PERATURAN DIREKTUR UTAMA
LEMBAGA PENYIARAN PUBLIK RADIO REPUBLIK INDONESIA

NOMOR 03 TAHUN 2026

TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN LEMBAGA PENYIARAN PUBLIK
RADIO REPUBLIK INDONESIA

DENGAN RAHMAT TUHAN YANG MAHA ESA

DIREKTUR UTAMA
LEMBAGA PENYIARAN PUBLIK RADIO REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk melindungi kerahasiaan, integritas, dan ketersediaan Aset Informasi Lembaga Penyiaran Publik Radio Republik Indonesia dari berbagai bentuk ancaman Keamanan Informasi, perlu mengatur pengelolaan Keamanan Informasi di lingkungan Lembaga Penyiaran Publik Radio Republik Indonesia;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Direktur Utama Lembaga Penyiaran Publik Radio Republik Indonesia tentang Sistem Manajemen Keamanan Informasi di Lingkungan Lembaga Penyiaran Publik Radio Republik Indonesia;

Mengingat : 1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);

2. Peraturan Pemerintah Nomor 12 Tahun 2005 tentang Lembaga Penyiaran Publik Radio Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2005 Nomor 29, Tambahan Lembaran Negara Republik Indonesia Nomor 4486) sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 3 Tahun 2024 tentang Perubahan atas Peraturan Pemerintah Nomor 12 Tahun 2005 tentang Lembaga Penyiaran Publik Radio Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 7, Tambahan Lembaran Negara Republik Indonesia Nomor 6908);

3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik

Indonesia...

Indonesia Nomor 6400);

4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

5. 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;

6. Peraturan Dewan Direksi Lembaga Penyiaran Publik Radio Republik Indonesia Nomor 07 Tahun 2021 tentang Organisasi dan Tata Kerja Lembaga Penyiaran Publik Radio Republik Indonesia sebagaimana telah diubah sebagian dengan Peraturan Dewan Direksi Lembaga Penyiaran Publik Radio Republik Indonesia Nomor 2 Tahun 2024 tentang Perubahan Atas Peraturan Dewan Direksi Nomor 07 Tahun 2021 tentang Organisasi dan Tata Kerja Lembaga Penyiaran Publik Radio Republik Indonesia.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Direktur Utama ini yang dimaksud dengan:

1. Lembaga Penyiaran Publik Radio Republik Indonesia yang selanjutnya disebut RRI adalah Lembaga Penyiaran Publik yang menyelenggarakan kegiatan penyiaran radio, dengan menggunakan spektrum frekuensi radio melalui udara,kabel, dan/atau media lainya.

2. Informasi adalah satu atau sekumpulan data, termasuk tapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik, (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

3. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) Informasi.

4. Aset Informasi adalah segala sesuatu yang dapat memberikan nilai tambah bagi RRI dalam menunjang proses bisnis dan perlu dilindungi dari berbagai ancaman Keamanan Informasi.

5. Kriptografi adalah disiplin ilmu yang meliputi prinsip, sarana dan metode untuk menyediakan keamanan informasi, termasuk kerahasiaan, integritas data, autentikasi dan nir-penyangkalan.

6. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi.

sistem…

7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.

8. Infrastruktur SPBE adalah semua perangkat keras,perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung,dan perangkat elektronik lainnya.

9. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik.

10. Pihak Ketiga adalah Kementerian/Lembaga, penyedia barang dan/atau jasa yang menjadi mitra kerja RRI.

11. 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 menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan Keamanan Informasi.

12. *Chief Information Officer* yang selanjutnya disingkat CIO adalah pejabat pengarah informasi yang dijabat oleh Direktur Teknologi dan Media Baru sebagai koordinator penyelenggaraan tata kelola teknologi di lingkungan RRI.

13. *Chief Information Security Officer* yang selanjutnya disingkat CISO adalah pejabat yang berperan sebagai koordinator dalam pelaksanaan implementasi kebijakan dan standar SMKI di lingkungan RRI.

14. Tim Tanggap Insiden Siber yang selanjutnya disebut RRI-CSIRT adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.

15. Aplikasi adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan.

16. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja dari layanan Sistem Elektronik.

17. Pusat Data adalah fasilitas fisik yang digunakan untuk menyimpan sistem komputer dan komponen-komponen terkait seperti sistem telekomunikasi dan penyimpanan data.

18. Audit Keamanan Informasi adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi Informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi

dengan...

dengan kriteria dan/atau standar yang telah ditetapkan terhadap beroperasinya Keamanan Informasi.

19. Auditor Keamanan Informasi adalah yang selanjutnya disebut Auditor adalah orang yang memiliki kompetensi untuk melakukan Audit Keamanan Informasi.

BAB II
RUANG LINGKUP

Pasal 2

(1) Peraturan Direktur Utama ini mengatur kebijakan dan standar SMKI yang digunakan sebagai pedoman pelindungan keamanan Aset Informasi milik RRI.

(2) Aset Informasi milik RRI sebagaimana dimaksud pada ayat (1) terdiri dari Aset Informasi pada SPBE RRI dalam bentuk:
   a. data dan Informasi, meliputi data siaran, data gaji, data kepegawaian, kontrak, perjanjian kerahasiaan, kebijakan RRI, hasil penelitian, prosedur operasional, serta data dan Informasi lainnya terkait kelangsungan layanan SPBE RRI;
   b. Aplikasi;
   c. Infrastruktur SPBE; dan
   d. sumber daya manusia.

BAB III
PELAKSANA SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 3

(1) Pengelolaan keamanan informasi yang diatur dalam Peraturan Direktur Utama ini, dilaksanakan oleh pegawai di lingkungan RRI dan Pihak Ketiga.

(2) Pengelolaan sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Direktur Teknologi dan Media Baru selaku CIO dan sekaligus CISO.

(3) CISO sebagaimana dimaksud pada ayat (2) dalam melaksanakan tugasnya membentuk dan menetapkan Tim Keamanan Informasi, termasuk RRI-CSIRT.

BAB IV
PELAKSANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 4

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

SMKI…

(2) SMKI pada SPBE RRI sebagaimana dimaksud pada ayat (1) terdiri atas:
a. pengendalian keamanan sumber daya manusia;
b. pengendalian keamanan Aset Informasi;
c. pengendalian keamanan akses;
d. pengendalian keamanan fisik dan lingkungan;
e. pengendalian keamanan operasional;
f. pengendalian keamanan komunikasi;
g. pengendalian keamanan pengembangan dan pemeliharan;
h. pengendalian Pihak Ketiga;
i. pengendalian Kriptografi;
j. pengendalian keamanan Insiden Siber;
k. pengendalian kelangsungan layanan informasi; dan
l. pengendalian kepatuhan.

Bagian Kedua
Pengendalian Keamanan Sumber Daya Manusia

Pasal 5

(1) Pengendalian keamanan sumber daya manusia sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf a, dilakukan untuk mengendalikan pegawai dan Pihak Ketiga dalam melaksanakan kebijakan SMKI.

(2) Keamanan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan dengan cara:
a. mengomunikasikan peran dan tanggung jawab pelaksanaan kebijakan Keamanan Informasi dalam SPBE RRI kepada seluruh pegawai yang terlibat dalam pengelolaan dan pengamanan Aset Informasi;
b. melakukan pembagian tugas dan wewenang (*segregation of duty)* untuk menghindari kesalahan atau pelanggaran;
c. melakukan pemeriksaan data pribadi pegawai dan Pihak Ketiga yang terlibat dalam pengelolaan dan pengamanan Aset Informasi dan/atau SPBE RRI;
d. membuat perjanjian tertulis dengan pegawai dan Pihak Ketiga yang terlibat dalam penggunaan dan/atau pengelolaan SPBE RRI yang memuat tanggung jawab terhadap Keamanan Informasi dan/atau SPBE dan sanksi atas pelanggaran keamanan SPBE RRI dan/atau Keamanan Informasi;
e. menghentikan hak penggunaan Aset Informasi dan/atau SPBE RRI bagi pegawai yang sedang dalam pemeriksaan terkait dengan dugaan pelanggaranan Keamanan Informasi;
f. mencabut hak akses atas Aset Informasi dan/atau SPBE RRI yang dimiliki pegawai apabila yang bersangkutan sudah tidak memiliki kepentingan terhadap Aset Informasi dan/atau SPBE RRI, dimutasi, atau berhenti bekerja di lingkungan RRI;
g. membuat berita acara serah terima terkait pengembalian atau penerimaan Aset Informasi dan/atau SPBE RRI yang digunakan selama bekerja bagi pegawai yang berhenti bekerja atau mutasi;
h. memberikan edukasi kesadaran Keamanan Informasi

dan/atau...

dan/atau keamanan SPBE RRI melalui kegiatan sosialisasi, bimbingan teknis, dan/atau pelatihan mengenai Keamanan Informasi SPBE yang dilaksanakan secara berkala; dan

i. memelihara catatan pelatihan, kompetensi, pengamanan, dan kualifikasi pegawai yang mengelola Keamanan Informasi dan/atau SPBE RRI.

Bagian Ketiga
Pengendalian Keamanan Aset Informasi

Pasal 6

(1) Pengendalian keamanan Aset Informasi sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf b dilakukan untuk mengamankan Aset Informasi pada SPBE RRI berdasarkan tingkat kekritisan data.

(2) Tingkat kekritisan data sebagaimana dimaksud pada ayat (1) terdiri atas:
a. Sangat Rahasia;
b. Rahasia dan/atau Terbatas; dan
c. Biasa.

(3) Keamanan Aset Informasi dilakukan dengan cara:
a. mengidentifikasi Aset Informasi dan/atau Informasi pada SPBE RRI dan mendokumentasikan ke dalam daftar inventaris Aset Informasi yang memuat tingkat kekritisan data dan penanggung jawab setiap Aset Informasi;
b. menetapkan pihak-pihak yang dapat mengakses Aset Informasi;
c. menyusun dan menetapkan aturan dan/atau prosedur penggunaan Aset Informasi;
d. melakukan penilaian tingkat Risiko (*risk register*) Keamanan Informasi dan mengidentifikasi potensi ancaman dan kerentanan pada Aset Informasi;
e. menempatkan Aset Informasi di lokasi yang aman guna mengurangi Risiko Aset Informasi dapat diakses oleh pihak yang tidak berwenang;
f. penggunaan Aset Informasi yang dibawa ke luar dari lingkungan Pusat Data atau tempat layanan SPBE RRI harus disetujui oleh Direktur Teknologi dan Media Baru;
g. melakukan sanitasi terhadap perangkat penyimpanan data yang sudah tidak digunakan lagi sebelum digunakan kembali atau dimusnahkan;
h. melakukan pemusnahan perangkat penyimpanan data secara aman sesuai prosedur pemusnahan perangkat penyimpanan; dan
i. melaksanakan manajemen aset Teknologi Informasi dan Komunikasi sesuai dengan ketentuan manajemen aset Teknologi Informasi dan Komunikasi yang ditetapkan oleh kementerian yang melaksanakan tugas di bidang komunikasi dan informatika.

(4) Keamanan Aset Informasi sebagaimana dimaksud pada ayat (3) diatur dalam prosedur yang berlaku di lingkungan RRI.

bagian...

Bagian Keempat
Pengendalian Keamanan Akses

Paragraf 1
Umum

Pasal 7

(1) Pengendalian keamanan akses sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf c dilakukan untuk memastikan perangkat pegawai dan Pihak Ketiga yang terhubung ke dalam SPBE RRI dan/atau Aset Informasi mendapatkan perlindungan keamanan dan tidak dapat diakses oleh pihak yang tidak berhak.

(2) Keamanan akses sebagaimana dimaksud pada ayat (1) dilakukan dengan cara:
   a. menyusun prosedur pengelolaan hak akses pegawai dan Pihak Ketiga yang berisi ketentuan akses ke Aset Informasi dan/atau SPBE RRI sesuai dengan kebutuhan organisasi, persyaratan keamanan, dan peraturan yang berlaku;
   b. mengelola akses pegawai dan Pihak Ketiga;
   c. mengendalikan akses ke jaringan dan layanan jaringan Informasi;
   d. mengendalikan akses ke Aplikasi dan sistem informasi;
   e. mengendalikan perangkat kerja jarak jauh;
   f. melakukan pemantauan terhadap akses ke Aset Informasi dan/atau SPBE RRI; dan
   g. menghapus akun setiap pegawai dan Pihak Ketiga yang tidak lagi berkepentingan terhadap akses Aset Informasi dan/atau SPBE RRI.

(3) Pengelolaan akses pegawai dan Pihak Ketiga sebagaimana dimaksud pada ayat (2) huruf b dilakukan dengan cara:
   a. menggunakan akun yang unik untuk setiap pegawai dan Pihak Ketiga;
   b. memeriksa tingkat akses yang diberikan sesuai dengan tujuan pegawai dan Pihak Ketiga;
   c. membatasi dan mengendalikan penggunaan hak akses khusus jika diperlukan;
   d. mengatur pengelolaan kata sandi pegawai dan Pihak Ketiga sesuai dengan ketentuan pengelolaan kata sandi di RRI;
   e. memantau dan mengevaluasi hak akses pegawai dan Pihak Ketiga dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya;
   f. memelihara catatan pengguna layanan (*user log)*;
   g. menonaktifkan akses pegawai dan Pihak Ketiga yang telah berakhir penugasannya; dan
   h. memantau dan mengevaluasi akun dan hak akses secara berkala paling sedikit 1 (satu) kali dalam 6 (enam) bulan.

(4) Pengendalian akses ke jaringan dan layanan jaringan Informasi sebagaimana dimaksud pada ayat (2) huruf c dilakukan dengan cara:
   a. menerapkan prosedur otorisasi pemberian akses ke jaringan dan layanan jaringan untuk setiap akses ke dalam jaringan internal;

b. akses...

b. akses ke Infrastruktur SPBE dan Aplikasi yang digunakan hanya untuk melakukan diagnosa harus dikontrol dan hanya digunakan untuk pegawai bertugas dalam rangka pengujian, pemecahan masalah, serta pengembangan sistem informasi;
c. memisahkan jaringan untuk pegawai dan Pihak Ketiga, sistem informasi, dan layanan Informasi;
d. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu; dan
e. melakukan penghentian layanan jaringan yang mengalami gangguan Keamanan Informasi.

(5) Pengendalian akses ke Aplikasi dan Sistem Informasi sebagaimana dimaksud pada ayat (2) huruf d dilakukan dengan cara:
a. akses terhadap Aplikasi SPBE RRI hanya diberikan kepada pegawai dan Pihak Ketiga sesuai dengan peruntukannya dan dikontrol dengan menggunakan sistem manajemen akses;
b. setiap pegawai dan Pihak Ketiga wajib memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya dan proses otorisasi pegawai dan Pihak Ketiga wajib menggunakan teknis autentikasi yang sesuai untuk memvalidasi identitas;
c. menggunakan sistem pengelolaan kata sandi yang dapat memastikan kualitas kata sandi yang dibuat pegawai dan Pihak Ketiga;
d. fasilitas masa waktu tenggang (*session time-out)* wajib diaktifkan untuk menutup dan mengunci layar komputer, Aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pegawai dan Pihak Ketiga setelah periode tertentu;
e. membatasi waktu koneksi untuk sistem informasi dan Aplikasi yang memiliki klasifikasi rahasia dan sangat rahasia; dan
f. akses ke kode sumber Aplikasi dibatasi secara ketat dan diperuntukkan hanya bagi pihak yang sah dan berkepentingan melalui hak akses khusus.

(6) Pengendalian perangkat kerja jarak jauh sebagaimana dimaksud pada ayat (2) huruf e dilakukan dengan cara menentukan parameter keamanan yang harus dipenuhi oleh perangkat kerja jarak jauh yang digunakan dalam mengakses Aset Informasi, yang terdiri dari:
a. jaringan pribadi maya (*Virtual Private Network/*VPN);
b. sertifikat protokol kriptografi (*Secure Socket Layer/*SSL); dan/atau
c. autentikasi dua langkah (*Two Step Authentication).*

(7) Pemantauan terhadap akses ke Aset Informasi dan/atau SPBE RRI sebagaimana dimaksud pada ayat (2) huruf f meliputi:
a. kegagalan akses;
b. penggunaan hak akses tidak wajar;
c. alokasi dan penggunaan hak akses khusus;
d. penelusuran transaksi pengiriman *file* sistem atau dokumen tertentu yang mencurigakan; dan
e. penggunaan sumber daya sensitif.

paragraf...

Paragraf 2
Hak Akses Khusus

Pasal 8

(1) Penggunaan hak akses khusus sebagaimana dimaksud dalam Pasal 3 ayat (3) huruf c diperlukan dalam hal adanya akses ke Aset Informasi yang bersifat rahasia pada sistem operasi, perangkat penyimpanan (*storage devices), file server,* dan Aplikasi sensitif.

(2) Pemberian hak akses khusus sebagaimana dimaksud pada ayat (1) dilakukan dengan cara:
   a. mengidentifikasi hak akses khusus untuk dialokasi kepada pegawai dan Pihak Ketiga terkait;
   b. memberikan hak akses khusus hanya kepada pegawai dan Pihak Ketiga sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu;
   c. mengelola proses otorisasi dan catatan dari seluruh hak akses khusus; dan
   d. memberikan hak akses khusus secara terpisah dari akun yang digunakan untuk kegiatan umum.

Paragraf 3
Pengelolaan Kata Sandi

Pasal 9

Pengelolaan kata sandi sebagaimana dimaksud dalam Pasal 3 ayat (3) huruf d dilakukan dengan cara:
a. menjaga kerahasian kata sandi dan menghindari menyimpan catatan kata sandi*;*
b. mengganti kata sandi apabila terdapat indikasi sistem dan kata sandi mengalami penyalahgunaan atau kebocoran;
c. menggunakan kata sandi yang berkualitas meliputi:
   1. panjang minimal 8 (delapan) karakter;
   2. menggunakan kombinasi huruf besar dan kecil dan angka, atau huruf besar dan kecil, angka, dan/atau simbol khusus; dan
   3. untuk Sistem Elektronik yang tidak dimungkinkan untuk mengikuti penggunaan kata sandi yang berkualitas wajib mendapatkan persetujuan ketua tim kerja yang mempunyai tugas dan fungsi di bidang teknologi dan media baru dengan mempertimbangkan kendala dan risiko yang ada.
d. kata sandi tidak boleh sama dengan *User ID* dan tidak berdasar pada sesuatu yang mudah ditebak, seperti nama, nomor telepon, tanggal lahir, nama anggota keluarga, dan/atau nama atau identitas perusahaan atau instansi;
e. mengganti kata sandi secara berkala selama 3 (tiga) bulan dengan menghindari penggunaan kata sandi yang pernah digunakan;
f. setiap pegawai dan Pihak Ketiga wajib menjaga kerahasiaan kata sandi dan tidak diperbolehkan memberikan kata sandi kepada orang lain dan/atau menggunakan kata sandi milik orang lain; dan
g. dalam 3 (tiga) bulan, setiap pegawai dan Pihak Ketiga wajib

melakukan…

melakukan akses minimal 1 (satu) kali agar akses pegawai dan Pihak Ketiga tersebut tidak dinonaktifkan.

Bagian Kelima
Pengendalian Keamanan Fisik dan Lingkungan

Pasal 10

(1) Pengendalian keamanan fisik dan lingkungan sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf d, dilakukan untuk memberikan pelindungan, pemeliharaan, keamanan, dan ketersediaan Aset Informasi yang terdiri dari:
a. area yang aman; dan
b. pengamanan Infrastruktur SPBE.

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

(3) Pengamanan Infrastruktur SPBE sebagaimana dimaksud pada ayat (1) huruf b dilaksanakan ketentuan:
a. menempatkan dan melindungi Infrastruktur SPBE RRI dari ancaman dan bahaya lingkungan, serta akses tidak sah;
b. melindungi Infrastruktur SPBE dari kegagalan catu daya (*power supply)* dan gangguan lain yang disebabkan oleh kegagalan perangkat pendukung;
c. melindungi kabel daya dan telekomunikasi yang membawa Data dan Informasi dari intersepsi, interferensi, dan/atau kerusakan;
d. memelihara Infrastruktur SPBE untuk menjamin keutuhan dan ketersediaan Infrastruktur SPBE dan/atau Aset Informasi;
e. menghapus data yang sudah tidak dipergunakan dalam penyimpanan data secara permanen sebelum digunakan kembali, dihapus, atau dimusnahkan;
f. penggunaan Aset Informasi yang dibawa ke luar dari lingkungan RRI harus disetujui oleh Direktur Teknologi dan Media Baru; dan
g. menerapkan aturan bagi pegawai dan Pihak Ketiga yang meninggalkan area kerja agar membersihkan media yang menampilkan Informasi bersifat rahasia dan sangat rahasia.

(4) dalam…

(4) Dalam hal Aset Informasi dibawa ke luar dari lingkungan RRI sebagaimana dimaksud pada ayat (3) huruf f, pegawai dan Pihak Ketiga harus memastikan Aset Informasi memiliki pelindungan keamanan yang tepat.

Bagian Keenam
Pengendalian Keamanan Operasional

Pasal 11

(1) Pengendalian keamanan operasional sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf e dilakukan untuk:
   a. memastikan operasional yang aman dan benar pada Aset Informasi;
   b. mengimplementasikan dan memelihara keamanan Aset Informasi;
   c. mengelola layanan yang diberikan oleh Pihak Ketiga; dan
   d. meminimalkan Risiko; dan
   e. melindungi keutuhan dan ketersediaan Aset Informasi.

(2) Pengendalian keamanan operasional sebagaimana dimaksud pada ayat (1) terdiri dari:
   a. pengendalian penggunaan Infrastruktur SPBE;
   b. pengendalian perencanaan dan penerimaan sistem informasi;
   c. pengendalian program yang membahayakan;
   d. pengendalian data cadangan; dan
   e. pengendalian pencatatan (*log)*.

Pasal 12

(1) Pengendalian terhadap penggunaan Infrastruktur SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a dilakukan dengan cara:
   a. mendokumentasikan, memelihara, dan menyediakan prosedur penggunaan Infrastruktur SPBE 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 berwenang terhadap Aset Informasi dan/atau SPBE RRI.

Pasal 13

Pengendalian terhadap perencanaan dan penerimaan sistem informasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b dilakukan dengan cara:
a. memantau penggunaan Infrastruktur SPBE dan membuat perkiraan pertumbuhan kebutuhan ke depan untuk

memastikan...

memastikan ketersediaan kapasitas; dan
b. menetapkan kriteria penerimaan untuk sistem informasi yang baru, pemutakhiran, dan versi baru serta melakukan pengujian sebelum penerimaan.

Pasal 14

Pengendalian terhadap program yang membahayakan sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c dilakukan dengan cara:
a. menerapkan sistem pendeteksian, pencegahan, dan pemulihan sebagai bentuk pelindungan terhadap ancaman program yang membahayakan (*malware)*;
b. memberikan pelindungan dengan menggunakan:
   1. perangkat parameter keamanan jaringan (*firewall)*;
   2. perangkat deteksi adanya penyusup (*Intrusion Prevention System/IPS*);
   3. perangkat antivirus;
   4. perangkat manajemen akses;
   5. perangkat pendukung lainnya sesuai dengan perkembangan teknologi keamanan SPBE; dan
c. melakukan penilaian kerentanan terhadap Infrastruktur SPBE (*vulnerability assessment)* dan uji coba kerentanan keamanan Sistem Informasi (*penetration testing)* secara berkala dan melakukan tindakan pelindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi.

Pasal 15

Pengendalian terhadap data cadangan sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf d dilakukan dengan cara:
a. melakukan pembuatan data cadangan Informasi dan Infrastruktur SPBE yang berada di Pusat Data dan/atau area kerja layanan SPBE RRI secara berkala;
b. mengambil dan menguji salinan cadangan data atau Informasi, Infrastruktur SPBE, dan salinan lengkap sistem informasi secara berkala; dan
c. memproses pembuatan data cadang Informasi... prosedur pencadangan data.

Pasal 16

(1) Pengendalian terhadap pencatatan sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf e dilakukan dengan cara:
   a. mencatat *(logging)* setiap aktivitas administrator, aktivitas pengguna, peristiwa kegagalan, dan kejadian keamanan serta disimpan dalam periode tertentu;
   b. menerapkan audit terhadap *log* yang mencatat aktivitas pengguna dan kejadian Keamanan Informasi dalam kurun waktu tertentu untuk membantu investigasi di masa mendatang; dan
   c. melindungi sistem pencatatan dari pemalsuan dan akses yang tidak berwenang.

(2) Penerapan audit terhadap *log* sebagaimana dimaksud pada ayat (1) huruf b untuk mengetahui:
   a. kegagalan akses;
   b. penggunaan hak akses tidak wajar;
   c. alokasi dan penggunaan hak akses khusus;
   d. penelusuran transaksi pengiriman berkas (*file)* sistem informasi atau dokumen tertentu yang mencurigakan; dan
   e. penggunaan sumber daya sensitif.

Bagian Ketujuh
Pengendalian Keamanan Komunikasi

Pasal 17

(1) Pengendalian keamanan komunikasi sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf f dilakukan untuk memastikan keamanan pertukaran Informasi melalui jaringan komunikasi.

(2) Pengendalian keamanan komunikasi sebagaimana dimaksud pada ayat (1) dilaksanakan dengan:
   a. pengendalian keamanan jaringan;
   b. pengendalian pertukaran Informasi; dan
   c. pengendalian Infrastruktur SPBE.

Pasal 18

Pengamanan terhadap keamanan jaringan sebagaimana dimaksud dalam Pasal 17 ayat (2) huruf a dilakukan dengan cara:
a. 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...

Pasal 19

Pengamanan terhadap pertukaran Informasi sebagaimana dimaksud dalam Pasal 17 ayat (2) huruf b dilakukan dengan cara:

a. Informasi yang terdapat dalam layanan Aplikasi SPBE RRI 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 berklasifikasi rahasia dan sangat rahasia; dan
d. menetapkan prosedur pertukaran Informasi yang mengatur sistem informasi dan keamanan yang digunakan untuk pertukaran Informasi.

Pasal 20

Pengamanan terhadap Infrastruktur SPBE sebagaimana dimaksud dalam Pasal 17 ayat (2) huruf c dilakukan dengan cara:

a. menerapkan pencatatan aktivitas Pengguna dan kejadian keamanan SPBE RRI 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 Kedelapan
Pengendalian Keamanan Pengembangan dan Pemeliharaan

Pasal 21

(1) Pengendalian keamanan pengembangan dan pemeliharaan sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf g dilakukan untuk memastikan Keamanan Informasi merupakan bagian yang terintegrasi dalam siklus pengelolaan Aset Informasi guna mencegah terjadinya kesalahan, eksploitasi, modifikasi, dan perusakan Aset Informasi oleh pihak yang tidak berwenang.

(2) pengendalian…

(2) Pengendalian keamanan pengembangan dan pemeliharaan sebagaimana dimaksud pada ayat (1) dilakukan dengan ketentuan:
   a. pemisahan perangkat pengembangan dan operasional SPBE;
   b. penerapan standar keamanan yang relevan dalam proses pembangunan dan pengembangan SPBE; dan
   c. uji kelaikan SPBE.

Pasal 22

Pengendalian terhadap pemisahan perangkat pengembangan dan operasional SPBE sebagaimana dimaksud dalam Pasal 21 ayat (2) huruf a dilakukan dengan cara:
a. memisahkan lingkungan pengembangan dan pengujian serta operasional Aplikasi SPBE RRI, baik secara fisik, nonfisik (*logic),* maupun aksesnya;
b. menjaga agar lingkungan pengembangan tidak boleh diakses dari sistem operasional layanan;
c. mengupayakan lingkungan pengujian sama dengan lingkungan operasional layanan; dan
d. menjaga agar data yang memiliki klasifikasi rahasia dan sangat rahasia tidak boleh disalin ke dalam lingkungan sistem pengujian.

Pasal 23

(1) Pengendalian terhadap penerapan standar keamanan yang relevan dalam proses pembangunan dan pengembangan SPBE sebagaimana dimaksud dalam Pasal 21 ayat (2) huruf b dilakukan dengan cara memastikan dalam proses perencanaan dan pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE, termasuk yang dilakukan oleh Pihak Ketiga, telah memasukkan fitur-fitur keamanan dalam spesifikasi aplikasi dan infrastruktur SPBE yang dibangun atau dikembangkan.

(2) Fitur-fitur keamanan yang dimasukkan sesuai dengan standar keamanan relevan sebagaimana dimaksud pada ayat (1) meliputi:
   a. standar keamanan data dan Informasi;
   b. standar keamanan Aplikasi;
   c. standar keamanan Pusat Data;
   d. standar keamanan sistem penghubung layanan; dan
   e. standar keamanan jaringan intra.

(3) Standar keamanan relevan sebagaimana dimaksud pada ayat (2) paling sedikit memenuhi standar keamanan yang ditetapkan oleh lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

Pasal 24

(1) Pengendalian terhadap uji kelaikan SPBE sebagaimana dimaksud dalam Pasal 21 ayat (2) huruf c dilakukan dengan cara:

a. melaksanakan…

a. melaksanakan uji kelaikan Aplikasi SPBE RRI sebelum SPBE tersebut digunakan dan/atau sewaktu-waktu sesuai kebutuhan; dan
b. mengevaluasi dan melaksanakan kembali uji kelaikan SPBE RRI pada setiap perubahan besar (*major)* untuk menjamin keutuhan sistem informasi tidak terganggu.

(2) Pelaksanaan uji kelaikan Aplikasi SPBE sebelum digunakan dan/atau sewaktu-waktu sesuai kebutuhan sebagaimana dimaksud pada ayat (1) huruf a mencakup aspek:
a. uji fungsi, yaitu pengujian yang memastikan Aplikasi SPBE RRI yang dibangun dan/atau dikembangkan telah memenuhi fungsi-fungsi sesuai dengan dokumentasi terkait;
b. uji integrasi, yaitu pengujian yang memastikan Aplikasi SPBE RRI yang dibangun dan/atau dikembangkan telah memenuhi kebutuhan dan persyaratan integrasi dengan Aplikasi, Data, serta komponen-komponen lain yang terkait;
c. uji beban, yaitu pengujian yang memastikan Aplikasi SPBE RRI yang dibangun dan/atau dikembangkan dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya; dan
d. uji keamanan, yaitu pengujian yang memastikan Aplikasi SPBE RRI yang dibangun dan/atau dikembangkan dapat menjaga keamanan Data dan Informasi yang terkait dengannya.

(3) Uji kelaikan pada aspek uji fungsi, uji integrasi, dan uji beban dapat menggunakan pedoman dan/atau instrumen pengukuran yang ditetapkan oleh kementerian yang menyelenggarakan tugas pemerintahan di bidang komunikasi dan informatika.

(4) Uji kelaikan pada aspek uji keamanan dapat menggunakan pedoman dan/atau instrumen pengukuran yang ditetapkan oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

(5) Pelaksanaan pembangunan dan pengembangan Aplikasi dilakukan sesuai dengan standar teknis dan prosedur pembangunan dan pengembangan Aplikasi yang ditetapkan oleh kementerian yang melaksanakan tugas di bidang komunikasi dan informatika.

Bagian Kesembilan
Pengendalian Pihak Ketiga

Pasal 25

(1) Pengendalian keamanan Pihak Ketiga sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf h dilakukan untuk memastikan pelindungan Aset Informasi yang dapat diakses oleh Pihak Ketiga.

(2) Pengendalian keamanan Pihak Ketiga sebagaimana dimaksud pada ayat (1) dilakukan dengan cara:
a. melakukan pemeriksaan latar belakang Pihak Ketiga

dengan…

dengan tetap memperhatikan privasi dan perlindungan data pribadi sesuai ketentuan peraturan perundang-undangan;

b. membuat dan meninjau ulang secara berkala perjanjian keamanan dengan Pihak Ketiga yang terlibat dalam penggunaan dan/atau pengelolaan Aset Informasi dan/atau SPBE RRI yang menyatakan tanggung jawab terhadap keamanan Aset Informasi;
c. memastikan secara berkala pengendalian Keamanan Informasi atas Aset Informasi dan/atau SPBE RRI, definisi layanan, perubahan layanan, penggunaan alih daya (subkontraktor), dan tingkat layanan yang termuat dalam kesepakatan penyediaan layanan, telah diterapkan, dioperasikan, dan dipelihara oleh Pihak Ketiga;
d. memastikan *Service Level Agreement* (SLA) Pihak Ketiga telah mengatur ketersediaan layanan dan penyelesaian Insiden Keamanan;
e. melakukan pemantauan terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh Pihak Ketiga secara berkala;
f. memperhatikan tingkat kekritisan data, 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 oleh Pihak Ketiga;
h. memberikan Informasi tentang gangguan keamanan dan mengkaji Informasi bersama Pihak Ketiga;
i. mencabut hak akses terhadap Aset Informasi dan/atau SPBE RRI yang dimiliki Pihak Ketiga apabila yang bersangkutan tidak lagi bekerja di RRI;
j. membuat berita acara serah terima terkait mengembalikan seluruh Aset Informasi yang dipergunakan selama bekerja bagi Pihak Ketiga yang berakhir masa kontraknya; dan
k. memastikan Pihak Ketiga dan tamu yang memasuki lingkungan Pusat Data dan/ atau tempat layanan SPBE RRI harus mematuhi standar keamanan fisik dan lingkungan.

(3) Perjanjian keamanan sebagaimana dimaksud pada ayat (2) huruf b disusun secara tertulis dengan paling sedikit memuat:

a. pelindungan atas Aset Informasi bersifat rahasia dan sangat rahasia dan hak kekayaan intelektual setiap pihak;
b. dalam hal Aset Informasi dan/atau SPBE RRI disediakan oleh Pihak Ketiga, maka dicantumkan jaminan bahwa tidak terdapat kode berbahaya (*malicious code)* dan celah akses ilegal (*backdoor)*;
c. hak untuk melakukan audit dan memantau kegiatan yang melibatkan Aset Informasi bersifat rahasia dan sangat rahasia;
d. pengawasan atas akses terhadap Aset Informasi yang diberikan pada Pihak Ketiga;
e. pelaporan terhadap pengungkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan;

f. syarat...

f. syarat untuk Informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian;
g. penggunaan jalur komunikasi yang aman untuk perpindahan Informasi antara RRI dengan Pihak Ketiga; dan
h. dalam hal Pihak Ketiga tidak lagi menjadi bagian dalam pengelolaan Aset Informasi dan/atau SPBE RRI, maka Aset Informasi dana/atau SPBE RRI yang dikuasai oleh Pihak Ketiga harus dikembalikan kepada RRI.

Bagian Kesepuluh
Pengendalian Kriptografi

Pasal 26

(1) Pengendalian Kriptografi sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf i dilaksanakan untuk memastikan penggunaan Kriptografi yang tepat guna melindungi kerahasiaan, keutuhan, dan keotentikan Data dan Informasi yang bersifat rahasia dan/atau sangat rahasia yang dikelola dalam Infrastruktur SPBE.

(2) Pengendalian Kriptografi sebagaimana dimaksud pada ayat (1) dilakukan dengan cara:
a. melakukan klasifikasi Informasi yang disimpan dan dikelola dalam perangkat informasi sesuai dengan ketentuan peraturan perundang-undangan; dan
b. menerapkan keamanan Kriptografi untuk Aset Informasi bersifat rahasia dan/atau sangat rahasia.

Pasal 27

Pengendalian Kriptografi sebagaimana dimaksud dalam Pasal 26 ayat (2) huruf b dilaksanakan dengan cara:
a. menerapkan jalur komunikasi aman dengan menerapkan sertifikat protokol Kriptografi (*Secure Socket Layer/*SSL) untuk proses otentikasi antara Pengguna dengan Aplikasi SPBE RRI berbasis *website*;
b. menjaga kerahasiaan kata sandi dan menyimpannya dalam basis data (*database)* SPBE RRI dengan mekanisme enkripsi (*hash function)*;
c. melindungi kerahasiaan data dan Informasi dengan klasifikasi rahasia dan/atau sangat rahasia dalam basis data (*database)* dengan mekanisme kriptografi simetrik;
d. menerapkan otentikasi berbasis tanda tangan digital dengan menggunakan Sertifikat Elektronik yang dikeluarkan oleh Pihak Ketiga terpercaya sesuai rekomendasi pegawai yang pengelola SPBE RRI;
e. menggunakan algoritma Kriptografi, modul Kriptografi, protokol Kriptografi, dan kunci Kriptografi sesuai ketentuan peraturan perundang-undangan dan/atau rekomendasi dari lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber; dan
f. menetapkan standar penggunaan Kriptografi sesuai dengan perkembangan teknologi.

bagian...

Bagian Kesebelas
Pengendalian Keamanan Insiden Siber

Pasal 28

(1) Pengendalian Keamanan Insiden Siber Insiden Siber dilaksanakan melalui Manajemen Insiden Siber.

(2) Manajemen Insiden Siber sebagaimana dimaksud pada ayat (1) dilaksanakan oleh RRI-CSIRT.

Pasal 29

(1) RRI-CSIRT sebagaimana dimaksud dalam Pasal 28 ayat (2) mempunyai tugas sebagai berikut:
   a. melakukan tindakan pencegahan Insiden Siber;
   b. melaksanakan prosedur penanganan dan pemulihan Insiden Siber jika terjadi Insiden Siber;
   c. menyusun skenario penanganan dan pemulihan Insiden Siber;
   d. melakukan simulasi berkala skenario penanganan dan pemulihan Insiden Siber yang telah disusun;
   e. memberikan pelatihan terhadap sumber daya manusia yang terlibat dalam simulasi penanganan dan pemulihan Insiden Siber sesuai skenario yang disusun;
   f. menjalankan program kesadaran ancaman dan penanganan Insiden Siber, serta berperan aktif pada seluruh pegawai;
   g. memastikan tersedianya kontak pelaporan Insiden Siber yang dapat diakses oleh seluruh pegawai di lingkungan RRI, termasuk oleh Pihak Ketiga; dan
   h. melaksanakan pengukuran tingkat penanganan Insiden Siber secara berkala.

(2) Tindakan pencegahan Insiden Siber sebagaimana dimaksud pada ayat (1) huruf a paling sedikit meliputi:
   a. melakukan penilaian kerentanan keamanan (*penetration testing)* untuk menemukan celah keamanan pada SPBE RRI;
   b. mengimplementasikan alat pemantauan keamanan berupa perangkat manajemen peristiwa dan Keamanan Informasi (*Security Information and Event Managemen*t/SIEM); dan
   c. melakukan pemantauan dan pendeteksian serangan keamanan terhadap Sistem Informasi SPBE RRI.

(3) Prosedur penyesuaian skenario penanganan Insiden Siber sebagaimana dimaksud pada ayat (1) huruf b meliputi:
   a. menerima laporan dan mencatat Insiden Siber;
   b. mengidentifikasi sumber serangan;

c. menganalisis…

c. menganalisis Informasi yang berkaitan dengan Insiden Siber;
d. melaporkan Insiden Siber kepada atasan;
e. memprioritaskan penanganan Insiden Siber berdasarkan tingkat dampak;
f. mengidentifikasi eskalasi penanganan Inside Siber;
g. mendokumentasikan bukti Insiden Siber;
h. menyusun laporan penanganan Insiden Siber; dan
i. mengevaluasi dan memperbaiki standar, prosedur, dan kontrol keamanan SPBE RRI agar Insiden siber serupa tidak terulang.

Bagian Kedua Belas
Pengendalian Kelangsungan Layanan Informasi

Pasal 30

(1) Pengendalian kelangsungan layanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf k dilakukan untuk menjamin ketersediaan layanan Informasi pada saat terjadi keadaan darurat.

(2) Pengendalian keberlangsungan layanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan dengan cara:
a. melakukan identifikasi Risiko terhadap keberlangsungan layanan Informasi;
b. menyusun dan mengimplementasikan rencana keberlangsungan layanan Informasi (*Business Continuity Planning*) untuk menjaga dan mengembalikan operasional Aset Informasi dan/atau SPBE RRI dalam jangka waktu yang disepakati serta tingkat keberlangsungan yang dibutuhkan;
c. melakukan uji coba rencana keberlangsungan layanan Informasi secara berkala; dan
d. melaksanakan pengelolaan layanan sesuai dengan pedoman manajemen layanan SPBE yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang komunikasi dan informatika.

(3) Rencana keberlangsungan layanan Informasi sebagaimana dimaksud pada ayat (2) huruf b paling sedikit meliputi:
a. prosedur keberlangsungan layanan Informasi SPBE RRI pada saat keadaan darurat, manajemen Risiko, analisis dampak kegiatan, pengembalian kondisi sebelum terjadi gangguan (*rollback)*, peralihan kondisi normal, dan uji coba keberlangsungan kegiatan;
b. penetapan peran dan penanggung jawab pegawai yang terlibat dalam pelaksanaan keberlangsungan layanan Informasi; dan
c. pelaksanaan sosialisasi dan pelatihan keberlangsungan layanan Informasi.

Bagian…

Bagian Ketiga Belas
Pengendalian Kepatuhan

Pasal 31

(1) Pengendalian kepatuhan sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf l dilakukan untuk memastikan kepatuhan pegawai dan Pihak Ketiga dalam melaksanakan keamanan Aset Informasi dan/atau SPBE RRI sesuai dengan ketentuan peraturan perundang-undangan.

(2) Pengendalian kepatuhan sebagaimana dimaksud pada ayat (1) dilakukan dengan cara:
   a. mengidentifikasi, mendokumentasikan, dan memelihara regulasi, standar, dan/atau prosedur Keamanan Informasi atau keamanan SPBE;
   b. memeriksa kepatuhan seluruh pegawai dan Pihak Ketiga terhadap regulasi, standar, dan prosedur Keamanan Informasi atau keamanan SPBE;
   c. mendapatkan Aplikasi hanya melalui sumber yang dikenal dan memiliki reputasi baik untuk memastikan tidak ada pelanggaran hak cipta;
   d. memeriksa kepatuhan penggunaan lisensi Aplikasi dan menerapkan pengendalian untuk memastikan jumlah Pengguna tidak melampaui lisensi yang dimiliki;
   e. memelihara bukti kepemilikan lisensi Aplikasi, program induk Sistem Elektronik (*master disk),* dan/atau buku manual;
   f. melakukan pemeriksaan ketiadaan produk bajakan yang terinstal dan menyebabkan terjadinya pelanggaran hak kekayaan intelektual;
   g. memastikan arsip siaran terlindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah, dan rilis tidak sah sesuai dengan ketentuan peraturan perundang-undangan, kontraktual, atau bisnis;
   h. memastikan pengamanan privasi dan data pribadi yang dapat diidentifikasikan sesuai ketentuan peraturan perundang-undangan;
   i. memastikan kesesuaian penerapan Kriptografi sesuai dengan ketentuan peraturan perundang-undangan; dan
   j. melakukan reviu sistem informasi secara berkala agar sesuai dengan kebijakan dan standar Keamanan Informasi.

BAB V
AUDIT KEAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 32

Audit Keamanan Informasi dilaksanakan secara berkala paling sedikit 1 (satu) kali dalam 2 (dua) tahun dan dimasukkan dalam Peta Rencana SPBE RRI untuk memastikan diterapkannya kebijakan, standar, dan prosedur Keamanan Informasi.

Bagian...

Bagian Kedua
Pelaksana Audit Keamanan Informasi

Pasal 33

Audit Keamanan Informasi sebagaimana dimaksud dalam Pasal 32 dilaksanakan melalui :
a. Audit Internal Keamanan Informasi; dan
b. Audit Eksternal Keamanan Informasi

Bagian Ketiga
Audit Internal Keamanan Informasi

Pasal 34

(1) Audit Internal Keamanan Informasi sebagaimana dimaksud dalam Pasal 33 huruf a dilaksanakan dengan cara:
   a. merencanakan, menetapkan, dan menjalankan program audit sesuai dengan pedoman Audit Internal Keamanan SPBE;
   b. mencatat setiap temuan audit secara formal oleh auditor dan diberikan kepada auditan;
   c. melakukan perbaikan terhadap setiap temuan yang diberikan oleh auditor dalam jangka waktu yang disepakati;
   d. melaporkan hasil audit keamanan kepada tim yang mengelola Keamanan Informasi sebagai bahan evaluasi penerapan kebijakan Keamanan Informasi;
   e. menyimpan dan mendokumentasikan proses dan hasil Audit Internal Keamanan Informasi sebagai alat bukti dari program audit; dan
   f. melaksanakan Audit Internal Keamanan Informasi dengan menggunakan instrumen penilaian Audit Keamanan SPBE yang ditetapkan oleh pimpinan lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

(2) Program audit sebagaimana dimaksud pada ayat (1) huruf a mencakup;
   a. frekuensi;
   b. metode;
   c. kriteria;
   d. lingkup;
   e. tanggung jawab; dan
   f. pelaporan audit,

   dengan mempertimbangkan pentingnya proses yang sedang berjalan dan hasil audit sebelumnya.

(3) Audit Internal Keamanan Informasi sebagaimana

dimaksud...

dimaksud pada ayat (1) dilaksanakan secara periodik oleh auditor pada Satuan Pengawasan Intern di lingkungan RRI.

(4) Satuan Pengawasan Intern dapat melibatkan pegawai yang memiliki kompetensi:
a. Audit TIK; dan/atau
b. audit keamanan informasi
sesuai ketentuan peraturan perundang-undangan.

Bagian Keempat
Audit Eksternal Keamanan Informasi

Pasal 35

Audit Eksternal Keamanan Informasi sebagaimana dimaksud dalam Pasal 33 huruf b dilaksanakan oleh Pihak Ketiga sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI
EVALUASI KINERJA DAN
PERBAIKAN BERKELANJUTAN KEAMANAN INFORMASI

Pasal 36

(1) Evaluasi kinerja Keamanan Informasi dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun dalam bentuk tinjauan manajemen untuk memastikan pencapaian target Keamanan Informasi yang telah direncanakan.

(2) Tinjauan manajemen Keamanan Informasi dilakukan berdasarkan peta rencana, sasaran Keamanan Informasi, dan hasil audit Keamanan Informasi dengan cara:
a. mengidentifikasi area proses yang memiliki Risiko tinggi terhadap keberhasilan pelaksanaan Keamanan Informasi;
b. menetapkan indikator kinerja pada setiap area proses;
c. memformulasi pelaksanaan Keamanan Informasi dengan mengukur secara kuantitatif kinerja yang diharapkan;
d. melakukan evaluasi terhadap pelaksanaan SMKI di lingkungan RRI;
e. menganalisis efektivitas pelaksanaan Keamanan Informasi; dan
f. mendukung dan merealisasikan program audit Keamanan Informasi.

(3) Hasil tinjauan manajemen Keamanan Informasi didokumentasikan sebagai bahan evaluasi kinerja Keamanan Informasi

Pasal...

Pasal 37

(1) Tindak lanjut dari hasil tinjauan manajemen sebagaimana dimaksud dalam Pasal 36 ayat (3) berupa perbaikan berkelanjutan.

(2) Tim melakukan perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dengan cara:
   a. mengatasi permasalahan dalam pelaksanaan Keamanan Informasi; dan
   b. memperbaiki pelaksanaan Keamanan Informasi secara berkala.

(3) Tindakan perbaikan yang telah dilakukan oleh tim didokumentasikan sebagai bahan evaluasi kinerja Keamanan Informasi.

BAB VII
KETENTUAN LAIN-LAIN

Pasal 38

Pedoman teknis dan/atau standar operasional prosedur yang diperlukan dalam rangka pelaksanaan Peraturan Direktur Utama ini diatur lebih lanjut oleh Direktur Teknologi dan Media Baru.

BAB VIII
KETENTUAN PENUTUP

Pasal 39

Peraturan Direktur Utama ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta

Pada Tanggal 6 Juli 2026

Direktur Utama
Lembaga Penyiaran Publik
Radio Republik Indonesia

I Hendrasmo