teknis dan pelaksanaan pengelolaan data dan statistik serta pengelolaan dan pendayagunaan teknologi informasi.
6. Kementerian adalah kementerian yang menyelenggarakan urusan pemerintahan di bidang pendidikan, kebudayaan, ilmu pengetahuan, dan teknologi.
7. Menteri adalah menteri yang menyelenggarakan urusan pemerintahan di bidang pendidikan, kebudayaan, ilmu pengetahuan, dan teknologi.

Pasal 2

(1) SMKI pada SPBE Kementerian digunakan sebagai pedoman bagi unit kerja di lingkungan Kementerian dalam pengamanan SPBE Kementerian.

(2) Pengamanan SPBE Kementerian sebagaimana dimaksud pada ayat (1) dilakukan terhadap aset SPBE Kementerian dalam bentuk:
   a. infrastruktur;
   b. data dan informasi; dan
   c. aplikasi.

BAB II

PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 3

(1) Unit kerja melakukan perencanaan SMKI pada SPBE di lingkungan unit kerja setiap tahun di bawah koordinasi Pengelola SPBE Kementerian.

(2) Perencanaan SMKI pada SPBE di lingkungan unit kerja sebagaimana dimaksud pada ayat (1) dilakukan dengan menyusun:
   a. program kerja keamanan SPBE di unit kerja yang disusun berdasarkan kategori risiko keamanan SPBE; dan
   b. target realisasi program kerja keamanan SPBE di unit kerja.

(3) Program kerja keamanan SPBE di unit kerja sebagaimana dimaksud pada ayat (2) huruf a paling sedikit memuat:
   a. edukasi kesadaran keamanan SPBE;
   b. manajemen risiko;
   c. penilaian kerentanan keamanan SPBE;
   d. peningkatan keamanan SPBE;
   e. penanganan insiden keamanan SPBE; dan
   f. audit keamanan SPBE.

(4) Target realisasi program kerja keamanan SPBE di unit kerja sebagaimana dimaksud pada ayat (2) huruf b ditetapkan berdasarkan kebutuhan unit kerja.

(5) Perencanaan SMKI pada SPBE di lingkungan unit kerja sebagaimana dimaksud pada ayat (1) disampaikan kepada Pengelola SPBE Kementerian melalui sekretaris unit utama.

Pasal 4

(1) Pengelola SPBE Kementerian melakukan analisis terhadap perencanaan SMKI pada SPBE di lingkungan unit kerja.

(2) Analisis sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan:
   a. kebutuhan organisasi; dan
   b. skala prioritas.

(3) Hasil analisis sebagaimana dimaksud pada ayat (2) diusulkan menjadi perencanaan SMKI pada SPBE Kementerian.

(4) Perencanaan SMKI pada SPBE Kementerian ditetapkan oleh Pengelola SPBE Kementerian.

(5) Perencanaan SMKI pada SPBE Kementerian sebagaimana dimaksud pada ayat (4) harus dilaksanakan oleh unit kerja.

BAB III

PENYELENGGARAAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Bagian Kesatu

Umum

Pasal 5

(1) SMKI pada SPBE Kementerian dilaksanakan dalam rangka memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan dalam pengelolaan SPBE Kementerian.

(2) SMKI pada SPBE Kementerian sebagaimana dimaksud pada ayat (1) meliputi:
   a. keamanan personil;
   b. keamanan aset;
   c. keamanan akses;
   d. keamanan kriptografi;
   e. keamanan fisik dan lingkungan;
   f. keamanan operasional;
   g. keamanan komunikasi;
   h. keamanan pengembangan dan pemeliharaan;
   i. keamanan pihak ketiga;
   j. manajemen insiden keamanan siber;
   k. manajemen keberlangsungan layanan SPBE Kementerian;
   l. pengendalian kepatuhan; dan
   m. audit keamanan SPBE Kementerian.

Bagian Kedua
Keamanan Personil

Pasal 6

(1) Keamanan personil sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a dilakukan untuk mengendalikan personil dalam melaksanakan kebijakan keamanan SPBE Kementerian.
(2) Keamanan personil dilakukan dengan cara:
   a. mengomunikasikan peran dan tanggung jawab pelaksanaan kebijakan keamanan SPBE kepada seluruh pegawai yang terlibat dalam pengelolaan dan pengamanan aset SPBE Kementerian;
   b. membuat perjanjian tertulis dengan pegawai yang terlibat dalam penggunaan dan/atau pengelolaan SPBE Kementerian yang memuat tanggung jawab terhadap keamanan SPBE dan sanksi atas pelanggaran keamanan SPBE;

c. menghentikan hak penggunaan aset SPBE Kementerian bagi pegawai yang sedang dalam pemeriksaan terkait dengan dugaan pelanggaran keamanan SPBE;
d. mencabut hak akses ke aset SPBE Kementerian yang dimiliki pegawai apabila yang bersangkutan sudah tidak memiliki kepentingan terhadap aset SPBE Kementerian, dimutasi, atau berhenti bekerja di lingkungan Kementerian;
e. membuat berita acara serah terima terkait pengembalian seluruh aset SPBE Kementerian yang digunakan selama bekerja bagi pegawai yang berhenti bekerja atau mutasi; dan
f. memberikan edukasi kesadaran keamanan SPBE melalui kegiatan sosialisasi, bimbingan teknis, dan pelatihan mengenai keamanan sistem informasi yang dilaksanakan secara berkala sesuai dengan tingkat tanggung jawabnya.

(3) Keamanan personil dilakukan oleh Koordinator SPBE Kementerian dan tim keamanan SPBE Kementerian.

Bagian Ketiga
Keamanan Aset

Pasal 7

(1) Keamanan aset sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b dilakukan untuk mengamankan aset SPBE Kementerian berdasarkan tingkat kekritisan.
(2) Tingkat kekritisan sebagaimana dimaksud pada ayat (1) terdiri atas:
a. sangat rahasia;
b. rahasia;
c. terbatas; dan
d. publik.

(3) Keamanan aset dilakukan dengan cara:

a. mengidentifikasi aset SPBE Kementerian dan mendokumentasikan ke dalam daftar inventaris aset SPBE Kementerian yang memuat tingkat kekritisan dan penanggung jawab setiap aset;

b. menetapkan pihak yang dapat mengakses aset SPBE Kementerian;

c. menetapkan aturan penggunaan aset SPBE Kementerian;

d. melakukan penilaian tingkat risiko (*risk register*) keamanan dan mengidentifikasi potensi ancaman dan kerentanan pada aset SPBE Kementerian;

e. menempatkan aset SPBE Kementerian di lokasi yang aman guna mengurangi risiko aset diakses oleh pihak yang tidak berwenang;

f. penggunaan aset SPBE Kementerian yang dibawa ke luar dari lingkungan pusat data atau tempat layanan SPBE Kementerian harus disetujui oleh pimpinan unit kerja;

g. perangkat penyimpanan data yang sudah tidak digunakan harus dilakukan sanitasi sebelum digunakan kembali atau dimusnahkan; dan

h. pemusnahan perangkat penyimpanan data harus dilakukan secara aman sesuai dengan prosedur pemusnahan perangkat penyimpanan.

(4) Keamanan aset sebagaimana dimaksud pada ayat (3) dilakukan oleh unit kerja.

Bagian Keempat

Keamanan Akses

Pasal 8

(1) Keamanan akses sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf c dilakukan untuk memastikan perangkat pengguna yang terhubung ke dalam SPBE Kementerian mendapatkan perlindungan keamanan dan tidak dapat diakses oleh pihak yang tidak berhak.

(2) Keamanan akses dilakukan dengan cara:

a. menyusun prosedur pengelolaan hak akses pengguna yang memuat ketentuan akses ke aset SPBE Kementerian sesuai dengan kebutuhan organisasi dan persyaratan keamanan;

b. mengelola akses pengguna dengan cara:

1. menggunakan akun yang unik untuk setiap pengguna;
2. memeriksa tingkat akses yang diberikan sesuai dengan tujuan penggunaan;
3. membatasi dan mengendalikan penggunaan hak akses khusus (jika ada);
4. mengatur pengelolaan kata sandi pengguna;
5. memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya;
6. memelihara catatan pengguna layanan (*user log*); dan
7. menonaktifkan akses pengguna yang telah berakhir penugasannya;

c. mengendalikan akses ke jaringan dan layanan jaringan SPBE dengan cara:

1. menerapkan prosedur otorisasi pemberian akses ke jaringan dan layanan jaringan untuk setiap akses ke dalam jaringan internal;
2. akses ke perangkat keras dan perangkat lunak yang digunakan untuk melakukan diagnosa harus dikontrol dan hanya digunakan untuk pegawai yang bertugas untuk melakukan pengujian, pemecahan masalah, serta pengembangan sistem;
3. memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi;
4. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu; dan

5. melakukan penghentian layanan jaringan pada area jaringan yang mengalami gangguan keamanan SPBE Kementerian;

d. mengendalikan akses ke aplikasi dan sistem informasi SPBE Kementerian dengan cara:
   1. akses terhadap aplikasi SPBE Kementerian hanya diberikan kepada pengguna sesuai dengan peruntukannya dan dikontrol dengan menggunakan sistem manajemen akses pengguna;
   2. setiap pengguna wajib memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya dan proses otorisasi pengguna wajib menggunakan teknik autentikasi yang sesuai untuk memvalidasi identitas pengguna;
   3. menggunakan sistem pengelolaan kata sandi yang dapat memastikan kualitas kata sandi yang dibuat pengguna;
   4. fasilitas masa waktu tenggang wajib diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu;
   5. membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi rahasia dan sangat rahasia; dan
   6. akses ke kode sumber aplikasi dibatasi secara ketat dan diperuntukkan hanya bagi pihak yang sah dan berkepentingan melalui hak akses khusus;

e. mengendalikan perangkat kerja jarak jauh sesuai dengan parameter keamanan yang harus dipenuhi oleh perangkat kerja jarak jauh yang digunakan dalam mengakses aset SPBE Kementerian, paling sedikit terdiri atas:
   1. jaringan pribadi maya (*Virtual Private Network*/ VPN);

2. sertifikat protokol kriptografi (*Secure Socket Layer*/SSL); dan/atau
3. autentikasi dua langkah *(Two Step Authentication)*;

f. hak akses khusus dapat dibuat untuk mengakses sistem informasi berklasifikasi rahasia pada sistem operasi, perangkat penyimpanan (*storage devices*), *file server*, dan aplikasi sensitif dengan cara:
1. mengidentifikasi hak akses khusus untuk dialokasikan kepada pengguna terkait;
2. memberikan hak akses khusus hanya kepada pengguna sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu;
3. mengelola proses otorisasi dan catatan dari seluruh hak akses khusus; dan
4. memberikan hak akses khusus secara terpisah dari akun yang digunakan untuk kegiatan umum;

g. melakukan pemantauan terhadap akses ke aset SPBE Kementerian meliputi:
1. kegagalan akses;
2. penggunaan hak akses tidak wajar;
3. alokasi dan penggunaan hak akses khusus;
4. penelusuran transaksi pengiriman *file* sistem atau dokumen tertentu yang mencurigakan; dan
5. penggunaan sumber daya sensitif; dan

h. menghapus akun setiap pegawai dan pihak ketiga yang tidak lagi memiliki kepentingan terhadap akses aset SPBE Kementerian.

(3) Keamanan akses sebagaimana dimaksud pada ayat (2) dilakukan oleh unit kerja.

Bagian Kelima
Keamanan Kriptografi

Pasal 9

(1) Keamanan kriptografi sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf d dilakukan untuk memastikan penggunaan kriptografi yang tepat untuk melindungi kerahasiaan, keutuhan, dan keotentikan data dan informasi rahasia dan/atau sangat rahasia yang dikelola dalam perangkat SPBE Kementerian.

(2) Keamanan kriptografi dilakukan dengan cara:
   a. melakukan klasifikasi informasi yang disimpan dan dikelola dalam perangkat SPBE sesuai dengan regulasi yang berlaku;
   b. menerapkan keamanan kriptografi untuk informasi berklasifikasi rahasia dan/atau sangat rahasia dengan cara:
      1. menerapkan jalur komunikasi aman dengan menerapkan sertifikat protokol kriptografi (*Secure Socket Layer*/SSL) untuk proses autentikasi antara pengguna dengan SPBE Kementerian berbasis *website*;
      2. menjaga kerahasiaan *password* dan menyimpannya dalam *database* SPBE Kementerian dengan mekanisme enkripsi (*hash function*);
      3. melindungi kerahasiaan data dan informasi rahasia dan/atau sangat rahasia dalam *database* SPBE Kementerian dengan mekanisme kriptografi simetrik;
      4. menerapkan autentikasi berbasis tanda tangan digital dengan menggunakan sertifikat elektronik yang dikeluarkan oleh pihak ketiga yang direkomendasikan oleh Pengelola SPBE Kementerian;

5. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan peraturan perundangan-undangan dan/atau rekomendasi lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber; dan
6. menetapkan standar penggunaan kriptografi sesuai dengan perkembangan teknologi.

(3) Keamanan kriptografi sebagaimana dimaksud pada ayat (2) dilakukan oleh unit kerja.

Bagian Keenam
Keamanan Fisik dan Lingkungan

Pasal 10

(1) Keamanan fisik dan lingkungan sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf e dilakukan untuk memberikan pelindungan, pemeliharaan, dan keamanan perangkat SPBE Kementerian.
(2) Keamanan fisik dan lingkungan dilakukan dengan cara:
    a. pemeliharaan perangkat SPBE Kementerian;
    b. pengamanan area;
    c. pelindungan terhadap ancaman eksternal dan lingkungan;
    d. penempatan dan perlindungan perangkat SPBE Kementerian; dan
    e. pengamanan kabel di pusat data dan/atau area kerja layanan SPBE Kementerian.
(3) Keamanan fisik dan lingkungan sebagaimana dimaksud pada ayat (2) dilakukan oleh unit kerja.

Pasal 11

Pemeliharaan perangkat SPBE Kementerian sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf a dilakukan dengan cara:

a. mencatat daftar perangkat yang digunakan untuk menjalankan SPBE Kementerian;
b. setiap perangkat yang digunakan untuk SPBE Kementerian dipelihara sesuai dengan buku petunjuk/ manual;
c. dalam hal pemeliharaan perangkat SPBE Kementerian tidak dapat dilakukan di tempat, maka pemindahan perangkat SPBE Kementerian dilakukan berdasarkan persetujuan Pengelola SPBE Kementerian;
d. dalam hal pemindahan perangkat SPBE Kementerian terdapat data dan/atau informasi berklasifikasi sangat rahasia dan rahasia yang tersimpan pada perangkat tersebut, maka data dan/atau informasi berklasifikasi sangat rahasia dan rahasia tersebut harus dipindahkan terlebih dahulu ke dalam media penyimpanan lain;
e. dalam hal pemeliharaan dilakukan oleh pihak ketiga, pelaksanaan pemeliharaan dilakukan dengan perjanjian kerja sama; dan
f. perjanjian kerja sama paling sedikit memuat pengaturan mengenai kerahasiaan, pemeliharaan yang disediakan, dan tingkat kinerja yang harus dipenuhi pihak ketiga.

Pasal 12

Pengamanan area sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf b dilakukan dengan cara:

a. menyimpan perangkat SPBE Kementerian di ruangan khusus yang dilindungi dengan pengamanan fisik paling sedikit meliputi:
    1. pintu dengan kontrol akses;
    2. kamera pengawas (*cctv*);
    3. pendeteksi asap (*smoke detector*);
    4. sistem pemadam kebakaran; dan
    5. perangkat pemutus aliran listrik;
b. akses ke pusat data dan/atau area kerja layanan SPBE Kementerian yang berisi data dan/atau informasi rahasia dan sangat rahasia harus dibatasi dan hanya diberikan kepada pegawai yang memiliki akses;

c. pihak ketiga yang memasuki pusat data dan/atau area kerja layanan SPBE Kementerian yang berisikan data dan/atau informasi rahasia dan sangat rahasia harus didampingi oleh pegawai yang ditugaskan sepanjang waktu kunjungan;
d. dilarang membawa dan/atau mengonsumsi makanan dan minuman di dalam ruang pusat data;
e. semua area yang digunakan untuk menyimpan aset data dan informasi penting merupakan area bebas dari asap;
f. menjaga batas minimum dan maksimum suhu dan kelembapan di dalam ruang pusat data sesuai dengan standar yang disyaratkan pabrikan perangkat;
g. pengamanan area pusat data dan area kerja layanan SPBE Kementerian dilakukan sesuai prosedur keamanan area; dan
h. pengamanan kantor, ruangan, dan fasilitas kerja sesuai dengan peraturan dan standar keamanan dan keselamatan kerja.

Pasal 13

Pelindungan terhadap ancaman eksternal dan lingkungan sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf c dilakukan dengan cara:

a. perangkat pemulihan dan media penyimpanan data cadangan wajib diletakkan di tempat yang aman dengan struktur yang memadai untuk menghindari kerusakan dari bencana;
b. semua perangkat SPBE Kementerian harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang disyaratkan oleh pabrikan perangkat;
c. pasokan listrik yang digunakan untuk mengoperasikan perangkat SPBE Kementerian harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan atau jangka waktu pengoperasian yang cukup, yang paling sedikit mencakup generator listrik dan suplai daya bebas gangguan (*Uniterruptable Power Supply*/UPS) dengan daya yang cukup dan dengan konfigurasi yang

dapat memindahkan pasokan listrik tanpa gangguan terhadap perangkat SPBE Kementerian;

d. bahan berbahaya atau mudah terbakar di lingkungan Kementerian wajib disimpan pada jarak yang aman dari pusat data dan area kerja layanan SPBE Kementerian; dan

e. perangkat pemadam kebakaran wajib disediakan dan diletakkan di tempat yang mudah dijangkau.

Pasal 14

Penempatan dan perlindungan perangkat SPBE Kementerian sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf d dilakukan dengan cara:

a. perangkat diletakkan pada lokasi yang meminimalisasi akses pihak yang tidak berwenang;

b. perangkat SPBE Kementerian yang menangani informasi sensitif diposisikan dan dibatasi sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak yang tidak berwenang;

c. perangkat SPBE Kementerian yang memerlukan perlindungan khusus wajib terisolasi;

d. kondisi lingkungan, seperti suhu dan kelembapan wajib dimonitor sesuai dengan kebutuhan;

e. perangkat SPBE Kementerian dilindungi dari kegagalan catu daya dan gangguan lain yang disebabkan kegagalan utilitas pendukung; dan

f. perlindungan petir wajib diterapkan untuk semua bangunan dan filter perlindungan petir dipasang untuk semua jalur komunikasi dan listrik.

Pasal 15

Pengamanan kabel di pusat data dan/atau area kerja layanan SPBE Kementerian sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf e dilakukan sesuai dengan standar elektrikal/ mekanikal pusat data yang berlaku.

Bagian Ketujuh
Keamanan operasional

Pasal 16

(1) Keamanan operasional sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf f dilakukan untuk:
    a. memastikan operasional yang aman dan benar pada aset SPBE Kementerian;
    b. mengimplementasikan dan memelihara keamanan aset SPBE Kementerian;
    c. mengelola layanan yang diberikan oleh pihak ketiga;
    d. meminimalkan risiko kegagalan; dan
    e. melindungi keutuhan dan ketersediaan aset SPBE Kementerian.
(2) Keamanan operasional dilakukan dengan cara melakukan pengendalian terhadap:
    a. penggunaan perangkat;
    b. perencanaan dan penerimaan sistem;
    c. program yang membahayakan;
    d. data cadangan; dan
    e. pencatatan.
(3) Keamanan operasional sebagaimana dimaksud pada ayat (2) dilakukan oleh unit kerja.

Pasal 17

Pengendalian terhadap penggunaan perangkat sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf a dilakukan dengan cara:

a. mendokumentasikan, memelihara, dan menyediakan prosedur penggunaan perangkat SPBE Kementerian sesuai dengan peruntukan;
b. melakukan pemisahan akses terhadap informasi yang memiliki klasifikasi rahasia dan sangat rahasia; dan

c. memisahkan perangkat pengembangan, pengujian, dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berhak terhadap sistem operasional.

Pasal 18

Pengendalian terhadap perencanaan dan penerimaan sistem sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf b dilakukan dengan cara:

a. memantau penggunaan perangkat SPBE Kementerian dan membuat perkiraan pertumbuhan kebutuhan ke depan untuk memastikan ketersediaan kapasitas; dan
b. menetapkan kriteria penerimaan untuk sistem informasi baru, pemutakhiran, dan versi baru serta melakukan pengujian sebelum penerimaan.

Pasal 19

Pengendalian terhadap program yang membahayakan sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf c dilakukan dengan cara:

a. menerapkan sistem pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan (*malware*);
b. memberikan pelindungan dengan menggunakan:
    1. perangkat perimeter keamanan jaringan (*firewall*);
    2. perangkat deteksi adanya penyusup (*Intrusion Prevention System*/IPS);
    3. perangkat antivirus;
    4. perangkat manajemen akses pengguna; dan
    5. perangkat pendukung lainnya sesuai perkembangan teknologi keamanan SPBE Kementerian; dan
c. melakukan penilaian kerentanan terhadap perangkat SPBE Kementerian (*vulnerability assessment*) dan uji coba kerentanan keamanan sistem (*penetration testing*) secara berkala dan melakukan tindakan perlindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi.

Pasal 20

Pengendalian terhadap data cadangan sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf d dilakukan dengan cara:

a. melakukan pembuatan data cadangan informasi dan perangkat lunak yang berada di pusat data dan/atau area kerja layanan SPBE Kementerian secara berkala;
b. mengambil dan menguji salinan cadangan data/ informasi, perangkat lunak, dan salinan lengkap sistem secara berkala; dan
c. memproses pembuatan data cadangan sesuai dengan prosedur pencadangan data.

Pasal 21

Pengendalian terhadap pencatatan sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf e dilakukan dengan cara:

a. mencatat setiap aktivitas administrator, aktivitas pengguna, peristiwa kegagalan, dan insiden keamanan serta disimpan dalam periode tertentu; dan
b. melindungi sistem pencatatan dari pemalsuan dan akses yang tidak berwenang.

Bagian Kedelapan
Keamanan komunikasi

Pasal 22

(1) Keamanan komunikasi sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf g dilakukan untuk memastikan keamanan pertukaran informasi melalui jaringan komunikasi.
(2) Keamanan komunikasi dilaksanakan dengan cara melakukan pengendalian terhadap:
    a. keamanan jaringan;
    b. pertukaran informasi; dan
    c. sistem pengolah informasi.
(3) Keamanan komunikasi sebagaimana dimaksud pada ayat (2) dilakukan oleh unit kerja.

Pasal 23

Pengamanan terhadap keamanan jaringan sebagaimana dimaksud dalam Pasal 22 ayat (2) huruf a dilakukan dengan cara:

a. unit kerja mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh pihak ketiga;
b. dalam hal pihak ketiga diizinkan mengakses ke jaringan, maka dilakukan pemantauan serta pencatatan kegiatan selama menggunakan jaringan; dan
c. melindungi jaringan dari pihak yang tidak berhak mengakses, dengan cara:
    1. mendokumentasikan arsitektur jaringan yang meliputi seluruh komponen perangkat keras dan perangkat lunak jaringan;
    2. menerapkan teknologi keamanan jaringan berbasis enkripsi dan autentikasi (termasuk sertifikat elektronik);
    3. menerapkan pemisahan jaringan untuk kelompok pengguna, layanan informasi, dan sistem informasi;
    4. menerapkan parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan; dan
    5. menerapkan prosedur penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.

Pasal 24

Pengamanan terhadap pertukaran informasi sebagaimana dimaksud dalam Pasal 22 ayat (2) huruf b dilakukan dengan cara:

a. informasi yang terdapat dalam layanan aplikasi SPBE yang melewati jaringan publik harus dilindungi dari upaya pengungkapan, modifikasi, dan perusakan dengan menerapkan mekanisme kriptografi;

b. melakukan pendeteksian dan perlindungan terhadap kode berbahaya (*malicious code*) yang disisipkan pada berkas (*file*) yang dikirim melalui sistem elektronik;
c. memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan untuk informasi elektronik berklasifikasi rahasia dan sangat rahasia; dan
d. menetapkan prosedur pertukaran informasi yang mengatur sistem dan keamanan yang digunakan untuk pertukaran informasi.

Pasal 25

Pengamanan terhadap sistem pengolah informasi sebagaimana dimaksud dalam Pasal 22 ayat (2) huruf c dilakukan dengan cara:

a. menerapkan pencatatan aktivitas pengguna dan kejadian keamanan SPBE dalam kurun waktu tertentu untuk membantu investigasi di masa mendatang (*audit logging*), antara lain:
    1. kegagalan akses;
    2. penggunaan hak akses tidak wajar;
    3. alokasi dan penggunaan hak akses khusus;
    4. penelusuran transaksi pengiriman berkas (*file*) sistem atau dokumen tertentu yang mencurigakan; dan
    5. penggunaan sumber daya sensitif.
b. menerapkan sistem pencatatan aktivitas administrator dan operator sistem;
c. menerapkan pencatatan kesalahan untuk dianalisis secara berkala dan diambil tindak pengamanan yang tepat; dan
d. memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.

Bagian Kesembilan
Keamanan Pengembangan dan Pemeliharaan

Pasal 26

(1) Keamanan pengembangan dan pemeliharaan sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf h dilakukan untuk memastikan bahwa keamanan SPBE Kementerian merupakan bagian yang terintegrasi dalam siklus hidup pengembangan dan pemeliharaan SPBE untuk mencegah terjadinya kesalahan, eksploitasi, modifikasi, dan perusakan SPBE oleh pihak yang tidak berwenang.
(2) Keamanan pengembangan dan pemeliharaan dilaksanakan dengan cara melakukan pengendalian terhadap:
    a. pemisahan perangkat pengembangan dan operasional SPBE Kementerian;
    b. penerapan standar keamanan yang relevan dalam proses pembangunan dan pengembangan SPBE Kementerian; dan
    c. uji kelaikan SPBE Kementerian.

Pasal 27

Pengendalian terhadap pemisahan perangkat pengembangan dan operasional SPBE Kementerian sebagaimana dimaksud dalam Pasal 26 ayat (2) huruf a dilakukan dengan cara:
a. memisahkan lingkungan pengembangan dan operasional aplikasi SPBE Kementerian baik secara fisik, nonfisik (*logic*), maupun aksesnya;
b. menjaga agar perangkat pengembangan tidak boleh diakses dari sistem operasional layanan;
c. mengupayakan lingkungan sistem pengujian sama dengan lingkungan sistem operasional layanan; dan
d. menjaga agar data yang memiliki klasifikasi rahasia dan sangat rahasia tidak boleh disalin ke dalam lingkungan sistem pengujian.

Pasal 28

Pengendalian terhadap penerapan standar keamanan yang relevan dalam proses pembangunan dan pengembangan SPBE Kementerian sebagaimana dimaksud dalam Pasal 26 ayat (2) huruf b dilakukan dengan cara:

a. memastikan bahwa dalam proses perencanaan dan pembangunan/pengembangan aplikasi dan infrastruktur SPBE Kementerian termasuk yang dilakukan oleh pihak ketiga telah memasukkan fitur-fitur keamanan dalam spesifikasi aplikasi dan infrastruktur SPBE yang dibangun/ dikembangkan;
b. fitur-fitur keamanan yang dimasukkan sesuai dengan standar keamanan yang relevan meliputi:
    1. standar keamanan data dan informasi;
    2. standar keamanan aplikasi;
    3. standar keamanan pusat data;
    4. standar keamanan sistem penghubung layanan; dan
    5. standar keamanan jaringan intra; dan
c. standar keamanan sebagaimana dimaksud dalam huruf b mengacu pada standar keamanan yang ditetapkan oleh lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

Pasal 29

Pengendalian terhadap uji kelaikan SPBE Kementerian sebagaimana dimaksud dalam Pasal 26 ayat (2) huruf c dilakukan dengan cara:

a. melaksanakan uji kelaikan SPBE Kementerian sebelum SPBE digunakan dan sewaktu-waku sesuai kebutuhan, yang mencakup aspek:
    1. uji fungsi, yaitu pengujian yang memastikan SPBE yang dibangun dan/atau dikembangkan telah memenuhi fungsi-fungsi sesuai dengan dokumentasi terkait;

2. uji integrasi, yaitu pengujian yang memastikan SPBE yang dibangun dan/atau dikembangkan telah memenuhi kebutuhan dan persyaratan integrasi dengan aplikasi, data, serta komponen-komponen lain yang terkait;
3. uji beban, yaitu pengujian yang memastikan SPBE yang dibangun dan/atau dikembangkan dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya; dan
4. uji keamanan, yaitu pengujian yang memastikan SPBE yang dibangun dan/atau dikembangkan dapat menjaga keamanan data dan informasi yang terkait dengannya; dan

b. mengevaluasi dan melaksanakan kembali uji kelaikan SPBE pada setiap perubahan besar (*major)* untuk menjamin keutuhan sistem tidak terganggu.

Bagian Kesepuluh
Keamanan Pihak Ketiga

Pasal 30

(1) Keamanan pihak ketiga sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf i dilakukan untuk memastikan pelindungan aset SPBE Kementerian dari akses oleh pihak ketiga.
(2) Keamanan pihak ketiga dilakukan dengan cara:
    a. melakukan pemeriksaan latar belakang pihak ketiga dengan tetap memperhatikan privasi dan perlindungan data pribadi;
    b. membuat perjanjian tertulis dengan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan SPBE Kementerian yang menyatakan tanggung jawab terhadap keamanan SPBE. Perjanjian tertulis dimaksud paling sedikit memuat:
        1. pelindungan atas informasi rahasia dan hak kekayaan intelektual setiap pihak;

2. dalam hal aset SPBE Kementerian disediakan oleh pihak ketiga, maka ada jaminan bahwa tidak terdapat kode berbahaya (*malicious code*) dan celah akses ilegal (*backdoor*);
3. hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia;
4. pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan;
5. syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian; dan
6. dalam hal pihak ketiga tidak lagi menjadi bagian dalam pengelolaan aset SPBE Kementerian, maka aset SPBE Kementerian harus dikembalikan ke unit kerja;

c. memastikan secara berkala bahwa pengendalian keamanan SPBE, definisi layanan, perubahan layanan, penggunaan alih daya (sub kontraktor), dan tingkat layanan telah diterapkan, dioperasikan, serta dipelihara oleh pihak ketiga;
d. melakukan pengaturan tingkat persetujuan layanan (*Service Level Agreement*/SLA) terkait penyelesaian insiden keamanan;
e. melakukan pemantauan terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh pihak ketiga secara berkala;
f. memperhatikan tingkat kekritisan, proses yang terkait dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan oleh pihak ketiga;
g. mencatat peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan;
h. memberikan informasi tentang gangguan keamanan dan mengkaji informasi bersama pihak ketiga;

i. mencabut hak akses terhadap informasi SPBE Kementerian yang dimiliki pihak ketiga apabila yang bersangkutan tidak lagi bekerja di Kementerian;
j. membuat berita acara serah terima terkait pengembalian seluruh aset SPBE Kementerian yang dipergunakan selama bekerja bagi pihak ketiga yang berakhir masa kontraknya; dan
k. memastikan pihak ketiga dan tamu yang memasuki lingkungan area pusat data dan tempat layanan SPBE Kementerian mematuhi standar keamanan fisik dan lingkungan.

(3) Keamanan pihak ketiga dilakukan sebagaimana dimaksud pada ayat (2) dilakukan oleh unit kerja.

Bagian Kesebelas
Manajemen Insiden Keamanan Siber

Pasal 31

(1) Manajemen insiden keamanan siber sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf j dilakukan untuk mengendalikan gangguan keamanan SPBE Kementerian.
(2) Insiden keamanan siber sebagaimana dimaksud pada ayat (1) meliputi:
a. penggantian tampilan laman (*web deface*);
b. program yang membahayakan (*malware, virus, worm, trojan,* dan *backdoor*);
c. program pemerasan (*ransomware*);
d. akses tidak berizin (*unauthorized access*);
e. kebocoran data (*data breach*);
f. penolakan layanan secara terdistribusi (*distributed denial of service*); dan
g. bentuk gangguan lainnya yang dapat mengganggu keamanan SPBE Kementerian.

(3) Manajemen insiden keamanan siber dilakukan dengan cara:

a. membentuk tim respon insiden keamanan siber (*Computer Security Incident Response Team/CSIRT*) yang bertugas melakukan pencegahan dan penanganan insiden keamanan siber yang terjadi di lingkungan Kementerian;

b. berkoordinasi dengan *EduCSIRT* di Pengelola SPBE Kementerian sebagai induk *CSIRT* Kementerian;

c. tim respon insiden keamanan siber melakukan tindakan pencegahan insiden keamanan siber yang meliputi:

1. melakukan uji coba kerentanan keamanan sistem (*penetration testing*) untuk menemukan kelemahan keamanan SPBE Kementerian dalam sistem SPBE Kementerian;
2. mengimplementasikan alat monitor keamanan berupa perangkat manajemen peristiwa dan keamanan informasi (*Security Information and Event Management*/SIEM); dan
3. melakukan pemantauan dan pendeteksian serangan terhadap sistem SPBE Kementerian;

d. Dalam hal terjadi insiden keamanan siber, tim respon insiden keamanan siber melaksanakan prosedur penanganan insiden keamanan siber yang meliputi:

1. menerima laporan dan mencatat insiden keamanan siber;
2. mengidentifikasi sumber serangan;
3. menganalisis informasi yang berkaitan dengan insiden keamanan siber;
4. memprioritaskan penanganan insiden berdasarkan tingkat dampak;
5. mengidentifikasi eskalasi penanganan insiden;
6. mendokumentasikan bukti insiden keamanan siber;
7. menyusun laporan penanganan insiden keamanan siber; dan

8. mengevaluasi dan memperbaiki standar, prosedur, dan kontrol keamanan SPBE Kementerian agar insiden keamanan siber serupa tidak terulang kembali;

e. menyusun berbagai macam skenario penanganan insiden keamanan siber;

f. melakukan simulasi skenario penanganan insiden keamanan siber yang telah disusun secara berkala;

g. memberikan pelatihan terhadap sumber daya manusia internal yang terlibat pada penanganan insiden sesuai skenario yang disusun;

h. menjalankan program kesadaran ancaman dan penanganan insiden serta berperan aktif pada seluruh karyawan; dan

i. melakukan pengukuran tingkat kematangan penanganan insiden secara berkala.

(4) Manajemen insiden keamanan siber sebagaimana dimaksud pada ayat (3) dilakukan oleh unit kerja.

Bagian Keduabelas

Manajemen Keberlangsungan Layanan SPBE Kementerian

Pasal 32

(1) Manajemen keberlangsungan layanan SPBE Kementerian sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf k dilakukan untuk menjamin ketersediaan layanan SPBE Kementerian pada saat terjadi keadaan darurat.

(2) Manajemen keberlangsungan layanan SPBE Kementerian dilakukan dengan cara:

a. melakukan identifikasi risiko pada keberlangsungan layanan SPBE Kementerian;

b. menyusun dan menerapkan rencana keberlangsungan layanan SPBE Kementerian (*Business Continuity Planning*) untuk menjaga dan mengembalikan operasional SPBE dalam jangka waktu yang disepakati dan tingkat keberlangsungan yang dibutuhkan;

c. rencana keberlangsungan layanan SPBE Kementerian paling sedikit meliputi:
   1. prosedur keberlangsungan layanan SPBE Kementerian pada saat keadaan darurat, manajemen risiko, analisis dampak kegiatan, pengembalian kondisi semula (*rollback*), peralihan kondisi normal, dan uji coba keberlangsungan kegiatan;
   2. penetapan peran dan tanggung jawab pegawai yang terlibat dalam pelaksanaan keberlangsungan layanan SPBE Kementerian; dan
   3. pelaksanaan sosialisasi dan pelatihan keberlangsungan layanan SPBE Kementerian;
d. memiliki redundansi yang cukup pada aplikasi umum dan/atau sistem elektronik kategori strategis kementerian untuk memenuhi ketersediaan layanan SPBE Kementerian;
e. melakukan uji coba rencana keberlangsungan layanan SPBE Kementerian secara berkala; dan
f. melaksanakan proses keberlangsungan layanan SPBE Kementerian pada saat keadaan darurat sesuai prosedur keberlangsungan layanan SPBE Kementerian.

(3) Manajemen keberlangsungan layanan SPBE Kementerian sebagaimana dimaksud pada ayat (2) dilakukan unit kerja.

Bagian Ketigabelas
Pengendalian Kepatuhan

Pasal 33

(1) Pengendalian kepatuhan sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf l dilakukan untuk memastikan kepatuhan pegawai dan pihak ketiga dalam melaksanakan keamanan SPBE Kementerian sesuai dengan ketentuan peraturan perundang-undangan.

(2) Pengendalian kepatuhan dilakukan dengan cara:
   a. mengidentifikasi, mendokumentasikan, dan memelihara regulasi terkait keamanan SPBE Kementerian;
   b. memeriksa kepatuhan seluruh pegawai dan pihak ketiga terhadap regulasi, standar, dan prosedur keamanan SPBE Kementerian;
   c. mendapatkan perangkat lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan tidak ada pelanggaran hak cipta;
   d. memeriksa kepatuhan penggunaan lisensi perangkat lunak dan menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;
   e. memelihara bukti kepemilikan lisensi, program induk sistem elektronik (*master disk*), buku manual, dan lain sebagainya; dan
   f. melakukan pemeriksaan bahwa tidak ada produk bajakan yang terinstal (pelanggaran hak kekayaan intelektual).

(3) Pengendalian kepatuhan sebagaimana dimaksud pada ayat (2) dilakukan tim keamanan SPBE Kementerian.

Bagian Keempatbelas
Audit Keamanan SPBE Kementerian

Pasal 34

(1) Audit Keamanan SPBE Kementerian sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf m dilakukan untuk memastikan kepatuhan pegawai dan pihak ketiga dalam melaksanakan keamanan SPBE Kementerian sesuai dengan ketentuan peraturan perundang-undangan.

(2) Audit keamanan SPBE Kementerian sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. audit internal keamanan SPBE Kementerian; dan
   b. audit eksternal keamanan SPBE Kementerian.

Pasal 35

(1) Audit internal keamanan SPBE Kementerian sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf a dilaksanakan dengan ketentuan sebagai berikut:
   a. audit internal keamanan SPBE Kementerian dilaksanakan oleh tim audit internal teknologi informasi dan komunikasi Kementerian yang diketuai oleh Pengelola SPBE Kementerian dan beranggotakan dari unsur pengawasan internal dan unit kerja terkait;
   b. tim audit internal teknologi informasi dan komunikasi Kementerian merencanakan, menetapkan, dan menjalankan program audit mencakup frekuensi, metode, kriteria, tanggung jawab, dan pelaporan audit;
   c. audit internal keamanan SPBE Kementerian dilaksanakan paling sedikit 1 (satu) kali tiap 2 (dua) tahun atau sewaktu-waktu sesuai penugasan Koordinator SPBE Kementerian;
   d. audit internal keamanan SPBE Kementerian dimasukkan dalam peta rencana SPBE Kementerian;
   e. audit internal keamanan SPBE Kementerian dilaksanakan oleh auditor yang memiliki kompetensi, objektifitas, dan ketidakberpihakan (imparsialitas) dalam melaksanakan audit internal keamanan SPBE Kementerian;
   f. setiap temuan audit harus dicatat secara formal oleh auditor dan diberikan kepada *auditee*;
   g. *auditee* harus melakukan perbaikan terhadap setiap temuan yang diberikan oleh auditor dalam jangka waktu yang disepakati;
   h. laporan audit internal keamanan SPBE Kementerian dilaporkan kepada Koordinator SPBE Kementerian sebagai bahan evaluasi penerapan kebijakan keamanan SPBE Kementerian; dan

i. audit internal keamanan SPBE Kementerian dilaksanakan sesuai dengan prosedur audit internal keamanan SPBE.

(2) Audit eksternal keamanan SPBE Kementerian sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf b dilaksanakan dengan ketentuan sebagai berikut:

a. audit eksternal keamanan SPBE Kementerian dilaksanakan oleh pihak ketiga yang berkompeten;

b. dalam hal SPBE merupakan aplikasi umum dan/atau sistem elektronik berkategori strategis maka audit eksternal keamanan SPBE Kementerian dilaksanakan paling sedikit 1 (satu) kali dalam 2 (dua) tahun oleh lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber;

c. dalam hal SPBE merupakan aplikasi khusus maka audit eksternal keamanan SPBE Kementerian dilaksanakan paling sedikit 1 (satu) kali dalam 2 (dua) tahun oleh lembaga audit teknologi informasi dan komunikasi yang teregistrasi pada lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber; dan

d. audit eksternal keamanan SPBE Kementerian dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

BAB IV
PENANGGUNG JAWAB DAN PELAKSANA SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 36

(1) Koordinator SPBE Kementerian bertanggung jawab atas pelaksanaan SMKI pada SPBE Kementerian.

(2) Dalam melaksanakan SMKI pada SPBE Kementerian, Koordinator SPBE Kementerian membentuk tim keamanan SPBE Kementerian.

(3) Tim keamanan SPBE Kementerian sebagaimana dimaksud pada ayat (2) diketuai oleh Pengelola SPBE Kementerian.

(4) Tim keamanan SPBE Kementerian sebagaimana dimaksud pada ayat (2) beranggotakan perwakilan unit kerja Kementerian.

(5) Tim keamanan SPBE Kementerian ditetapkan oleh Koordinator SPBE Kementerian.

BAB V
DUKUNGAN PENGOPERASIAN

Pasal 37

(1) Koordinator SPBE Kementerian memberikan dukungan pengoperasian keamanan informasi Kementerian dengan menyediakan:
   a. sumber daya manusia keamanan informasi Kementerian; dan
   b. anggaran keamanan SPBE Kementerian.

(2) Sumber daya manusia keamanan informasi Kementerian sebagaimana dimaksud pada ayat (1) huruf a harus memiliki kompetensi di bidang:
   a. keamanan infrastruktur teknologi informasi dan komunikasi;
   b. keamanan aplikasi; dan
   c. keamanan data dan informasi.

(3) Koordinator SPBE Kementerian memfasilitasi peningkatan kompetensi sumber daya manusia keamanan informasi Kementerian melalui kegiatan pelatihan dan/atau bimbingan teknis.

(4) Anggaran keamanan SPBE Kementerian sebagaimana dimaksud pada ayat (1) huruf b berdasarkan peta rencana keamanan SPBE Kementerian.

BAB VI

EVALUASI KINERJA

Pasal 38

(1) Koordinator SPBE Kementerian melakukan evaluasi kinerja terhadap pelaksanaan keamanan SPBE Kementerian.

(2) Evaluasi kinerja terhadap pelaksanaan keamanan SPBE Kementerian sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

(3) Evaluasi kinerja terhadap pelaksanaan keamanan SPBE Kementerian berdasarkan peta rencana keamanan SPBE Kementerian dengan cara:
   a. mengidentifikasi kegiatan yang memiliki risiko tinggi terhadap keberhasilannya;
   b. menetapkan sasaran dan indikator kinerja pada setiap kegiatan;
   c. mengukur capaian kinerja dan efektifitas penerapan keamanan SPBE Kementerian;
   d. mendukung dan merealisasikan kegiatan audit keamanan SPBE Kementerian sebagai bagian dari evaluasi penerapan keamanan SPBE Kementerian; dan
   e. melakukan langkah-langkah perbaikan untuk mencapai target indikator kinerja dan memperbaiki hasil temuan audit.

(4) Dalam melaksanakan evaluasi kinerja terhadap pelaksanaan keamanan SPBE Kementerian sebagaimana dimaksud pada ayat (3), Koordinator SPBE Kementerian dibantu oleh tim keamanan SPBE Kementerian.

(5) Hasil evaluasi kinerja terhadap pelaksanaan keamanan SPBE Kementerian menjadi dasar bagi unit kerja dalam melakukan perbaikan berkelanjutan keamanan SPBE Kementerian.

BAB VII

PERBAIKAN BERKELANJUTAN

Pasal 39

(1) Perbaikan berkelanjutan keamanan SPBE Kementerian sebagaimana dimaksud dalam Pasal 38 ayat (5) dilaksanakan oleh unit kerja di bawah koordinasi Pengelola SPBE Kementerian.

(2) Perbaikan berkelanjutan keamanan SPBE Kementerian dilakukan dengan:
    a. mengatasi permasalahan dalam keamanan SPBE Kementerian; dan
    b. memperbaiki keamanan SPBE Kementerian secara periodik.

BAB VIII

KETENTUAN PENUTUP

Pasal 40

Peraturan Sekretaris Jenderal ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 15 Juli 2022

SEKRETARIS JENDERAL,

TTD.

SUHARTI

Salinan sesuai dengan aslinya,
Kepala Biro Hukum
Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi,

TTD.

Dian Wahyuni
NIP 196210221988032001