PERATURAN BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
NOMOR 1 TAHUN 2024
TENTANG
PENGELOLAAN INSIDEN SIBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 17 Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Pengelolaan Insiden Siber;

Mengingat :
1. Peraturan Presiden Nomor 28 tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);
2. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
3. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2021 Nomor 803) sebagaimana telah diubah dengan Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2023 tentang Perubahan atas Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2023 Nomor 544);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG PENGELOLAAN INSIDEN SIBER.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:
1. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.

2. Infrastruktur Informasi Vital yang selanjutnya disingkat IIV adalah Sistem Elektronik yang memanfaatkan teknologi informasi dan/atau teknologi operasional, baik berdiri sendiri maupun saling bergantung dengan Sistem Elektronik lainnya dalam menunjang sektor strategis, yang jika terjadi gangguan, kerusakan, dan/atau kehancuran pada infrastruktur dimaksud berdampak serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, atau perekonomian nasional.
3. Keamanan Siber adalah upaya adaptif dan inovatif untuk melindungi seluruh lapisan ruang siber, termasuk aset informasi yang ada di dalamnya, dari ancaman dan serangan siber, baik bersifat teknis maupun sosial.
4. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik.
5. Tim Tanggap Insiden Siber adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
6. Instansi Penyelenggara Negara adalah institusi legislatif, eksekutif, dan yudikatif di tingkat pusat dan daerah dan instansi lain yang dibentuk dengan peraturan perundang-undangan.
7. Orang adalah orang perseorangan, baik warga negara Indonesia, warga negara asing, maupun badan hukum.
8. Penyelenggara IIV adalah Instansi Penyelenggara Negara, badan usaha, dan/atau organisasi yang memiliki dan/atau mengoperasikan IIV.
9. Penyelenggara Sistem Elektronik adalah setiap Orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/ atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/ atau keperluan pihak lain.
10. Kementerian atau Lembaga adalah Instansi Penyelenggara Negara yang bertugas mengawasi dan mengeluarkan pengaturan terhadap sektornya.
11. Badan Siber dan Sandi Negara dan yang selanjutnya disebut Badan adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang Keamanan Siber dan sandi.
12. Kontrol Keamanan adalah tindakan pengendalian yang dilakukan oleh Penyelenggara IIV dalam mengelola risiko keamanan siber yang bentuknya dapat bersifat administratif, teknis, kebijakan manajemen, atau peraturan.

Pasal 2

Ruang lingkup Peraturan Badan ini meliputi:
a. Tim Tanggap Insiden Siber;
b. pelaporan Insiden Siber;
c. penanganan Insiden Siber; dan
d. pelaksanaan kesiapan terhadap Insiden Siber.

BAB II
TIM TANGGAP INSIDEN SIBER

Pasal 3

(1) Penanganan Insiden Siber dilaksanakan oleh Tim Tanggap Insiden Siber.
(2) Penanganan Insiden Siber sebagaimana dimaksud pada ayat (1) dilakukan melalui:
    a. penanggulangan dan pemulihan Insiden Siber;
    b. penyampaian informasi Insiden Siber kepada pihak terkait; dan
    c. diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber.
(3) Dalam melakukan penanganan Insiden Siber sebagaimana dimaksud pada ayat (2), Tim Tanggap Insiden Siber memiliki fungsi paling sedikit:
    a. pemberian peringatan terkait Keamanan Siber;
    b. perumusan panduan teknis penanganan Insiden Siber;
    c. pencatatan setiap laporan/aduan yang dilaporkan, pemberian rekomendasi langkah penanganan awal kepada pihak terdampak;
    d. pemilahan (*triage*) Insiden Siber sesuai dengan kriteria yang ditetapkan dalam rangka memprioritaskan Insiden Siber yang akan ditangani;
    e. penyelenggaraan koordinasi penanganan Insiden Siber kepada pihak yang berkepentingan; dan
    f. penyelenggaraan fungsi lainnya sesuai kebutuhan.
(4) Fungsi lainnya sebagaimana dimaksud pada ayat (3) huruf f dapat berupa:
    a. penanganan kerentanan Sistem Elektronik;
    b. penanganan artefak digital;
    c. pemberitahuan hasil pengamatan potensi ancaman;
    d. pendeteksian serangan;
    e. analisis risiko Keamanan Siber;
    f. konsultasi terkait kesiapan penanganan Insiden Siber; dan/atau
    g. pembangunan kesadaran dan kepedulian terhadap Keamanan Siber.

Pasal 4

Tim Tanggap Insiden Siber terdiri atas:
a. Tim Tanggap Insiden Siber nasional;
b. Tim Tanggap Insiden Siber sektoral; dan
c. Tim Tanggap Insiden Siber organisasi.

Pasal 5

(1) Badan membentuk Tim Tanggap Insiden Siber nasional sebagaimana dimaksud dalam Pasal 4 huruf a.
(2) Keanggotaan Tim Tanggap Insiden Siber nasional terdiri atas perwakilan:
    a. Badan;
    b. Kementerian atau Lembaga;
    c. Penyelenggara IIV; dan
    d. Penyelenggara Sistem Elektronik selain Penyelenggara IIV.

(3) Selain perwakilan unsur sebagaimana dimaksud pada ayat (2), Tim Tanggap Insiden Siber nasional dapat mengikutsertakan komunitas, ahli hukum, dan akademisi dalam keanggotaan sesuai dengan kebutuhan.

(4) Tim Tanggap Insiden Siber nasional sebagaimana dimaksud pada ayat (1) melaksanakan tugas dan menyelenggarakan fungsi sebagaimana dimaksud dalam Pasal 3 pada tingkat nasional.

(5) Dalam melaksanakan tugas dan menyelenggarakan fungsi sebagaimana dimaksud pada ayat (4), Tim Tanggap Insiden Siber nasional melakukan kegiatan:
   a. registrasi dan penerbitan surat tanda register Tim Tanggap Insiden Siber sektoral dan Tim Tanggap Insiden Siber organisasi;
   b. pembangunan dan pengelolaan pangkalan data Insiden Siber dari seluruh Tim Tanggap Insiden Siber yang teregister dan informasi mengenai Insiden Siber di tingkat nasional;
   c. penghubung dengan negara lain dalam penanganan Insiden Siber;
   d. penyusunan pilar strategi dan program kegiatan Tim Tanggap Insiden Siber nasional;
   e. forum analisis dan berbagi informasi Keamanan Siber dengan Tim Tanggap Insiden Siber yang teregistrasi; dan
   f. pembangunan program berbagi pengetahuan atau pengalaman terkait dengan penanganan Insiden Siber kepada seluruh Tim Tanggap Insiden Siber yang teregistrasi.

Pasal 6

(1) Kementerian atau Lembaga membentuk Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud dalam Pasal 4 huruf b.

(2) Keanggotaan Tim Tanggap Insiden Siber sektoral terdiri atas perwakilan:
   a. Kementerian atau Lembaga;
   b. Penyelenggara IIV; dan
   c. Penyelenggara Sistem Elektronik selain Penyelenggara IIV.

(3) Selain perwakilan unsur sebagaimana dimaksud pada ayat (2), Tim Tanggap Insiden Siber sektoral dapat mengikutsertakan komunitas, ahli hukum, dan akademisi dalam keanggotaan sesuai dengan kebutuhan.

(4) Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud pada ayat (1) melaksanakan tugas dan menyelenggarakan fungsi sebagaimana dimaksud dalam Pasal 3 pada tingkat sektoral.

(5) Dalam melaksanakan tugas dan menyelenggarakan fungsi sebagaimana dimaksud pada ayat (4), Tim Tanggap Insiden Siber sektoral melakukan kegiatan:
   a. forum analisis dan berbagi informasi Keamanan Siber dengan Tim Tanggap Insiden Siber di bawahnya; dan
   b. uji komunikasi dengan Tim Tanggap Insiden Siber organisasi yang ada di sektornya.

(6) Uji komunikasi sebagaimana dimaksud pada ayat (5) huruf b dilakukan dengan melakukan verifikasi kontak dan kelengkapan kontak.

Pasal 7

(1) Penyelenggara IIV membentuk Tim Tanggap Insiden Siber organisasi sebagaimana dimaksud dalam Pasal 4 huruf c.
(2) Tim Tanggap Insiden Siber organisasi sebagaimana dimaksud pada ayat (1) melaksanakan tugas dan menyelenggarakan fungsi sebagaimana dimaksud dalam Pasal 3 pada tingkat organisasi.
(3) Dalam melaksanakan tugas dan menyelenggarakan fungsi sebagaimana dimaksud pada ayat (2), Tim Tanggap Insiden Siber organisasi dapat menyelenggarakan kegiatan forum analisis dan berbagi informasi Keamanan Siber lintas sektor.

Pasal 8

(1) Setiap Penyelenggara Sistem Elektronik selain Penyelenggara IIV juga membentuk Tim Tanggap Insiden Siber organisasi.
(2) Ketentuan mengenai tugas Tim Tanggap Insiden Siber organisasi bagi Penyelenggara IIV sebagaimana dimaksud dalam Pasal 7 berlaku secara mutatis mutandis terhadap tugas Tim Tanggap Insiden Siber organisasi bagi Penyelenggara Sistem Elektronik selain Penyelenggara IIV.

Pasal 9

(1) Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud dalam Pasal 6, Tim Tanggap Insiden Siber organisasi yang dibentuk oleh Penyelenggara IIV sebagaimana dimaksud dalam Pasal 7, dan Tim Tanggap Insiden Siber organisasi yang dibentuk oleh Penyelenggara Sistem Elektronik selain Penyelenggara IIV sebagaimana dimaksud dalam Pasal 8 wajib melakukan registrasi kepada Tim Tanggap Insiden Siber nasional.
(2) Registrasi sebagaimana dimaksud pada ayat (1) bertujuan:
    a. mendapatkan informasi yang valid mengenai profil Tim Tanggap Insiden Siber sektoral dan Tim Tanggap Insiden Siber organisasi;
    b. mempermudah koordinasi pada saat penanganan Insiden Siber antar Tim Tanggap Insiden Siber; dan
    c. mempermudah penyampaian informasi terkait ancaman, kerentanan, serta serangan siber kepada pihak yang berkepentingan.

Pasal 10

Registrasi sebagaimana dimaksud dalam Pasal 9 ayat (1) terdiri atas tahapan:
a. pengajuan permohonan;
b. validasi permohonan; dan
c. penerbitan surat tanda register.

Pasal 11

(1) Pengajuan permohonan registrasi sebagaimana dimaksud dalam Pasal 10 huruf a disampaikan oleh Tim Tanggap Insiden Siber sektoral dan Tim Tanggap Insiden Siber organisasi kepada Tim Tanggap Insiden Siber nasional.
(2) Permohonan registrasi sebagaimana dimaksud pada ayat (1) dilakukan dengan mengisi formulir registrasi dan melampirkan:
    a. dokumen yang memuat profil Tim Tanggap Insiden Siber sesuai format *request for comment* 2350;
    b. dokumen legal yang memuat pembentukan atau pelaksanaan tugas Tim Tanggap Insiden Siber;
    c. data aset elektronik yang dapat diakses publik milik konstituen Tim Tanggap Insiden Siber, termasuk di dalamnya nama aset publik, alamat IP, dan nama domain; dan
    d. data kompetensi sumber daya manusia Tim Tanggap Insiden Siber.
(3) Formulir registrasi sebagaimana dimaksud pada ayat (2) paling sedikit memuat:
    a. jenis Tim Tanggap Insiden Siber
    b. nama Tim Tanggap Insiden Siber; dan
    c. pihak yang menerima layanan.

Pasal 12

(1) Tim Tanggap Insiden Siber nasional melakukan validasi terhadap permohonan registrasi sebagaimana dimaksud dalam Pasal 11 ayat (1).
(2) Validasi permohonan registrasi sebagaimana dimaksud dalam Pasal 10 huruf b dilakukan dengan:
    a. memeriksa kelengkapan dan kesesuaian berkas permohonan sesuai ketentuan sebagaimana dimaksud dalam Pasal 11; dan
    b. melakukan uji komunikasi.
(3) Berdasarkan hasil validasi sebagaimana dimaksud pada ayat (2), permohonan registrasi dinyatakan tidak valid jika:
    a. berkas permohonan dinyatakan belum lengkap dan belum sesuai; dan/atau
    b. uji komunikasi gagal.
(4) Dalam hal permohonan registrasi dinyatakan tidak valid sebagaimana dimaksud pada ayat (3), Tim Tanggap Insiden Siber pemohon melengkapi kekurangan atau memperbaiki berkas permohonan dan/atau melaksanakan uji komunikasi ulang paling lama 10 (sepuluh) hari kerja sejak diberikannya hasil validasi.
(5) Dalam hal berdasarkan hasil validasi permohonan registrasi dinyatakan valid, Tim Tanggap Insiden Siber nasional memberikan surat tanda register kepada pemohon.
(6) Pelaksanaan validasi sampai dengan dikeluarkan surat tanda register dilakukan dalam jangka waktu paling lama 21 (dua puluh satu) hari kerja sejak berkas permohonan diterima.

Pasal 13

(1) Surat tanda register sebagaimana dimaksud dalam Pasal 10 huruf c diterbitkan oleh Tim Tanggap Insiden Siber nasional.
(2) Surat tanda register sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
    a. nomor register;
    b. jenis Tim Tanggap Insiden Siber;
    c. nama Tim Tanggap Insiden Siber;
    d. tanggal penerbitan surat tanda register; dan
    e. masa berlaku surat tanda register.
(3) Masa berlaku surat tanda register sebagaimana dimaksud pada ayat (2) huruf e, yakni:
    a. 5 (lima) tahun bagi Tim Tanggap Insiden Siber sektoral; atau
    b. 3 (tiga) tahun bagi Tim Tanggap Insiden Siber organisasi;

    sejak tanggal diterbitkannya surat tanda register.

Pasal 14

Tim Tanggap Insiden Siber sektoral atau Tim Tanggap Insiden Siber organisasi harus mengajukan permohonan registrasi ulang dalam hal:

a. telah habis masa berlaku surat tanda register; atau
b. terdapat perubahan:
    1. organisasi yang mengakibatkan perubahan Tim Tanggap Insiden Siber organisasi; atau
    2. sektor yang mengakibatkan perubahan Tim Tanggap Insiden Siber sektoral.

BAB III
PELAPORAN INSIDEN SIBER

Pasal 15

(1) Setiap Insiden Siber wajib dilaporkan oleh Tim Tanggap Insiden Siber organisasi kepada Tim Tanggap Insiden Siber sektoral dengan tembusan kepada Tim Tanggap Insiden Siber nasional.
(2) Insiden Siber sebagaimana dimaksud pada ayat (1) ditentukan berdasarkan:
    a. hasil deteksi Tim Tanggap Insiden Siber;
    b. analisis Insiden Siber berdasarkan aduan dari pemilik sistem atau masyarakat; dan/atau
    c. pemberian peringatan dari Tim Tanggap Insiden Siber nasional setelah terkonfirmasi sebagai Insiden Siber.
(3) Insiden Siber yang dilaporkan sebagaimana dimaksud pada ayat (1) merupakan Insiden Siber yang paling sedikit mempunyai risiko tinggi.
(4) Laporan Insiden Siber sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
    a. informasi kontak pelapor;
    b. deskripsi Insiden Siber;
    c. kronologi Insiden Siber; dan
    d. dampak serangan.

(5) Dalam hal Insiden Siber terjadi pada IIV lingkup organisasinya, Tim Tanggap Insiden Siber organisasi wajib melaporkan Insiden Siber tersebut kepada Tim Tanggap Insiden Siber sektoral dengan tembusan kepada Tim Tanggap Insiden Siber nasional paling lambat 1 x 24 (satu kali dua puluh empat) jam setelah ditemukan adanya Insiden Siber pada IIV.

(6) Dalam hal Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud pada ayat (5) belum terbentuk, Tim Tanggap Insiden Siber organisasi wajib melaporkan Insiden Siber yang terjadi pada IIV lingkup organisasinya kepada Kementerian atau Lembaga sesuai sektornya dengan tembusan kepada Tim Tanggap Insiden Siber nasional paling lambat 1 x 24 (satu kali dua puluh empat) jam setelah ditemukan adanya Insiden Siber pada IIV.

(7) Insiden Siber yang dilaporkan sebagaimana dimaksud pada ayat (1) mengacu kepada hasil penerapan manajemen risiko pada organisasinya.

(8) Hasil penerapan manajemen risiko sebagaimana dimaksud pada ayat (7) berupa hasil analisis risiko berdasarkan dampak Insiden Siber yang ditimbulkan.

BAB IV
PENANGANAN INSIDEN SIBER

Bagian Kesatu
Penanganan Insiden Siber pada Penyelenggara IIV

Pasal 16

(1) Penanganan Insiden Siber sebagaimana dimaksud dalam Pasal 3 oleh Tim Tanggap Insiden Siber organisasi Penyelenggara IIV dilakukan terhadap Insiden Siber yang mengakibatkan gangguan pada keberlangsungan layanan Sistem Elektronik Penyelenggara IIV.

(2) Dalam hal diperlukan, Tim Tanggap Insiden Siber sektoral dan/atau Tim Tanggap Insiden Siber nasional memberikan bantuan atau mengoordinasikan bantuan dalam rangka penanganan Insiden Siber pada IIV berdasarkan laporan sebagaimana dimaksud dalam Pasal 15 ayat (5).

(3) Dalam hal diperlukan, Tim Tanggap Insiden Siber nasional memberikan bantuan atau mengoordinasikan bantuan dalam rangka penanganan Insiden Siber pada IIV berdasarkan laporan sebagaimana dimaksud dalam Pasal 15 ayat (6).

Bagian Kedua
Penanganan Insiden Siber pada Penyelenggara Sistem Elektronik selain Penyelenggara IIV

Pasal 17

(1) Penanganan Insiden Siber sebagaimana dimaksud dalam Pasal 3 oleh Tim Tanggap Insiden Siber organisasi Penyelenggara Sistem Elektronik selain Penyelenggara IIV dilakukan terhadap Insiden Siber yang mengakibatkan gangguan pada keberlangsungan layanan Sistem

Elektronik miliknya.

(2) Berdasarkan laporan sebagaimana dimaksud dalam Pasal 15 ayat (1), penanganan Insiden Siber dilakukan oleh Tim Tanggap Insiden Siber sektoral dalam hal Insiden Siber mengakibatkan gangguan pada keberlangsungan layanan Sistem Elektronik pada paling sedikit 2 (dua) organisasi atau paling banyak setengah jumlah organisasi dalam lingkup 1 (satu) sektor.

(3) Berdasarkan laporan sebagaimana dimaksud dalam Pasal 15 ayat (1), penanganan Insiden Siber dilakukan oleh Tim Tanggap Insiden Siber nasional dalam hal Insiden Siber mengakibatkan gangguan pada keberlangsungan layanan Sistem Elektronik pada:
   a. paling sedikit 2 (dua) sektor dengan jumlah paling sedikit 2 (dua) organisasi yang terdampak di setiap sektor; atau
   b. lebih dari setengah jumlah organisasi dalam lingkup 1 (satu) sektor.

Bagian Ketiga
Penanggulangan dan Pemulihan Insiden Siber

Pasal 18

(1) Penanggulangan dan pemulihan Insiden Siber merupakan fungsi yang bertujuan untuk mendukung kemampuan Penyelenggara IIV, Penyelenggara Sistem Elektronik selain Penyelenggara IIV, dan Tim Tanggap Insiden Siber dalam menyusun dokumen perencanaan penanggulangan dan pemulihan Insiden Siber, menerapkan aktivitas yang sesuai untuk mengambil tindakan terkait Insiden Siber yang terdeteksi, menahan meluasnya dampak dari Insiden Siber, memulihkan layanan yang terganggu karena Insiden Siber, serta mengurangi dampak dari Insiden Siber.

(2) Penanggulangan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (1) terdiri atas kategori kegiatan:
   a. menyusun perencanaan penanggulangan dan pemulihan Insiden Siber;
   b. menganalisis dan melaporkan Insiden Siber;
   c. melaksanakan penanggulangan dan pemulihan Insiden Siber; dan
   d. meningkatkan keamanan setelah terjadinya Insiden Siber.

(3) Kategori kegiatan menyusun perencanaan penanggulangan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (2) huruf a dilakukan oleh Penyelenggara IIV dan Penyelenggara Sistem Elektronik selain Penyelenggara IIV, terdiri atas subkategori kegiatan paling sedikit:
   a. menyusun dan menetapkan rencana tanggap Insiden Siber yang disetujui oleh pimpinan organisasi;
   b. menyusun dan menetapkan rencana keberlangsungan kegiatan yang disetujui oleh pimpinan organisasi;
   c. memastikan rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan dilaksanakan dan

disimulasikan secara berkala;

d. memastikan personel yang mengelola IIV dan Sistem Elektronik selain IIV mengetahui peran dan prosedur penanggulangan dan pemulihan sesuai rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan; dan

e. memastikan personel yang mengelola IIV dan Sistem Elektronik selain IIV memahami prosedur penggunaan rekam cadang.

(4) Kategori kegiatan menganalisis dan melaporkan Insiden Siber sebagaimana dimaksud pada ayat (2) huruf b dilakukan oleh Tim Tanggap Insiden Siber terdiri atas subkategori kegiatan paling sedikit:

a. mengumpulkan informasi kondisi terkini dari IIV dan Sistem Elektronik selain IIV baik dari hasil deteksi internal maupun sumber informasi eksternal;

b. mengidentifikasi dan menganalisis potensi dampak dari Insiden Siber;

c. memastikan Insiden Siber dikategorikan sesuai kriteria yang telah ditetapkan; dan

d. memastikan bahwa Insiden Siber dilaporkan kepada pihak yang terkait.

(5) Ketentuan mengenai pelaporan Insiden Siber sebagaimana dimaksud pada ayat (4) huruf d dilaksanakan berdasarkan ketentuan sebagaimana dimaksud dalam Pasal 15.

(6) Kategori kegiatan melaksanakan penanggulangan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (2) huruf c dilakukan oleh Tim Tanggap Insiden Siber terdiri atas subkategori kegiatan paling sedikit:

a. memastikan Insiden Siber diisolasi dan dimitigasi sesuai rencana tanggap Insiden Siber;

b. mengumpulkan dan memelihara bukti Insiden Siber dari IIV dan Sistem Elektronik selain IIV terdampak;

c. menginvestigasi dan eradikasi penyebab Insiden Siber;

d. mengoordinasikan dengan pihak terkait dalam rangka eskalasi penanggulangan Insiden Siber.

e. memastikan setiap aset informasi diperiksa keamanannya setelah penanganan Insiden Siber;

f. melaksanakan prosedur pencadangan dan pemulihan sistem dan data sesuai rencana keberlangsungan kegiatan;

g. menentukan dan menerapkan retensi terhadap hasil pencadangan yang sudah tidak terpakai sesuai ketentuan;

h. pengujian ulang terhadap fungsi vital dan fungsi pendukung untuk memastikan capaian pemulihan terpenuhi;

i. memastikan organisasi memiliki dan mengelola strategi komunikasi publik ketika terjadi Insiden Siber dan setelah penanggulangan serta pemulihan Insiden Siber; dan

j. penyampaian informasi penanggulangan dan pemulihan Insiden Siber kepada pihak terkait.

(7) Kegiatan meningkatkan keamanan setelah terjadinya Insiden Siber sebagaimana dimaksud pada ayat (2) huruf

d dilakukan oleh Penyelenggara IIV, Penyelenggara Sistem Elektronik selain Penyelenggara IIV, dan Tim Tanggap Insiden Siber terdiri atas subkategori kegiatan paling sedikit:

a. meninjau kembali efektifitas Kontrol Keamanan yang telah diterapkan;
b. mereviu dan/atau memperbarui dokumen rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan secara berkala;
c. mengumpulkan dan memelihara bukti hasil forensik digital; dan
d. meninjau efektivitas kinerja penanganan insiden yang dilakukan oleh tim tanggap Insiden Siber secara berkala.

(8) Panduan pelaksanaan penanggulangan dan pemulihan Insiden Siber sebagaimana dimaksud pada ayat (2) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 19

(1) Selain kegiatan sebagaimana dimaksud dalam Pasal 18 ayat (7), dalam meningkatkan keamanan setelah terjadinya Insiden Siber, Tim Tanggap Insiden Siber, Penyelenggara IIV, dan Penyelenggara Sistem Elektronik selain Penyelenggara IIV dapat melakukan kegiatan pembelajaran Insiden Siber.
(2) Pembelajaran Insiden Siber sebagaimana dimaksud pada ayat (1) dilakukan dengan melakukan reviu setelah terjadinya Insiden Siber.
(3) Reviu setelah terjadinya Insiden Siber sebagaimana dimaksud pada ayat (2) dilakukan untuk membahas paling sedikit:
    a. riwayat terjadinya Insiden Siber;
    b. peninjauan kembali efektivitas Kontrol Keamanan yang telah diterapkan;
    c. penilaian atas efektivitas kinerja Tim Tanggap Insiden Siber;
    d. koordinasi dan kerja sama yang perlu diperbaiki;
    e. teknis penanggulangan dan pemulihan Insiden Siber yang perlu diperbaiki;
    f. kebijakan penanggulangan dan pemulihan yang perlu diperbarui; dan/atau
    g. rencana tanggap Insiden Siber dan rencana keberlangsungan yang perlu diperbarui.
(4) Hasil pembelajaran Insiden Siber sebagaimana dimaksud pada ayat (1) disampaikan oleh Tim Tanggap Insiden Siber organisasi kepada Tim Tanggap Insiden Siber sektoral dengan tembusan kepada Tim Tanggap Insiden Siber nasional.
(5) Dalam hal Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud pada ayat (4) belum terbentuk, hasil pembelajaran Insiden Siber sebagaimana dimaksud pada ayat (1) disampaikan oleh Tim Tanggap Insiden Siber organisasi kepada Kementerian atau Lembaga sesuai sektornya dengan tembusan kepada Tim Tanggap Insiden Siber nasional.

(6) Hasil pembelajaran Insiden Siber sebagaimana dimaksud pada ayat (1) dapat disebarluaskan melalui mekanisme diseminasi informasi.

Bagian Keempat
Penyampaian Informasi Insiden dan Diseminasi Informasi

Pasal 20

(1) Tim Tanggap Insiden Siber melakukan penyampaian informasi Insiden Siber kepada pihak terdampak.
(2) Informasi Insiden Siber sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
    a. jenis indikasi Insiden Siber;
    b. kode distribusi informasi;
    c. sistem dan/atau aset terdampak; dan
    d. rekomendasi mitigasi.

Pasal 21

(1) Tim Tanggap Insiden Siber melakukan diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber.
(2) Diseminasi informasi untuk mencegah dan/atau mengurangi dampak dari Insiden Siber sebagaimana dimaksud pada ayat (1) menggunakan kode distribusi informasi.
(3) Kode distribusi informasi sebagaimana dimaksud pada ayat (2) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

BAB V
PELAKSANAAN KESIAPAN TERHADAP INSIDEN SIBER

Pasal 22

(1) Pelaksanaan kesiapan terhadap Insiden Siber sebagaimana dimaksud dalam Pasal 2 huruf d dilaksanakan oleh Penyelenggara IIV, Kementerian atau Lembaga, dan Badan.
(2) Pelaksanaan kesiapan terhadap Insiden Siber sebagaimana dimaksud pada ayat (1) dilaksanakan melalui kegiatan penyusunan perencanaan penanggulangan dan pemulihan Insiden Siber sebagaimana dimaksud dalam Pasal 18 ayat (3).

Pasal 23

(1) Setiap Penyelenggara Sistem Elektronik selain Penyelenggara IIV juga melaksanakan kesiapan terhadap Insiden Siber.
(2) Ketentuan mengenai tugas penyusunan pelaksanaan kesiapan Insiden Siber bagi Penyelenggara IIV sebagaimana dimaksud dalam Pasal 22 berlaku secara mutatis mutandis terhadap tugas penyusunan pelaksanaan kesiapan Insiden Siber bagi Penyelenggara Sistem Elektronik selain Penyelenggara IIV.

Pasal 24

(1) Rencana tanggap Insiden Siber sebagaimana dimaksud dalam Pasal 18 ayat (3) huruf a disusun untuk mempersiapkan penanganan berbagai jenis Insiden Siber yang mungkin terjadi.
(2) Rencana tanggap Insiden Siber sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
    a. tahapan penanganan Insiden Siber;
    b. jenis Insiden Siber yang ditangani;
    c. daftar peran dan tanggung jawab anggota Tim Tanggap Insiden Siber;
    d. daftar perangkat, teknologi, dan sumber daya yang diperlukan;
    e. daftar proses pemulihan jaringan dan data yang penting/kritikal; dan
    f. daftar pihak internal dan eksternal yang perlu dihubungi.
(3) Rencana tanggap Insiden Siber dievaluasi dan diperbarui secara berkala sesuai dengan kebutuhan.

Pasal 25

(1) Rencana keberlangsungan kegiatan sebagaimana dimaksud dalam Pasal 18 ayat (3) huruf b disusun untuk memastikan keberlangsungan kegiatan.
(2) Rencana keberlangsungan kegiatan sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
    a. daftar peran dan tanggung jawab anggota tim pelaksana rencana keberlangsungan kegiatan;
    b. strategi dan lini masa untuk memulihkan fungsi dan layanan bisnis sesuai kritikal/prioritas;
    c. daftar sumber daya utama, peralatan, dan staf yang dibutuhkan untuk menjalankan fungsi dan layanan bisnis kritikal/prioritas; dan
    d. tahapan dan lini masa untuk pemulihan penuh.
(3) Rencana keberlangsungan kegiatan dievaluasi dan diperbarui secara berkala sesuai dengan kebutuhan.

Pasal 26

(1) Rencana tanggap Insiden Siber sebagaimana dimaksud dalam Pasal 24 rencana keberlangsungan kegiatan sebagaimana dimaksud dalam Pasal 25 dilaksanakan dan disimulasikan secara berkala oleh Tim Tanggap Insiden Siber dan pemangku kepentingan.
(2) Simulasi tanggap Insiden Siber dan simulasi keberlangsungan kegiatan sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Penyelenggara IIV, Kementerian atau Lembaga, dan Badan paling sedikit 1 (satu) kali dalam 2 (dua) tahun.

BAB VI
KETENTUAN PERALIHAN

Pasal 27

(1) Tim Tanggap Insiden Siber organisasi dan Tim Tanggap Insiden Siber sektoral wajib mengajukan permohonan registrasi sebagaimana dimaksud dalam Pasal 11 paling

lambat 6 (enam) bulan sejak Peraturan Badan ini diundangkan.

(2) Tim Tanggap Insiden Siber organisasi dan Tim Tanggap Insiden Siber sektoral yang telah teregister sesuai ketentuan Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber, wajib melengkapi dan menyesuaikan berkas registrasinya sesuai ketentuan sebagaimana dimaksud dalam Pasal 11 ayat (2).

BAB VII
KETENTUAN PENUTUP

Pasal 28

Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud dalam Pasal 6 dan Tim Tanggap Insiden Siber organisasi Penyelenggara IIV sebagaimana dimaksud dalam Pasal 7 dibentuk paling lambat 6 (enam) bulan sejak Peraturan Badan ini diundangkan.

Pasal 29

Pada saat Peraturan Badan ini mulai berlaku, Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber (Berita Negara Republik Indonesia Tahun 2020 Nomor 1488), dicabut dan dinyatakan tidak berlaku.

Pasal 30

Peraturan Badan ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Jakarta
pada tanggal 10 Januari 2024

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 18 Januari 2024

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

ttd.

ASEP N. MULYANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2024 NOMOR 43

LAMPIRAN
PERATURAN BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
NOMOR 1 TAHUN 2024
TENTANG PENGELOLAAN INSIDEN SIBER

PANDUAN PENGELOLAAN INSIDEN SIBER

A. Pelaksanaan Penanggulangan dan Pemulihan Insiden Siber
   1. Menyusun perencanaan penanggulangan dan pemulihan Insiden Siber.
      Kegiatan yang dilakukan meliputi:
      a. menyusun dan menetapkan rencana tanggap Insiden Siber yang disetujui oleh pimpinan organisasi.
         Pada kegiatan ini dilakukan hal-hal sebagai berikut:
         1) menentukan dan menetapkan prosedur tanggap insiden siber yang mencakup tindakan yang harus dilakukan termasuk pembagian peran antara pihak manajemen, personel pengelola IIV dan Sistem Elektronik selain IIV, dan pihak lainnya;
         2) menyusun dan menetapkan prosedur rencana tanggap Insiden Siber mulai dari tahapan persiapan, identifikasi, kontainmen, eradiksi, pemulihan, dan peningkatan berkelanjutan;
         3) menentukan skenario Insiden Siber yang mungkin terjadi pada layanan IIV dan Sistem Elektronik selain IIV yang selanjutnya dituangkan dalam dokumen rencana tanggap Insiden Siber; dan
         4) memastikan rencana tanggap Insiden Siber dikomunikasikan kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan.

      b. menyusun dan menetapkan rencana keberlangsungan kegiatan yang disetujui oleh pimpinan organisasi.
         Pada kegiatan ini dilakukan hal-hal sebagai berikut:
         1) menentukan dan menetapkan daftar fungsi dan layanan vital bagi Penyelenggara IIV dan Sistem Elektronik selain IIV yang dilengkapi dengan peran dan tanggung jawab masing-masing pihak terkait;
         2) menentukan dan menetapkan strategi, tahapan, dan target waktu yang dibutuhkan dalam memulihkan dan menjalankan fungsi serta layanan vital secara penuh/kembali normal;
         3) menentukan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital; dan
         4) memastikan rencana keberlangsungan layanan dikomunikasikan kepada pihak yang berkepentingan sesuai ketentuan yang berlaku.

      c. memastikan rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan dilaksanakan dan disimulasikan secara berkala.
         Pada kegiatan ini dilakukan simulasi secara berkala terhadap rencana tanggap Insiden Siber dan rencana keberlangsungan

kegiatan berdasarkan prosedur yang telah dibuat pada tahap sebelumnya.

d. memastikan personel yang mengelola IIV dan Sistem Elektronik selain IIV mengetahui peran dan prosedur penanggulangan dan pemulihan sesuai rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan.
   Pada kegiatan ini dilakukan hal-hal sebagai berikut:
   1) menentukan dan menetapkan personel yang ditugaskan dalam tim tanggap Insiden Siber;
   2) memastikan personel mengetahui peran dan urutan pengoperasian;
   3) mengidentifikasi siapa saja pihak-pihak terkait dalam proses penanggulangan dan pemulihan Insiden Siber;
   4) mengembangkan dan mengelola aturan mengenai penerbitan dan distribusi informasi setelah terjadinya Insiden Siber.

e. memastikan personel yang mengelola IIV dan Sistem Elektronik selain IIV memahami prosedur penggunaan rekam cadang.
   Pada kegiatan ini personel melakukan prosedur rekam cadang untuk mengamankan aset informasi berupa sistem /data yang tersimpan di dalam sistem IIV dan Sistem Elektronik selain IIV serta memastikan media yang digunakan untuk menyimpan data telah diamankan.

2. Menganalisis dan melaporkan Insiden Siber.
   Kegiatan yang dilakukan meliputi:
   a. mengumpulkan informasi kondisi terkini dari IIV dan Sistem Elektronik selain IIV baik dari hasil deteksi internal maupun sumber informasi eksternal.
      Pada kegiatan ini dilakukan hal-hal sebagai berikut:
      1) Memeriksa hasil analisis deteksi peristiwa siber untuk mengetahui ada atau tidaknya anomali pada sistem; dan
      2) Mengumpulkan dan menganalisis laporan peristiwa siber yang diterima baik dari pengguna layanan maupun sumber eksternal organisasi.

   b. mengidentifikasi dan menganalisis potensi dampak dari Insiden Siber.
      Pada kegiatan ini dilakukan identifikasi dan analisis terhadap potensi dampak Insiden Siber pada layanan IIV dan Sistem Elektronik selain IIV, termasuk organisasi dan pihak terkait seperti mitra ketiga berdasarkan laporan lengkap Insiden Siber.
      Aktivitas yang dilakukan dalam kegiatan ini yaitu:
      1) melakukan konfirmasi terhadap orang yang terlibat dalam Insiden Siber dan sistem yang digunakan.
      2) melakukan deteksi sumber Insiden Siber:
         a) identifikasi informasi, dapat dilakukan dengan melihat lokasi, nomor serial, nomor model, *hostname*, MAC *address*, *IP address* dari komputer yang digunakan, *log* pada sistem operasi dan aplikasi;
         b) identifikasi insiden, dapat dilihat melalui beberapa cara seperti:
            i. Lihat IPS/IDS/Firewall pada jaringan yang memberikan peringatan saat terjadi intrusi pada jaringan;

ii. *Antimalware* memberi peringatan saat mendeteksi *host* / media yang terinfeksi malware;
iii. Administrator melihat adanya *file* baru yang mempunyai nama yang tidak biasa digunakan *(unusual character)*;
iv. *Log* pada aplikasi mencatat adanya tindakan percobaan login yang banyak dari IP address yang tidak diketahui; dan
v. Administrator melihat surat elektronik yang tertolak oleh sistem (*bounced email*) yang banyak dengan konten yang anomali *(suspicious content)*.

Analisis Insiden Siber dilakukan untuk mengetahui paling sedikit:
1) Sistem Elektronik yang terkena Insiden Siber.
Sistem Elektronik yang terkena Insiden Siber sebagaimana perlu diketahui kategori Sistem Elektroniknya.
2) Ruang lingkup dampak Insiden Siber.
Ruang lingkup dampak Insiden Siber diketahui untuk menentukan Tim Tanggap Insiden Siber yang terkait.
3) Pemrioritasan Insiden Siber.
Pemrioritasan Insiden Siber dilakukan dengan mempertimbangkan kategori Sistem Elektronik dan ruang lingkup dampak Insiden Siber.
4) Penyerang yang menyebabkan Insiden Siber.

c. memastikan Insiden Siber dikategorikan sesuai kriteria yang telah ditetapkan.
Pada kegiatan ini, laporan Insiden Siber dikumpulkan, dikategorisasikan, dan diprioritaskan sesuai dampak risiko terhadap organisasi.

d. memastikan bahwa Insiden Siber dilaporkan kepada pihak yang terkait.
Pada kegiatan ini dilakukan hal-hal sebagai berikut:
1) melaporkan informasi mengenai Insiden Siber kepada pihak yang berwenang sesuai dengan kriteria yang diterapkan oleh organisasi dan peraturan perundangan yang berlaku; dan
2) memastikan proses koordinasi dengan pemangku kepentingan dilakukan sesuai dengan rencana tanggap Insiden Siber.

3. Melaksanakan penanggulangan dan pemulihan Insiden Siber.
Kegiatan yang dilakukan meliputi:
a. memastikan Insiden Siber diisolasi dan dimitigasi sesuai rencana tanggap Insiden Siber.
Tujuan dari isolasi adalah untuk membatasi jangkauan dan skala Insiden Siber agar Insiden Siber tidak semakin memburuk. Informasi yang dikumpulkan pada fase ini cukup untuk menentukan akar masalah dari Insiden Siber.
Pada tahapan ini juga dilakukan penahanan *containment*. Tahap ini menyediakan waktu untuk mengembangkan strategi remediasi yang disesuaikan. Bagian penting dari penahanan *(containment)* adalah pengambilan keputusan (misalnya, mematikan sistem, memutusnya dari jaringan, menonaktifkan fungsi tertentu). Keputusan seperti itu lebih mudah dilakukan

jika ada strategi dan prosedur yang telah ditentukan.
Organisasi harus menetapkan risiko yang dapat diterima dalam menangani Insiden Siber dan mengembangkan strategi yang sesuai. Organisasi harus membuat strategi/prosedur penahanan terpisah untuk setiap jenis insiden utama, dengan kriteria yang didokumentasikan dengan jelas untuk memfasilitasi pengambilan keputusan. Prosedur *containment* dapat dilakukan dengan cara sebagai berikut:

1) isolasi sistem yang terkena insiden;
2) *backup data* yang berkaitan dengan insiden (misalnya hasil pengumpulan bukti berbentuk *log, screenshot,* dan lainnya);
3) identifikasi semua layanan *(service)* dan koneksi yang terhubung;
4) identifikasi metode penyerang ketika masuk ke sistem pertama kali, dengan melihat *log* pada sistem;
5) periksa kode-kode berbahaya yang ada dalam sistem; dan
6) lakukan pemantauan pada jaringan yang terkena Insiden Siber, jika terdapat paket yang dicurigai/anomali, segera blokir dan dokumentasikan (dapat dicatat sumber IP, bentuk paket, waktu, dan lainnya).

b. mengumpulkan dan memelihara bukti Insiden Siber dari Sistem Elektronik terdampak.
Pada kegiatan ini dilakukan hal-hal sebagai berikut:

1) mengategorikan informasi mengenai Insiden Siber yang terdeteksi dan menyimpannya sesuai ukuran dampak terkait keamanan, penyebab insiden, dan faktor lainnya yang diperlukan.
2) melakukan forensik digital terhadap aset informasi yang terdampak Insiden Siber untuk menemukenali penyebab Insiden Siber sesuai dengan ketentuan peraturan perundang-undangan.

c. menginvestigasi dan eradikasi penyebab Insiden Siber.
Pada kegiatan ini, seluruh komponen aset informasi yang terdampak insiden diperiksa. Investigasi dilakukan untuk menentukan penyebab dan gejala dari Insiden Siber. Beberapa hal yang bisa dilakukan, di antaranya:

1) mencari tanda dan sebab dari suatu Insiden Siber;
2) mencari tahu bagaimana serangan dieksekusi.

Penghapusan atau eradikasi Insiden Siber dilakukan untuk menghilangkan komponen Insiden Siber. Penghapusan Insiden Siber juga termasuk penghapusan kerentanan Sistem Elektronik yang menyebabkan terjadinya Insiden Siber. Penghapusan kerentanan Sistem Elektronik dilakukan untuk persiapan pemulihan Sistem Elektronik. Penghapusan dilakukan dengan beberapa cara seperti:

1) menentukan tanda dan sebab dari suatu Insiden Siber;
2) melakukan *restore backup* untuk mendapatkan *new fresh system*;
3) menghapus penyebab Insiden Siber, seperti *malware*;
4) menonaktifkan akun pengguna yang terkena Insiden Siber;
5) melalui *reset password* jika diperlukan;
6) melakukan mitigasi terhadap kerentanan yang tereksploitasi saat Insiden Siber;

7) selama eradikasi, sangat penting untuk mengidentifikasi semua *host* yang terkena Insiden Siber; dan
8) melakukan improvisasi pertahanan dan melakukan *vulnerability analysis* untuk melihat potensi ancaman yang dapat terjadi.

d. mengoordinasikan dengan pihak terkait dalam rangka eskalasi penanggulangan Insiden Siber.
Apabila kegiatan yang telah dijelaskan di atas sudah dilakukan namun Insiden Siber masih meningkat atau meluas, maka buat prosedur terkait eskalasi Insiden Siber.
Hal-hal yang bisa dimasukkan ke dalam prosedur eskalasi Insiden Siber yaitu:
1) melaporkan kepada Tim Tanggap Insiden Siber (TTIS) sektoral dan nasional; dan
2) menyiapkan informasi yang relevan terkait Insiden Siber yang terjadi.

Koordinasi Insiden Siber dilakukan guna:
1) Menentukan pihak yang dapat melakukan teknis penahanan dan penghapusan Insiden Siber, serta penghapusan kerentanan Sistem Elektronik.
2) Menentukan pemangku kepentingan yang perlu dilibatkan dalam penahanan dan eradikasi Insiden Siber, serta penghapusan kerentanan Sistem Elektronik.

Pihak yang dapat melakukan teknis dapat berupa:
1) Penyelenggara Sistem Elektronik;
2) Tim Tanggap Insiden Siber; dan/atau
3) Pihak lain yang memiliki kemampuan teknis yang dibutuhkan.

Kerjasama dengan pihak yang melakukan teknis dilakukan dengan memperhatikan kerahasiaan informasi, perlindungan data, dan sesuai dengan ketentuan peraturan perundangan-undangan.

e. memastikan setiap aset informasi diperiksa keamanannya setelah penanggulangan Insiden Siber.
Pada kegiatan ini, dilakukan pemeriksaan terhadap seluruh aset informasi yang berhubungan dengan Sistem Elektronik dan memastikannya bersih dari indikasi ancaman atau serangan yang telah terjadi.

f. melaksanakan prosedur pencadangan dan pemulihan sistem dan data sesuai rencana keberlangsungan kegiatan.
Pada kegiatan ini dilakukan hal-hal sebagai berikut:
1) melaksanakan prosedur pemulihan sistem/data dari media penyimpanan apabila terjadi keadaan darurat;
2) melaksanakan simulasi secara periodik terhadap prosedur pemulihan sistem/data dari media penyimpanan rekam cadang;
3) melakukan prosedur rekam cadang secara optimal dengan memanfaatkan perangkat-perangkat penyimpanan yang memiliki fitur *job-schedulling*;
4) melakukan enkripsi terhadap data yang disimpan pada media penyimpanan rekam cadang;
5) menentukan waktu pelaksanaan rekam cadang terhadap

data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi; dan
6) mendokumentasikan hasil pelaksanaan rekam cadang data.

g. menentukan dan menerapkan retensi terhadap hasil pencadangan yang sudah tidak terpakai sesuai ketentuan.
Pada kegiatan ini dilakukan hal-hal sebagai berikut:
1) memastikan media penyimpanan rekam cadang telah disimpan secara aman;
2) meminta persetujuan pimpinan organisasi sebelum melakukan pemusnahan terhadap data yang disimpan pada media rekam cadang; dan
3) melakukan format ulang media rekam cadang dan memastikan data sudah tidak dapat diakses lagi.

h. pengujian ulang terhadap fungsi vital dan fungsi pendukung untuk memastikan capaian pemulihan terpenuhi.
Setelah upaya pemulihan elektronik terdampak dilakukan, dilakukan kegiatan pengujian ulang terhadap fungsi vital dan fungsi pendukung untuk memastikan capaian pemulihan terpenuhi. Capaian pemulihan dinilai berdasarkan:
1) waktu pemulihan di bawah batas waktu maksimal yang ditetapkan berdasarkan rencana keberlangsungan kegiatan;
2) jumlah data yang terpulihkan sesuai dengan batas jumlah data minimal yang ditetapkan berdasarkan rencana keberlangsungan kegiatan; dan/atau
3) fungsi vital dan fungsi pendukung yang terpulihkan sesuai dengan batas fungsi vital dan fungsi pendukung minimal yang ditetapkan berdasarkan rencana keberlangsungan kegiatan.

i. memastikan organisasi memiliki dan mengelola strategi komunikasi publik ketika terjadi Insiden Siber dan setelah penanggulangan serta pemulihan Insiden Siber.
Pada kegiatan ini dilakukan hal-hal sebagai berikut:
1) menyusun dan menerapkan strategi komunikasi publik dalam hal mengelola informasi yang perlu disampaikan terkait Insiden Siber; dan
2) memastikan bahwa proses penanganan dan pemulihan insiden dikomunikasikan dengan pihak yang berkepentingan sesuai dengan peraturan perundangan.

j. penyampaian informasi penanggulangan dan pemulihan Insiden Siber kepada pihak terkait.
Pada kegiatan ini dilakukan penyusunan laporan hasil penanganan Insiden Siber dan menyampaikannya kepada Kementerian atau Lembaga di masing-masing sektor.

4. Meningkatkan keamanan setelah terjadinya Insiden Siber.
Kegiatan yang dilakukan meliputi:
a. meninjau kembali efektifitas kontrol keamanan yang telah diterapkan.
Pada kegiatan ini dilakukan evaluasi kontrol keamanan yang diterapkan apakah masih relevan terhadap spektrum ancaman yang ada atau perlu ada perbaikan dan penambahan.

b. mereviu dan/atau memperbarui dokumen rencana tanggap Insiden Siber dan rencana keberlangsungan kegiatan secara berkala.
Pada kegiatan ini dilakukan hal-hal sebagai berikut:
1) Melakukan reviu dan pembaharuan teradap spektrum ancaman yang ada atau perlu ada perbaikan dan penambahan.
2) Melakukan reviu dan pembaharuan terhadap dokumen rencana tanggap Insiden Siber dan pemulihan apabila terdapat hal-hal yang dapat dijadikan pembelajaran berkelanjutan bagi organisasi.

c. mengumpulkan dan memelihara bukti hasil forensik digital.
Pada kegiatan ini dilakukan hal-hal sebagai berikut:
1) Mengumpulan laporan hasil pelaksanaan forensik digital yang meliputi informasi-informasi yang relevan.
2) Menyampaikan laporan hasil pelaksanaan forensik digital kepada pihak berwajib untuk selanjutnya dilakukan proses investigasi dan penegakan hukum sesuai ketentuan yang berlaku.

d. meninjau efektivitas kinerja penanganan insiden yang dilakukan oleh tim tanggap insiden siber secara berkala.
Pada kegiatan ini dilakukan hal-hal sebagai berikut:
1) Melakukan peninjauan secara berkala terhadap efektifitas kinerja penganganan insiden.
2) Melakukan langkah-langkah perbaikan terhadap pelaksanaan penanganan Insiden Siber baik dari segi teknologi, tata Kelola, atau peningkatan kapasitas SDM.

B. Ketentuan Kode Distribusi Informasi pada Tim Tanggap Insiden Siber (TTIS)

Traffic Light Protocol (TLP) dibuat untuk memfasilitasi pembagian informasi sensitif untuk penerima informasi yang lebih luas dan kolaborasi yang lebih efektif. Berbagi informasi terjadi dari sumber informasi, kepada satu atau beberapa penerima. TLP adalah set yang terdiri atas empat label yang digunakan untuk menunjukkan batas pembagian yang akan diterapkan oleh penerima. Hanya label yang tercantum dalam standar ini yang dianggap valid oleh FIRST.

Empat label TLP adalah: TLP:RED, TLP:AMBER, TLP:GREEN, dan TLP:CLEAR. Dalam bentuk tulisan, keempat label TLP tersebut HARUS tidak mengandung spasi dan HARUS dalam huruf kapital. Label TLP HARUS tetap dalam bentuk aslinya, meskipun digunakan dalam bahasa lain.

Penggunaan:

1. Menggunakan TLP dalam sistem olah pesan.
Olah pesan berlabel TLP HARUS menunjukkan label TLP informasi yang dipertukarkan, serta batasan tambahan lainnya, langsung sebelum informasi itu sendiri ditunjukkan. Label TLP HARUS berada di baris subjek email. Jika diperlukan, pastikan juga untuk menandai bagian akhir teks yang akan diberi label TLP.
2. Menggunakan TLP dalam dokumen.
Dokumen berlabel TLP HARUS menunjukkan label TLP informasi, serta batasan tambahan apa pun, di header dan footer setiap halaman. Label TLP HARUS menggunakan huruf dengan jenis

ukuran 12 poin atau lebih besar untuk pengguna dengan gangguan penglihatan. Direkomendasikan untuk meletakan label TLP dengan format rata kanan.

3. Cara menggunakan TLP dalam pertukaran informasi otomatis.
   Penggunaan TLP dalam pertukaran informasi otomatis tidak ditentukan: ini diserahkan kepada perancang pertukaran tersebut, tetapi HARUS sesuai dengan standar ini.
   Kode warna TLP dalam RGB, CMYK dan Hex:

	RGB: font			RGB: background			CMYK: font				CMYK: background				Hex: font	Hex: background
	R	G	B	R	G	B	C	M	Y	K	C	M	Y	K		
TLP:RED	255	43	43	0	0	0	0	83	83	0	0	0	0	100	#FF2B2B	#000000
TLP:AMBER	255	192	0	0	0	0	0	25	100	0	0	0	0	100	#FFC000	#000000
TLP:GREEN	51	255	0	0	0	0	79	0	100	0	0	0	0	100	#33FF00	#000000
TLP:CLEAR	255	255	255	0	0	0	0	0	0	0	0	0	0	100	#FFFFFF	#000000

Catatan tentang pengkodean warna: ketika kontras warna antara teks dan latar belakang terlalu sedikit, mereka yang memiliki penglihatan rendah kesulitan membaca teks atau tidak dapat melihatnya sama sekali. TLP dirancang untuk mengakomodasi mereka yang memiliki penglihatan rendah. Sumber HARUS mematuhi kode warna TLP untuk memastikan kontras warna yang cukup untuk pembaca tersebut.

Definisi TLP:

a. Komunitas: Komunitas adalah grup yang memiliki tujuan, praktik, dan hubungan kepercayaan informal yang sama. Komunitas bisa jadi seluas semua praktisi keamanan siber di suatu negara (atau di suatu sektor atau wilayah).
b. Organisasi: Organisasi adalah grup yang memiliki afiliasi yang sama melalui keanggotaan formal dan terikat oleh kebijakan umum yang ditetapkan oleh organisasi. Sebuah organisasi bisa jadi seluas semua anggota organisasi berbagi informasi, tapi jarang lebih luas.
c. Klien: Klien adalah orang atau entitas yang menerima layanan keamanan siber dari organisasi. Klien secara default disertakan dalam TLP:AMBER sehingga penerima dapat berbagi informasi lebih jauh ke hilir agar klien dapat mengambil tindakan untuk melindungi diri mereka sendiri. Untuk tim dengan tanggung jawab nasional, definisi ini mencakup pemangku kepentingan dan konstituen.
d. Label TLP:
   1) TLP:RED = Untuk mata dan telinga penerima individu saja, tidak ada pengungkapan lebih lanjut. Sumber dapat menggunakan TLP:RED ketika informasi tidak dapat ditindaklanjuti secara efektif tanpa risiko signifikan terhadap privasi, reputasi, atau operasi organisasi yang terlibat. Oleh karena itu, penerima tidak boleh berbagi informasi TLP:RED dengan orang lain. Dalam konteks rapat, misalnya, informasi TLP:RED terbatas pada mereka yang hadir dalam rapat.
   2) TLP:AMBER = Pengungkapan terbatas, penerima hanya dapat menyebarkan ini berdasarkan kebutuhan untuk mengetahuinya dalam organisasi dan kliennya. Perhatikan bahwa

TLP:AMBER+STRICT membatasi berbagi hanya untuk organisasi. Sumber dapat menggunakan TLP:AMBER ketika informasi memerlukan dukungan untuk ditindaklanjuti secara efektif, namun membawa risiko terhadap privasi, reputasi, atau operasi jika dibagikan di luar organisasi yang terlibat. Penerima dapat membagikan informasi TLP:AMBER dengan anggota organisasi mereka sendiri dan kliennya, tetapi hanya berdasarkan kebutuhan untuk mengetahui guna melindungi organisasi mereka dan kliennya serta mencegah kerugian lebih lanjut. Catatan: jika sumber ingin membatasi berbagi hanya untuk organisasi, mereka harus menentukan TLP:AMBER+STRICT.

3) TLP:GREEN = Pengungkapan terbatas, penerima dapat menyebarkan ini dalam komunitasnya. Sumber dapat menggunakan TLP:GREEN ketika informasi berguna untuk meningkatkan kesadaran dalam komunitas mereka yang lebih luas. Penerima dapat berbagi informasi TLP:GREEN dengan rekan dan organisasi mitra dalam komunitas mereka, tetapi tidak melalui saluran yang dapat diakses publik. Informasi TLP:GREEN tidak boleh dibagikan di luar komunitas. Catatan: jika "komunitas" tidak ditentukan, asumsikan komunitas keamanan/pertahanan siber.
4) TLP:CLEAR = Penerima dapat menyebarkan ini ke seluruh dunia, tidak ada batasan pengungkapan. Sumber dapat menggunakan TLP:CLEAR ketika informasi membawa risiko penyalahgunaan minimal atau tidak dapat diperkirakan, sesuai dengan aturan dan prosedur yang berlaku untuk rilis publik. Tunduk pada aturan hak cipta standar, informasi TLP:CLEAR dapat dibagikan tanpa batasan.

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN