PERATURAN
KEPALA BADAN METEOROLOGI, KLIMATOLOGI, DAN GEOFISIKA
REPUBLIK INDONESIA
NOMOR 8 TAHUN 2024
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN METEOROLOGI, KLIMATOLOGI, DAN GEOFISIKA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 48 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan Peraturan Badan Meteorologi, Klimatologi, dan Geofisika tentang Sistem Manajemen Keamanan Informasi;

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 diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
2. Undang-Undang Nomor 31 Tahun 2009 tentang Meteorologi, Klimatologi, dan Geofisika (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 139, Tambahan Lembaran Negara Republik Indonesia Nomor 5058);
3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185);
4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
5. Peraturan Presiden Nomor 12 Tahun 2024 tentang Badan Meteorologi, Klimatologi, dan Geofisika (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 25);
6. Peraturan Badan Meteorologi, Klimatologi, dan Geofisika Nomor 6 Tahun 2020 tentang Organisasi dan Tata Kerja

Balai Besar Meteorologi, Klimatologi, dan Geofisika, Stasiun Meteorologi, Stasiun Klimatologi, dan Stasiun Geofisika (Berita Negara Republik Indonesia Tahun 2020 Nomor 1371) sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Badan Meteorologi, Klimatologi, dan Geofisika Nomor 4 Tahun 2023 tentang Perubahan Kedua atas Peraturan Badan Meteorologi, Klimatologi, dan Geofisika Nomor 6 Tahun 2020 tentang Organisasi dan Tata Kerja Balai Besar Meteorologi, Klimatologi, dan Geofisika, Stasiun Meteorologi, Stasiun Klimatologi, dan Stasiun Geofisika (Berita Negara Republik Indonesia Tahun 2023 Nomor 857);

7. Peraturan Badan Meteorologi, Klimatologi, dan Geofisika Nomor 7 Tahun 2020 tentang Organisasi dan Tata Kerja Sekolah Tinggi Meteorologi, Klimatologi, dan Geofisika (Berita Negara Republik Indonesia Tahun 2020 Nomor 1372);
8. Peraturan Badan Meteorologi, Klimatologi, dan Geofisika Nomor 8 Tahun 2020 tentang Organisasi dan Tata Kerja Stasiun Pemantau Atmosfer Global (Berita Negara Republik Indonesia Tahun 2020 Nomor 1373);
9. Peraturan Badan Meteorologi, Klimatologi, dan Geofisika Nomor 2 Tahun 2024 tentang Organisasi dan Tata Kerja Badan Meteorologi, Klimatologi, dan Geofisika (Berita Negara Republik Indonesia Tahun 2024 Nomor 365);

MEMUTUSKAN:

Menetapkan : PERATURAN KEPALA BADAN METEOROLOGI, KLIMATOLOGI, DAN GEOFISIKA TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Kepala Badan ini yang dimaksud dengan:

1. Teknologi Informasi dan Komunikasi selanjutnya disebut TIK adalah terminologi yang mencakup seluruh peralatan teknis untuk memproses dan menyampaikan informasi.
2. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
3. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
4. Data adalah 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.
5. Informasi adalah satu atau sekumpulan Data, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat

elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

6. Aplikasi adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan.
7. Infrastruktur 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.
8. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan Informasi berdasarkan pendekatan risiko.
9. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersedian, dan kenirsangkalan informasi.
10. Risiko adalah segala kejadian dalam setiap aktivitas yang mungkin timbul karena faktor ketidakpastian, yang mengandung potensi untuk menghambat pencapaian sasaran kinerja dari layanan Sistem Elektronik.
11. Manajemen Risiko adalah aktivitas terkoordinasi untuk identifikasi, penilaian, dan penentuan prioritas Risiko yang kemudian akan dikelola, dipantau, dan dikontrol untuk mengurangi dampak dan/ atau kemungkinan terjadinya Risiko tersebut.
12. Rencana Tindak Lanjut Risiko yang selanjutnya disingkat RTL adalah respon yang direncanakan manajemen untuk menindaklanjuti hasil evaluasi Risiko, seperti *mitigate/reduce, avoid, share/ transfer* atau *accept.*
13. 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 kriteria dan/atau standar yang telah ditetapkan terhadap beroperasinya Keamanan Informasi.
14. Auditor Keamanan Informasi yang selanjutnya disebut Auditor adalah orang yang memiliki kompetensi untuk melakukan Audit Keamanan Informasi.
15. Auditan adalah subjek atau pihak yang diaudit oleh auditor.
16. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
17. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam keamanan informasi antara lain namun tidak terbatas pada *web defacement, malware (virus, worm, trojan backdoor* dan *ransomware*), *unauthorized access, data breach,* dan *Distributed Denial of Service* (DDoS).

18. Tim Tanggap Insiden Siber yang selanjutnya disebut BMKG-CSIRT adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
19. Tim Pengelola Sistem Manajemen Keamanan Informasi yang selanjutnya disebut Tim SMKI adalah sekelompok orang yang bertanggung jawab untuk menyusun, mengomunikasikan, memastikan, dan memantau pelaksanaan SMKI di Badan Meteorologi, Klimatologi, dan Geofisika.
20. Badan Meteorologi, Klimatologi, dan Geofisika yang selanjutnya disingkat BMKG adalah lembaga pemerintah nonkementerian yang melaksanakan tugas pemerintahan di bidang penyelenggaraan meteorologi, klimatologi, dan geofisika.
21. Sekretaris Utama adalah pimpinan unit kerja yang menyelenggarakan koordinasi pelaksanaan tugas, pembinaan, dan pemberian dukungan administrasi kepada seluruh unsur organisasi.
22. Aset Informasi adalah segala sesuatu yang dapat memberikan nilai tambah bagi Badan Meteorologi Klimatologi dan Geofisika dalam menunjang proses bisnis dan perlu dilindungi dari berbagai ancaman Keamanan Informasi.
23. *Removable* Media adalah media yang digunakan untuk penyimpanan Informasi yang dirancang untuk dengan mudah dimasukkan ke dalam PC/Notebook/perangkat portabel lainnya berupa CD, DVD, *flashdisk*, ataupun semua jenis kartu memori yang dapat dilepas atau *portable*.
24. Pusat Data adalah fasilitas fisik yang digunakan untuk menyimpan sistem komputer dan komponen-komponen terkait seperti sistem telekomunikasi dan penyimpanan Data.
25. Tempat Layanan Informasi adalah lokasi atau fasilitas di mana informasi disimpan, diproses, atau ditransmisikan.
26. Pihak Ketiga adalah tenaga kerja alihdaya, pihak yang terafiliasi, dan petugas lembaga lain yang melakukan kegiatan yang terkait dengan tugas pokok BMKG.

Pasal 2

(1) Peraturan Kepala Badan ini dimaksudkan sebagai kebijakan internal manajemen Keamanan Informasi SPBE di lingkungan BMKG.
(2) Kebijakan internal manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) meliputi:
    a. penetapan ruang lingkup;
    b. penetapan penanggung jawab;
    c. perencanaan;
    d. dukungan pengoperasian;
    e. kendali keamanan;
    f. audit Keamanan Informasi; dan
    g. evaluasi kinerja dan perbaikan berkelanjutan Keamanan Informasi.
(3) Kendali keamanan sebagaimana dimaksud pada ayat (2) huruf e terdiri dari:

a. keamanan sumber daya manusia;
b. keamanan Aset Informasi;
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 Siber;
k. manajemen keberlangsungan layanan Informasi; dan
l. pengendalian kepatuhan.

BAB II
KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu
Penetapan Ruang Lingkup

Pasal 3

(1) Penetapan ruang lingkup manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a meliputi:
   a. Data dan Informasi SPBE;
   b. Aplikasi SPBE;
   c. Infrastruktur SPBE; dan
   d. sumber daya manusia SPBE.
(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan Aset Informasi yang harus diamankan dalam SPBE.

Bagian Kedua
Penetapan Penanggung Jawab

Pasal 4

(1) Sekretaris Utama berperan sebagai penanggung jawab SMKI.
(2) Sekretaris Utama bertanggung jawab untuk:
   a. memastikan pelaksanaan kebijakan Keamanan Informasi;
   b. menyediakan sumber daya manusia dan infrastuktur yang memadai untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan Keamanan Informasi BMKG;
   c. menetapkan kriteria penerimaan Risiko dan tingkat Risiko yang dapat diterima;
   d. memastikan pelaksanaan audit internal Keamanan Informasi;
   e. menetapkan arsitektur Keamanan Informasi;
   f. menetapkan peta rencana 5 (lima) tahunan dan sasaran Keamanan Informasi setiap tahunnya;
   g. melakukan tinjauan secara berkala atas pelaksanaan kebijakan SMKI; dan

h. menyampaikan kinerja pelaksanaan kebijakan Keamanan Informasi kepada Kepala BMKG

(3) Dalam melaksanakan tugas sebagai penanggung jawab SMKI, Sekretaris Utama dibantu oleh Tim SMKI selaku pelaksana teknis Keamanan Informasi.

(4) Tim SMKI sebagaimana dimaksud pada ayat (3) terdiri dari:
a. Penanggung Jawab;
b. Ketua;
c. Koordinator;
d. Unit pengawasan internal; dan
e. Anggota.

(5) Tim SMKI sebagaimana dimaksud pada ayat (4) ditetapkan oleh Kepala BMKG.

Pasal 5

(1) Ketua Tim SMKI sebagaimana dimaksud dalam Pasal 4 ayat (4) huruf b dijabat oleh pimpinan tinggi pratama yang mempunyai tugas dan fungsi di bidang keamanan teknologi, Informasi dan komunikasi pada BMKG.

(2) Ketua Tim SMKI memiliki kewenangan dalam menentukan komposisi, kualifikasi, dan jumlah anggota tim.

(3) Koordinator sebagaimana dimaksud dalam Pasal 4 ayat (4) huruf c melakukan tanggung jawab atas pelaksanaan kegiatan Keamanan Informasi.

(4) Unit pengawasan internal sebagaimana dimaksud dalam Pasal 4 ayat (4) huruf d berperan melaksanakan audit internal Keamanan Informasi.

(5) Unit pengawasan internal bertanggung jawab untuk:
a. menyusun pedoman audit internal Keamanan Informasi;
b. menyusun perencanaan audit internal Keamanan Informasi;
c. melaksanakan kegiatan audit internal Keamanan Informasi;
d. memberikan rekomendasi perbaikan atas hasil temuan audit internal Keamanan Informasi; dan
e. menyampaikan laporan audit internal Keamanan Informasi kepada Sekretaris Utama.

(6) Anggota sebagaimana dimaksud dalam Pasal 4 ayat (4) huruf e berperan membantu Koordinator dalam melaksanakan tugas Keamanan Informasi.

Pasal 6

(1) Tim SMKI bertanggung jawab untuk:
a. menyusun, mengomunikasikan, dan memantau pelaksanaan kebijakan Keamanan Informasi di BMKG;
b. melakukan analisis kebutuhan keamanan informasi;
c. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Informasi;
d. memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur Informasi termasuk yang dilakukan oleh Pihak Ketiga, paling sedikit memenuhi standar teknis dan prosedur Keamanan Informasi yang ditetapkan oleh lembaga

yang melaksanakan tugas pemerintahan di bidang keamanan siber;

e. memastikan peningkatan kesadaran, kepedulian, dan kepatuhan oleh seluruh pegawai terhadap kebijakan, prosedur, dan standar Keamanan Informasi;
f. memastikan penerapan dokumen perjanjian kerahasiaan (*Non Disclosure Agreement*) guna menjaga kerahasiaan Aset Informasi;
g. mengendalikan dan menjaga kemutakhiran kebijakan, prosedur, dan standar Keamanan Informasi;
h. memfasilitasi pelaksanaan audit internal dan audit eksternal Keamanan Informasi;
i. memastikan diterapkannya Manajemen Risiko, manajemen perubahan, manajemen Insiden Siber, manajemen kapasitas, manajemen permasalahan, serta manajemen aset dan konfigurasi;
j. mendorong perbaikan penerapan Keamanan Informasi berdasarkan hasil temuan audit internal dan audit eksternal; dan
k. menyusun laporan evaluasi penerapan kebijakan Keamanan Informasi dan menyampaikannya kepada Sekretaris Utama.

(2) Dalam memfasilitasi pelaksanaan audit internal Keamanan Informasi sebagaimana dimaksud pada ayat (2) huruf h, Tim SMKI dapat menunjuk pihak yang berkompeten di bidang Audit Keamanan Informasi sebagai konsultan.

(3) Analisis kebutuhan Keamanan Informasi sebagaimana dimaksud pada ayat (2) huruf b diselenggarakan dengan cara:
a. mengidentifikasi Aplikasi dan Infrastruktur untuk keamanan informasi;
b. mengidentifikasi standar kompetensi personel keamanan informasi; dan
c. mengidentifikasi program peningkatan kompetensi keamanan informasi dan penanggulangan Insiden Siber.

Bagian Ketiga
Perencanaan Keamanan Informasi

Pasal 7

(1) Perencanaan Keamanan Informasi dilakukan oleh Tim SMKI.

(2) BMKG sebagai penyelenggara SPBE yang merupakan Sistem Elektronik lingkup publik, melakukan kategorisasi setiap Sistem Elektronik yang dimilikinya sebagai salah satu dasar dalam pelaksanaan Keamanan Informasi.

(3) Penentuan kategorisasi Sistem Elektronik sebagaimana dimaksud pada ayat (2) dilakukan sesuai dengan ketentuan peraturan perundang-undangan yang ditetapkan oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

Pasal 8

(1) Pelaksanaan Keamanan Informasi dilakukan dengan memperhatikan berbagai Risiko yang dapat mengakibatkan terjadinya kegagalan Keamanan Informasi di BMKG.

(2) Dalam melaksanakan perencanaan Keamanan Informasi, Tim SMKI melakukan Manajemen Risiko Keamanan Informasi dengan cara:
   a. menyusun profil Risiko (penetapan, penilaian, dan penanganan Risiko) Keamanan Informasi;
   b. menyusun RTL bersama dengan unit terkait; dan
   c. melakukan sosialisasi dan komunikasi RTL kepada para pemilik risiko.

(3) Dalam menyusun penetapan, penilaian, dan penanganan Risiko Keamanan Informasi sebagaimana dimaksud pada ayat (2) huruf a meliputi:
   a. identifikasi sasaran;
   b. penetapan kategori Risiko;
   c. penetapan area dampak Risiko;
   d. penetapan pemilik Risiko;
   e. penerapan kriteria Risiko;
   f. kriteria kemungkinan;
   g. kriteria dampak;
   h. identifikasi ancaman;
   i. matriks analisis Risiko;
   j. selera Risiko;
   k. identifikasi Risiko;
   l. analisis Risiko;
   m. evaluasi Risiko;
   n. penanganan Risiko;
   o. prioritisasi Risiko;
   p. rencana penanganan Risiko SPBE;
   q. Risiko residual; dan
   r. pemantauan Risiko.

(4) Manajemen Risiko sebagaimana dimaksud pada ayat (2) dilakukan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan jika ada perubahan Aset Informasi dan/atau proses bisnis yang berdampak signifikan terhadap profil Risiko yang ditetapkan sesuai dengan kebijakan metodologi penilaian Risiko dan peluang.

Pasal 9

(1) Tim SMKI menyusun program kerja Keamanan Informasi berdasarkan RTL sebagai wujud realisasi atas tindak lanjut Risiko Keamanan Informasi.

(2) Program kerja Keamanan Informasi sebagaimana dimaksud pada ayat (1) paling sedikit meliputi:
   a. edukasi kesadaran Keamanan Informasi;
   b. penilaian kerentanan Keamanan Informasi;
   c. peninjaringagkatan Keamanan Informasi;
   d. penanganan Insiden Siber; dan
   e. audit Keamanan Informasi.

(3) Program kerja Keamanan Informasi dituangkan dalam peta rencana Keamanan Informasi yang disusun untuk periode 5 (lima) tahunan dengan sasaran Keamanan Informasi yang ditetapkan untuk setiap tahunnya.

(4) Peta rencana Keamanan Informasi sebagaimana dimaksud pada ayat (3) menjadi bagian dari peta rencana SPBE.

Bagian Keempat
Dukungan Pengoperasian

Pasal 10

(1) Sekretaris Utama memberikan dukungan pengoperasian Keamanan Informasi dengan menyediakan sumber daya manusia Keamanan Informasi yang berkompeten dan anggaran Keamanan Informasi.
(2) Sumber daya manusia Keamanan Informasi sebagaimana dimaksud pada ayat (1) harus memiliki kompetensi:
    a. keamanan infrastruktur TIK; dan
    b. keamanan Aplikasi.
(3) Dalam hal sumber daya manusia Keamanan Informasi yang disediakan belum memiliki kompetensi memadai, maka Sekretaris Utama dapat memfasilitasi peningkatan kompetensi melalui kegiatan pelatihan dan/atau bimbingan teknis.
(4) Sekretaris Utama memfasilitasi penyelenggaraan kegiatan kesadaran keamanan informasi bagi pegawai di lingkungan BMKG.
(5) Sekretaris Utama menyediakan anggaran Keamanan Informasi berdasarkan arsitektur dan peta rencana Keamanan Informasi yang telah disusun sesuai usulan dari unit kerja yang mempunyai tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi.
(6) Penyediaan anggaran Keamanan Informasi sebagaimana dimaksud pada ayat (5) dibebankan pada Daftar Isian Pelaksanaan Anggaran (DIPA) BMKG atau sumber lainnya yang sah dan tidak mengikat.

Bagian Kelima
Kendali Keamanan

Pasal 11

Pelaksanaan kendali keamanan dalam SMKI terdiri dari:
a. keamanan sumber daya manusia;
b. keamanan Aset Informasi;
c. keamanan akses;
d. keamanan kriptografi;
e. keamanan fisik dan lingkungan;
f. keamanan operasional;
g. keamanan komunikasi;
h. keamanan pengembangan dan pemeliharaan; dan
i. keamanan Pihak Ketiga.

Paragraf 1
Keamanan Sumber Daya Manusia

Pasal 12

(1) Keamanan sumber daya manusia sebagaimana dimaksud dalam Pasal 11 huruf a, dilakukan untuk mengendalikan sumber daya manusia baik pegawai maupun Pihak Ketiga dalam melaksanakan kebijakan SMKI.

(2) Keamanan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Tim SMKI bekerja sama dengan unit kerja terkait dengan cara:
a. mengomunikasikan peran dan tanggung jawab pelaksanaan kebijakan SMKI kepada seluruh pegawai dan Pihak Ketiga 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;
d. membuat perjanjian tertulis dengan pegawai dan Pihak Ketiga yang terlibat dalam penggunaan dan/atau pengelolaan Informasi yang menyatakan tanggung jawab terhadap Keamanan Informasi dan sanksi atas pelanggaran Keamanan Informasi;
e. menghentikan hak penggunaan Aset Informasi bagi pegawai yang sedang dalam pemeriksaan terkait dengan dugaan pelanggaran Keamanan Informasi;
f. mencabut hak akses ke Aset Informasi yang dimiliki pegawai dan Pihak Ketiga apabila yang bersangkutan tidak lagi memiliki kepentingan terhadap Aset Informasi, dimutasi, atau tidak lagi bekerja di BMKG;
g. membuat berita acara serah terima terkait penerimaan seluruh Aset Informasi yang dipergunakan selama bekerja dan pengembalian seluruh Aset Informasi bagi pegawai yang berhenti bekerja atau mutasi;
h. memberikan edukasi kesadaran Keamanan Informasi melalui kegiatan sosialisasi, bimbingan teknis, dan/atau pelatihan mengenai Keamanan Informasi yang dilaksanakan secara berkala; dan
i. memelihara catatan pelatihan, kompetensi, pengalaman, dan kualifikasi pegawai yang mengelola Keamanan Informasi.

Paragraf 2
Keamanan Aset Informasi

Pasal 13

(1) Keamanan Aset Informasi sebagaimana dimaksud dalam Pasal 11 huruf b, dilakukan untuk mengamankan Aset Informasi berdasarkan tingkat kritikalitasnya.
(2) Keamanan Aset Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait dengan cara:
a. mengidentifikasi Aset Informasi dan mendokumentasikannya dalam daftar inventaris Aset Informasi yang memuat tingkat kritikalitas dan penanggung jawab setiap aset;
b. memberikan label sesuai tingkat kritikalitas;
c. menetapkan pihak-pihak yang dapat mengakses Aset Informasi;
d. menyusun prosedur penggunaan Aset Informasi;

e. menempatkan Aset Informasi di lokasi yang aman guna mengurangi Risiko aset Informasi dapat diakses oleh pihak yang tidak berwenang;
f. melakukan sanitasi terhadap perangkat penyimpanan Data yang sudah tidak digunakan lagi sebelum digunakan kembali atau dimusnahkan;
g. melakukan pemusnahan perangkat penyimpanan Data secara aman sesuai prosedur pemusnahan perangkat penyimpanan; dan
h. melaksanakan manajemen aset TIK sesuai dengan ketentuan manajemen aset TIK yang ditetapkan oleh kementerian yang melaksanakan tugas di bidang komunikasi dan informatika.

(3) Pengamanan atas Data dan/atau Informasi *Removable* Media di BMKG diatur dalam prosedur penanganan *Removable Media.*

Paragraf 3
Keamanan Akses

Pasal 14

(1) Keamanan akses sebagaimana dimaksud dalam Pasal 11 huruf c, dilakukan untuk mengendalikan akses ke Aset Informasi dengan memastikan perangkat pengguna yang terhubung ke Aset Informasi mendapatkan perlindungan keamanan dan tidak diakses oleh pihak yang tidak berhak.
(2) Keamanan akses terhadap Aset Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait dengan cara:
a. menyusun prosedur pengelolaan hak akses pengguna yang berisi ketentuan akses ke Aset Informasi sesuai dengan kebutuhan organisasi, persyaratan keamanan, dan peraturan yang berlaku;
b. mengelola akses pengguna;
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
g. menghapus akun setiap pegawai dan Pihak Ketiga yang tidak lagi memiliki kepentingan terhadap akses Aset Informasi.

(3) Pengelolaan akses pengguna sebagaimana dimaksud pada ayat (2) huruf b dilakukan dengan cara:
a. menggunakan akun yang unik untuk setiap pengguna;
b. memeriksa tingkat akses yang diberikan sesuai dengan tujuan penggunaan;
c. membatasi dan mengendalikan penggunaan hak akses khusus (jika ada);
d. mengatur pengelolaan kata sandi pengguna sesuai dengan ketentuan pengelolaan kata sandi di BMKG;

e. memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya;
f. memelihara catatan pengguna layanan (*user log*);
g. menonaktifkan akses pengguna 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 ke infrastruktur dan Aplikasi yang digunakan untuk melakukan diagnosa harus dikontrol dan hanya digunakan untuk pegawai yang bertugas untuk melakukan pengujian, pemecahan masalah, serta pengembangan sistem;
c. memisahkan jaringan untuk pengguna, sistem Informasi, dan layanan Informasi;
d. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu; dan
e. melakukan penghentian layanan jaringan pada area 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 dan sistem Informasi hanya diberikan kepada pengguna sesuai dengan peruntukannya dan dikontrol dengan menggunakan sistem manajemen akses pengguna;
b. setiap pengguna harus memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya dan proses otorisasi pengguna harus menggunakan teknik otentikasi yang sesuai untuk memvalidasi identitas pengguna;
c. menggunakan sistem pengelolaan kata sandi sesuai dengan ketentuan pengelolaan kata sandi di BMKG untuk memastikan kualitas kata sandi yang dibuat pengguna;
d. fasilitas *session time-out* harus diaktifkan untuk menutup dan mengunci layar komputer, Aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu;
e. membatasi waktu koneksi untuk sistem informasi dan Aplikasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia; dan
f. akses ke kode sumber Aplikasi dibatasi secara ketat diperuntukkan hanya bagi pihak-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-parameter keamanan yang harus

dipenuhi oleh perangkat kerja jarak jauh yang digunakan dalam mengakses Aset Informasi, yang terdiri dari:
a. *Virtual Private Network* (VPN);
b. *Secure Socket Layer* (SSL); dan/atau
c. *Two Step Authentication.*

(7) Pemantauan terhadap akses ke Aset Informasi sebagaimana dimaksud pada ayat (2) huruf g 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.

(8) Dalam hal diperlukan adanya akses ke Aset Informasi berklasifikasi rahasia, dapat dibuat hak akses khusus untuk mengakses sistem Informasi berklasifikasi rahasia pada sistem operasi, perangkat penyimpanan (*storage devices*), *file server*, dan Aplikasi sensitif.

(9) Pemberian hak akses khusus sebagaimana dimaksud pada ayat (8) dilakukan dengan cara:
a. mengidentifikasi hak akses khusus untuk dialokasikan kepada pengguna terkait;
b. memberikan hak akses khusus hanya kepada pengguna 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 lainnya.

(10) Pengelolaan kata sandi sebagaimana dimaksud pada ayat (3) huruf d dilakukan dengan cara:
a. menjaga kerahasiaan *password* dan menghindari menyimpan catatan *password*;
b. mengganti *password* apabila ada indikasi sistem dan *password* mengalami penyalahgunaan atau kebocoran.
c. menggunakan *password* yang berkualitas meliputi:
   1) panjang minimal 8 (delapan) karakter;
   2) menggunakan kombinasi huruf dan angka, sedapat mungkin menggunakan karakter spesial (seperti: !$%#*) kecuali apabila sistem atau Aplikasi tidak memungkinkan; dan
   3) untuk sistem yang tidak dimungkinkan mengikuti penggunaan *password* yang berkualitas harus mendapatkan persetujuan dari pimpinan unit kerja yang mempunyai tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi dengan mempertimbangkan kendala dan Risiko yang ada.
d. *password* tidak boleh sama dengan *User* ID dan tidak berdasar pada sesuatu yang mudah ditebak misalnya: nama, nomor telepon, tanggal lahir, nama anggota keluarga, nama/identitas perusahaan.

e. mengganti *password* secara reguler selama 3 (tiga) bulan dengan menghindari menggunakan *password* yang sudah pernah digunakan.
f. setiap pengguna wajib menjaga kerahasiaan *password* dan tidak diperkenankan memberikan *password* kepada orang lain dan/atau menggunakan *password* milik orang lain.
g. dalam 3 (tiga) bulan, setiap pengguna wajib melakukan akses minimal 1 (satu) kali agar akses pengguna tersebut tidak dinonaktifkan.

Paragraf 4
Keamanan Kriptografi

Pasal 15

(1) Keamanan kriptografi sebagaimana dimaksud dalam Pasal 11 huruf d, dilaksanakan untuk memastikan penggunaan kriptografi yang tepat guna melindungi kerahasiaan, keutuhan, dan keotentikan Data dan informasi rahasia dan/atau sangat rahasia yang dikelola dalam perangkat Informasi.
(2) Keamanan kriptografi untuk Informasi rahasia dan/atau sangat rahasia dilaksanakan oleh Tim SMKI bekerja sama dengan unit kerja terkait 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 Informasi berklasifikasi rahasia dan/atau sangat rahasia.
(3) Penerapan keamanan kriptografi sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan dengan cara:
   a. menerapkan jalur komunikasi aman dengan menerapkan *Secure Socket Layer* (SSL) untuk proses otentikasi antara pengguna dengan Aplikasi berbasis *website*;
   b. menjaga kerahasiaan kata sandi dan menyimpannya dalam basis Data dengan mekanisme *hash function*;
   c. melindungi Data dan Informasi dengan klasifikasi rahasia dan/atau sangat rahasia yang dipertukarkan, dikirimkan, dan disimpan dalam basis Data dengan melakukan enkripsi;
   d. menerapkan otentikasi berbasis tanda tangan digital dengan menggunakan Sertifikat Elektronik yang dikeluarkan oleh Pihak Ketiga terpercaya; dan
   e. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan dan/atau rekomendasi dari lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

Paragraf 5
Keamanan Fisik dan Lingkungan

Pasal 16

(1) Keamanan fisik dan lingkungan sebagaimana dimaksud dalam Pasal 11 huruf e, dilakukan untuk memberikan pelindungan, pemeliharaan, keamanan, dan ketersediaan Aset Informasi.

(2) Keamanan fisik dan lingkungan sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Tim SMKI bekerja sama dengan unit kerja terkait dengan cara:
   a. menyimpan infrastruktur di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai;
   b. membatasi akses ke Pusat Data dan/atau Tempat Layanan Informasi yang berisi Data dan/atau Informasi rahasia dan/atau sangat rahasia dan hanya diberikan kepada pegawai yang memiliki akses;
   c. mendampingi Pihak Ketiga yang memasuki Pusat Data dan/atau Tempat Layanan Informasi yang berisikan Data dan/atau Informasi rahasia dan/ atau sangat rahasia oleh pegawai yang ditugaskan sepanjang waktu kunjungan;
   d. melarang membawa makanan dan minuman ke dalam ruang Pusat Data;
   e. melakukan pengawasan terhadap kondisi suhu dan kelembapan sesuai batas minimum dan maksimum di dalam ruang *server* sesuai standar yang disyaratkan pabrikan perangkat;
   f. melakukan pengamanan area Pusat Data dan/atau Tempat Layanan Informasi sesuai prosedur keamanan area;
   g. melakukan pengamanan kantor, ruangan, dan fasilitas kerja sesuai dengan peraturan dan standar keamanan dan keselamatan kerja, termasuk *clear screen policy* dan *clean desk policy*;
   h. melakukan pemeliharaan infrastruktur yang digunakan untuk menjalankan Aplikasi sesuai dengan buku petunjuk;
   i. melakukan pemindahan infrastruktur yang tidak dapat dilakukan pemeliharaan di tempat, berdasarkan persetujuan pejabat pimpinan tinggi pratama yang mempunyai tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi;
   j. melakukan *backup* Data dan/atau Informasi berklasifikasi rahasia dan/atau sangat rahasia yang tersimpan pada perangkat ke media lain saat dilakukan pemindahan infrastruktur penyimpanan;
   k. menghindari kerusakan dari hama dan bencana alam terhadap infrastruktur beserta perangkat pemulihan dan media penyimpanan Data cadangan dengan diletakkan di tempat yang aman dengan struktur yang memadai;
   l. menyediakan pasokan daya yang sesuai dengan spesifikasi yang disyaratkan oleh pabrikan infrastruktur;

m. menyediakan sumber daya listrik alternatif yang digunakan untuk mengoperasikan infrastruktur dengan daya dan jangka waktu ketersediaan atau jangka waktu pengoperasian yang cukup tanpa gangguan terhadap infrastruktur;
n. menyimpan bahan berbahaya dan/atau mudah terbakar pada jarak yang aman dari Pusat Data dan Tempat Layanan Informasi;
o. menyediakan, memelihara, dan meletakkan perangkat pemadam kebakaran di tempat yang mudah dijangkau;
p. membatasi pihak yang tidak berwenang pada lokasi infrastruktur dan Informasi sensitif;
q. menerapkan perangkat perlindungan petir untuk semua bangunan, jalur komunikasi, dan listrik; dan
r. melakukan pengamanan kabel di Pusat Data dan/atau Tempat Layanan Informasi.

(3) Penyimpanan infrastruktur di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai sebagaimana dimaksud pada ayat (2) huruf a antara lain:
a. pintu dengan kontrol akses;
b. kamera pengawas;
c. pendeteksi asap;
d. sistem pemadam kebakaran; dan
e. perangkat pemutus aliran listrik.

(4) Pengamanan kabel di Pusat Data dan/atau Tempat Layanan Informasi sebagaimana dimaksud pada ayat (2) huruf r meliputi:
a. kabel listrik dan jaringan komunikasi harus terlindungi dan tidak diletakkan di area publik;
b. pemisahan antara kabel listrik dengan kabel Data; dan
c. penandaan kabel untuk mempermudah penanganan apabila terjadi masalah, menghindari kesalahan, dan didokumentasikan dengan baik.

(5) Dalam hal pemeliharaan dilakukan oleh Pihak Ketiga, maka pelaksanaannya dilakukan dengan membuat perjanjian kerja sama yang paling sedikit memuat:
a. perjanjian menjaga kerahasiaan;
b. pemeliharaan yang disediakan; dan
c. tingkat kinerja yang harus dipenuhi Pihak Ketiga.

Paragraf 6
Keamanan Operasional

Pasal 17

(1) Keamanan operasional sebagaimana dimaksud dalam Pasal 11 huruf f, dilakukan untuk memastikan implementasi, operasional, pemeliharaan yang aman dari Aset Informasi, pengelolaan layanan oleh Pihak Ketiga, meminimalkan Risiko kegagalan, dan melindungi keutuhan dan ketersediaan Aset Informasi.

(2) Keamanan operasional dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait dengan cara:

a. mendokumentasikan, memelihara, dan menyediakan prosedur penggunaan perangkat Informasi sesuai dengan peruntukannya;
b. mengelola dan mengendalikan perubahan dalam infrastruktur TIK dan sistem Aplikasi sesuai dengan prosedur manajemen perubahan;
c. menetapkan kriteria penerimaan untuk sistem Informasi baru, pemutakhiran dan versi baru, serta melakukan pengujian sebelum penerimaan;
d. memantau penggunaan Aset Informasi yang dimiliki dan membuat proyeksi kebutuhan ke depan untuk menjamin ketersediaan Aset Informasi yang dibutuhkan;
e. memonitor dan mengevaluasi kapasitas dan ketersediaan Aset Informasi yang kritikal;
f. melakukan pemisahan akses terhadap Informasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia;
g. memisahkan lingkungan pengembangan, pengujian, dan operasional untuk mengurangi Risiko perubahan atau akses oleh pihak yang tidak berhak terhadap sistem operasional;
h. menerapkan sistem pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman *malware*;
i. melakukan perlindungan dengan cara memasang perangkat *firewall, Intrusion Prevention System* (IPS), antivirus, perangkat manajemen akses pengguna, dan perangkat monitoring/pendukung lainnya sesuai perkembangan teknologi Keamanan Informasi;
j. melakukan pembuatan *backup* informasi dan Aplikasi yang berada di Pusat Data dan/atau Tempat Layanan Informasi secara berkala sesuai dengan prosedur *backup*;
k. mengambil dan menguji secara berkala salinan cadangan Data dan/atau Informasi, Aplikasi, dan *image* sistem;
l. mencatat (*logging*) setiap aktivitas administrator, aktivitas pengguna, peristiwa kegagalan, dan kejadian keamanan serta disimpan dalam periode tertentu;
m. melindungi sistem pencatatan (*log*) dari pemalsuan dan akses yang tidak berwenang;
n. melakukan penilaian kerentanan terhadap perangkat informasi (*vulnerability assessment*) secara berkala;
o. melakukan tindakan perlindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi;
p. menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindak pengamanan yang tepat;
q. memastikan semua perangkat pengolah Informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati; dan
r. menerapkan audit terhadap *log* yang mencatat aktivitas pengguna dan kejadian Keamanan Informasi

dalam kurun waktu tertentu untuk membantu investigasi di masa mendatang.

(3) Penerapan audit terhadap *log* sebagaimana dimaksud dalam ayat (2) huruf r untuk mengetahui:
   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 7
Keamanan Komunikasi

Pasal 18

(1) Keamanan komunikasi sebagaimana dimaksud dalam Pasal 11 huruf g, dilakukan untuk memastikan keamanan pertukaran Informasi melalui jaringan komunikasi.

(2) Keamanan komunikasi dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait 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. melakukan pemantauan serta pencatatan kegiatan penggunakan jaringan kepada Pihak Ketiga yang diberikan izin mengakses jaringan;
   c. melindungi jaringan dari pihak yang tidak berhak mengakses;
   d. menerapkan mekanisme kriptografi untuk melindungi informasi yang terdapat dalam Aplikasi yang melewati jaringan publik dari upaya pengungkapan, modifikasi, dan perusakan;
   e. melakukan pendeteksian dan perlindungan terhadap kode berbahaya (*malicious code*) yang disisipkan pada file yang dikirim melalui Sistem Elektronik;
   f. memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan untuk Informasi elektronik berklasifikasi rahasia dan/atau sangat rahasia; dan
   g. menetapkan prosedur pertukaran Informasi yang mengatur sistem dan keamanan yang digunakan untuk pertukaran Informasi.

(3) Pelindungan jaringan dari pihak yang tidak berhak mengakses sebagaimana dimaksud pada ayat (2) huruf c paling sedikit dilaksanakan dengan cara:
   a. mendokumentasikan arsitektur jaringan yang meliputi seluruh komponen infrastruktur dan Aplikasi jaringan;
   b. menerapkan teknologi keamanan jaringan berbasis enkripsi dan otentikasi (termasuk Sertifikat Elektronik);
   c. menerapkan pemisahan jaringan untuk kelompok pengguna, layanan Informasi, dan sistem Informasi;
   d. menerapkan parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan; dan

e. menerapkan prosedur penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau Aplikasi.

Paragraf 8
Keamanan Pengembangan dan Pemeliharaan

Pasal 19

(1) Keamanan pengembangan dan pemeliharaan sistem sebagaimana dimaksud dalam Pasal 11 huruf h, dilakukan untuk memastikan bahwa 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) Keamanan pengembangan dan pemeliharaan dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait dengan cara:
   a. memisahkan lingkungan pengembangan, pengujian, dan operasional Aplikasi baik secara fisik, *logic*, maupun aksesnya;
   b. menjaga agar lingkungan pengembangan tidak boleh diakses dari sistem operasional layanan;
   c. mengupayakan lingkungan pengujian sama dengan lingkungan operasional layanan;
   d. memilih Data uji dengan hati-hati, melindungi, dan mengendalikannya;
   e. mengawasi dan memantau aktivitas pembangunan dan/atau pengembangan Aplikasi dan infrastruktur yang dialihdayakan pada Pihak Ketiga;
   f. memastikan bahwa dalam proses perencanaan, pembangunan, dan pengembangan Aplikasi dan Infrastruktur termasuk yang dilakukan oleh Pihak Ketiga, telah memasukkan fitur-fitur keamanan dalam spesifikasi Aplikasi dan Infrastruktur yang dibangun dan/atau dikembangkan;
   g. memasukkan fitur-fitur keamanan sesuai dengan standar keamanan relevan; dan
   h. melaksanakan uji kelaikan Aplikasi sebelum digunakan dan/atau sewaktu-waktu sesuai kebutuhan.

(3) Fitur-fitur keamanan yang sesuai dengan standar keamanan relevan sebagaimana dimaksud pada ayat (2) huruf g mencakup:
   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.

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

(5) Pelaksanaan uji kelaikan Aplikasi sebelum digunakan dan/atau sewaktu-waktu sesuai kebutuhan sebagaimana dimaksud pada ayat (2) huruf h mencakup aspek:

a. uji fungsi, bertujuan untuk memastikan Aplikasi yang dibangun dan/atau dikembangkan telah memenuhi fungsi-fungsi sesuai dengan dokumentasi terkait;
b. uji integrasi, bertujuan untuk memastikan Aplikasi yang dibangun dan/atau dikembangkan telah memenuhi kebutuhan dan persyaratan integrasi dengan Aplikasi, Data, serta komponen-komponen lain yang terkait;
c. uji beban, bertujuan untuk memastikan aplikasi yang dibangun dan/atau dikembangkan dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya; dan
d. uji keamanan, bertujuan untuk memastikan Aplikasi yang dibangun dan/atau dikembangkan dapat menjaga keamanan Data dan Informasi yang terkait dengannya.

(6) 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.

(7) 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.

(8) 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.

Paragraf 9
Keamanan Pihak Ketiga

Pasal 20

(1) Keamanan Pihak Ketiga sebagaimana dimaksud dalam Pasal 11 huruf i, dilakukan untuk memastikan perlindungan dari Aset Informasi yang dapat diakses oleh Pihak Ketiga.

(2) Keamanan Pihak Ketiga sebagaimana dimaksud pada ayat (1) dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait dengan cara:
a. melakukan pemeriksaan latar belakang Pihak Ketiga dengan tetap memperhatikan privasi dan perlindungan Data pribadi;
b. membuat dan meninjau ulang secara berkala perjanjian keamanan dengan Pihak Ketiga yang terlibat dalam penggunaan dan/atau pengelolaan Aset Informasi yang menyatakan tanggung jawab terhadap keamanan Aset Informasi;
c. memastikan secara berkala bahwa pengendalian Keamanan Informasi, definisi layanan, 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 kritikalitas, 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 akses Informasi yang dimiliki Pihak Ketiga apabila yang bersangkutan tidak lagi bekerja di BMKG;
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 Informasi 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. perlindungan atas Informasi rahasia dan/atau sangat rahasia dan hak kekayaan intelektual setiap pihak;
b. jaminan bahwa tidak terdapat *malicious code* dan *backdoor* pada Aset Informasi yang disediakan oleh Pihak Ketiga;
c. hak untuk melakukan audit dan memantau kegiatan yang melibatkan Informasi rahasia dan/atau sangat rahasia;
d. pengawasan atas akses terhadap Aset Informasi yang diberikan pada Pihak Ketiga;
e. pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan;
f. syarat untuk Informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian keamanan;
g. penggunaan jalur komunikasi yang aman untuk perpindahan Informasi antara BMKG dengan Pihak Ketiga; dan
h. menyerahkan kembali aset Informasi yang dikuasai Pihak Ketiga kepada Tim SMKI apabila sudah tidak menjadi bagian dalam pengelolaan Aset Informasi.

Paragraf 10
Manajemen Insiden Siber

Pasal 21

(1) Manajemen Insiden Siber dilaksanakan untuk mengendalikan Insiden Siber.
(2) Manajemen Insiden Siber sebagaimana dimaksud pada ayat (1) dilaksanakan oleh BMKG-CSIRT.
(3) BMKG-CSIRT sebagaimana dimaksud pada ayat (2) mempunyai tugas sebagai berikut:
    a. melakukan tindakan pencegahan Insiden Siber;
    b. melaksanakan prosedur penanganan Insiden Siber jika terjadi Insiden Siber;
    c. menyusun skenario penanganan Insiden Siber;
    d. melakukan simulasi berkala skenario penanganan Insiden Siber yang telah disusun;
    e. memberikan pelatihan terhadap sumber daya manusia yang terlibat dalam simulasi penanganan Insiden Siber sesuai skenario yang disusun;
    f. menjalankan program kesadaran ancaman dan penanganan Insiden Siber, serta ajakan peran aktif pada seluruh pegawai;
    g. memastikan tersedianya kontak pelaporan Insiden Siber yang dapat diakses oleh seluruh pegawai di lingkungan BMKG termasuk oleh Pihak Ketiga; dan
    h. melaksanakan pengukuran tingkat kematangan penanganan Insiden Siber secara berkala.
(4) Tindakan pencegahan Insiden Siber sebagaimana dimaksud pada ayat (3) huruf a paling sedikit meliputi:
    a. melakukan penilaian kerentanan dan/atau *penetration testing* untuk menemukan celah keamanan pada Aset Informasi;
    b. mengimplementasikan alat *monitoring* keamanan berupa *Security Information and Event Management* (SIEM); dan
    c. melakukan *monitoring* dan pendeteksian serangan terhadap Aset Informasi.
(5) Prosedur penyusunan skenario penanganan Insiden Siber sebagaimana dimaksud pada ayat (3) huruf c paling sedikit meliputi:
    a. menerima laporan dan mencatat Insiden Siber;
    b. mendeteksi Insiden Siber;
    c. memverifikasi laporan insiden siber dan mengumpulkan informasi awal;
    d. mengklasifikasi Insiden Siber berdasarkan jenis dan tingkat keparahannya;
    e. memberikan prioritas Insiden Siber berdasarkan dampak yang ditimbulkan;
    f. mengalokasikan sumber daya yang diperlukan dalam penanganan Insiden Siber;
    g. mengidentifikasi sumber serangan;
    h. menganalisis Informasi yang berkaitan dengan Insiden Siber;
    i. memprioritaskan penanganan insiden berdasarkan tingkat dampak;

j. memelihara artefak digital untuk keperluan investigasi;
k. menyusun laporan penanganan Insiden Siber; dan
l. mengevaluasi dan memperbaiki standar, prosedur, dan kontrol-kontrol Keamanan Informasi.

Paragraf 11
Manajemen Keberlangsungan Layanan Informasi

Pasal 22

(1) Manajemen keberlangsungan layanan Informasi dilakukan untuk menjamin ketersediaan layanan Informasi pada saat terjadi keadaan darurat.
(2) Manajemen keberlangsungan layanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Tim SMKI bekerja sama dengan unit terkait dengan cara:
   a. melakukan identifikasi Risiko terhadap keberlangsungan layanan Informasi;
   b. menyusun dan menerapkan rencana keberlangsungan layanan Informasi (*Business Continuity Planning)* untuk menjaga dan mengembalikan operasional Aset Informasi dalam jangka waktu yang disepakati serta tingkat keberlangsungan layanan Informasi yang dibutuhkan;
   c. melakukan uji coba rencana keberlangsungan layanan Informasi secara berkala; dan
   d. pelaksanaan pengelolaan layanan dilakukan sesuai dengan pedoman manajemen layanan SPBE yang ditetapkan oleh kementerian yang melaksanakan tugas di bidang komunikasi dan informatika.
(3) Dalam hal Aplikasi merupakan Aplikasi umum dan/atau Sistem Elektronik berkategori strategis, maka harus memiliki redundansi yang cukup untuk memenuhi ketersediaan layanan Informasi.
(4) Rencana keberlangsungan layanan Informasi sebagaimana dimaksud pada ayat (2) huruf b paling sedikit meliputi:
   a. prosedur keberlangsungan layanan Informasi pada saat keadaan darurat, Manajemen Risiko, analisis dampak kegiatan, pengembalian kondisi sebelum terjadi gangguan 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.

Paragraf 12
Pengendalian Kepatuhan

Pasal 23

(1) Pengendalian kepatuhan dilaksanakan untuk memastikan kepatuhan pegawai dan Pihak Ketiga dalam melaksanakan

Keamanan Informasi sesuai kontrak dan keselarasan dengan kebijakan Keamanan Informasi.

(2) Pengendalian kepatuhan Keamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait dengan cara:
   a. mengidentifikasi, mendokumentasikan, mereviu, dan memelihara regulasi, standar, dan prosedur Keamanan Informasi;
   b. memeriksa kepatuhan seluruh pegawai dan Pihak Ketiga terhadap regulasi, standar, dan prosedur Keamanan Informasi;
   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, *master disk*, dan buku manual;
   f. melakukan pemeriksaan bahwa tidak ada produk bajakan yang terinstal di BMKG;
   g. memastikan rekaman terlindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah, dan rilis tidak sah sesuai dengan persyaratan peraturan perundang-undangan, kontraktual, dan bisnis;
   h. memastikan pengamanan privasi dan Data pribadi yang dapat diidentifikasikan sesuai dengan persyaratan ketentuan peraturan perundang-undangan;
   i. memastikan kesesuaian penerapan kriptografi dengan ketentuan peraturan perundang-undangan; dan
   j. mereviu sistem Informasi secara berkala agar sesuai dengan kebijakan dan standar Keamanan Informasi.

Bagian Keenam
Audit Keamanan Informasi

Pasal 24

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

(2) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan melalui kegiatan Audit Internal Keamanan Informasi dan audit eksternal keamanan informasi.

(3) Audit Internal Keamanan Informasi dilaksanakan oleh unit kerja yang melaksanakan tugas di bidang pengawasan internal yang memiliki kompetensi memadai dan memiliki objektivitas serta imparsialitas (ketidakberpihakan) dalam melaksanakan Audit Internal Keamanan Informasi.

(4) Audit Internal Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan dengan cara:
   a. merencanakan, menetapkan, dan menjalankan program audit sesuai dengan pedoman Audit Internal Keamanan Informasi;
   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 SMKI dan Sekretaris Utama sebagai bahan evaluasi penerapan Kebijakan SMKI;
   e. menyimpan dan mendokumentasikan proses dan hasil audit internal 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.

(5) Program audit sebagaimana dimaksud pada ayat (4) 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.

(6) Audit Eksternal Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan oleh Pihak Ketiga sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Ketujuh
Evaluasi Kinerja dan Perbaikan Berkelanjutan Keamanan Informasi

Pasal 25

(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) Sekretaris Utama dengan dibantu Tim SMKI melakukan tinjauan manajemen Keamanan Informasi 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;
e. menganalisis efektifitas 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 26

(1) Tindak lanjut dari hasil tinjauan manajemen berupa perbaikan berkelanjutan.
(2) Tim SMKI 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 SMKI didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja Keamanan Informasi.

BAB III
KETENTUAN PENUTUP

Pasal 27

Peraturan Kepala Badan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 18 Oktober 2024

Plt. KEPALA BADAN METEOROLOGI, KLIMATOLOGI, DAN GEOFISIKA,
REPUBLIK INDONESIA,

Ttd.

DWIKORITA KARNAWATI

Salinan ini sesuai dengan aslinya,
Kepala Biro Hukum dan Organisasi

MOHAMAD MUSLIHHUDDIN