PERATURAN BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
NOMOR 2 TAHUN 2024
TENTANG
MANAJEMEN KRISIS SIBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 33 Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Manajemen Krisis 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 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 99);
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 MANAJEMEN KRISIS SIBER.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:
1. 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 yang bersifat teknis maupun sosial.

2. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya sistem elektronik.
3. Krisis Siber adalah situasi kedaruratan akibat dari Insiden Siber pada tingkat nasional yang berdampak terhadap keselamatan, keutuhan, dan kedaulatan negara.
4. Manajemen Krisis Siber adalah tata kelola penggunaan sumber daya dan langkah penanganan secara efektif yang dilakukan sebelum, saat, dan setelah terjadinya Krisis Siber.
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. Pemangku Kepentingan adalah para pihak yang memiliki peran dalam penerapan Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.
8. Penyelenggara Sistem Elektronik yang selanjutnya disingkat PSE 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.
9. Peristiwa Siber adalah kejadian pada sistem elektronik yang dapat diobservasi dan dapat memberikan indikasi terhadap terjadinya Insiden Siber.
10. Badan Siber dan Sandi Negara yang selanjutnya disebut Badan adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan sandi.

Pasal 2

Ruang lingkup Peraturan Badan ini meliputi:
a. persiapan penyelenggaraan Manajemen Krisis Siber; dan
b. penyelenggaraan Manajemen Krisis Siber.

BAB II
PERSIAPAN PENYELENGGARAAN MANAJEMEN KRISIS SIBER

Pasal 3

Persiapan penyelenggaraan Manajemen Krisis Siber sebagaimana dimaksud dalam Pasal 2 huruf a meliputi:
a. penyusunan rencana kontingensi Krisis Siber; dan
b. simulasi rencana kontingensi Krisis Siber.

Pasal 4

(1) Rencana kontingensi Krisis Siber sebagaimana dimaksud dalam Pasal 3 merupakan dokumen perencanaan yang disusun untuk menjadi acuan dalam meningkatkan kesiapsiagaan menghadapi Krisis Siber.

(2) Rencana kontingensi Krisis Siber sebagaimana dimaksud pada ayat (1) disusun dengan memperhatikan:
a. penilaian risiko Keamanan Siber nasional;
b. agenda prioritas nasional; dan/atau
c. lanskap Keamanan Siber.

(3) Rencana kontingensi Krisis Siber sebagaimana dimaksud pada ayat (1) memuat:
a. skenario ancaman;
b. karakteristik dan riwayat ancaman siber;
c. peran, tanggung jawab, dan pola komunikasi;
d. proses penanggulangan;
e. proses pemulihan;
f. pembiayaan; dan
g. pelaporan.

Pasal 5

(1) Rencana kontingensi Krisis Siber sebagaimana dimaksud dalam Pasal 3 disusun oleh Badan dengan mengikutsertakan Instansi Penyelenggara Negara.

(2) Selain Instansi Penyelenggara Negara sebagaimana dimaksud pada ayat (1), Badan dalam menyusun rencana kontingensi Krisis Siber dapat mengikutsertakan:
a. Tim Tanggap Insiden Siber nasional;
b. Tim Tanggap Insiden Siber sektor; dan/atau
c. Pemangku Kepentingan.

(3) Rencana kontingensi Krisis Siber ditetapkan oleh Kepala Badan.

Pasal 6

(1) Untuk memastikan aktualitas, validitas, dan kualitas rencana kontingensi Krisis Siber yang telah ditetapkan sebagaimana dimaksud dalam Pasal 5 ayat (3), Badan melakukan simulasi dengan cara:
a. latihan; dan
b. pemeranan.

(2) Latihan sebagaimana dimaksud pada ayat (1) huruf a dilaksanakan untuk menguji prosedur rencana kontingensi Krisis Siber yang bersifat teknis.

(3) Latihan sebagaimana dimaksud pada ayat (2) dilaksanakan melalui penyelenggaraan:
a. latihan teknis sektor tertentu;
b. latihan teknis fungsi tertentu;
c. latihan teknis menyeluruh; dan/atau
d. latihan teknis lainnya.

(4) Pemeranan sebagaimana dimaksud pada ayat (1) huruf b dilaksanakan untuk memberikan pengetahuan, pemahaman serta pengujian prosedur rencana kontingensi Krisis Siber dalam pengambilan keputusan yang bersifat manajerial.

(5) Pemeranan sebagaimana dimaksud pada ayat (4) dilaksanakan melalui penyelenggaraan:
a. seminar Krisis Siber;
b. lokakarya Krisis Siber; dan/atau
c. pemeranan pengambilan keputusan *(tabletop exercise)* Krisis Siber.

(6) Simulasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Badan paling sedikit 1 (satu) kali dalam 2 (dua) tahun.
(7) Dalam melakukan simulasi sebagaimana dimaksud pada ayat (1), Badan mengikutsertakan Instansi Penyelenggara Negara dan Pemangku Kepentingan.

Pasal 7

(1) Rencana kontingensi Krisis Siber sebagaimana dimaksud dalam Pasal 5 dievaluasi oleh Badan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau sewaktu-waktu sesuai kebutuhan.
(2) Dalam melakukan evaluasi sebagaimana dimaksud pada ayat (1), Badan mengikutsertakan Instansi Penyelenggara Negara.
(3) Badan dapat melakukan perubahan rencana kontingensi Krisis Siber berdasarkan hasil evaluasi sebagaimana dimaksud pada ayat (1).
(4) Penyusunan perubahan rencana kontingensi Krisis Siber sebagaimana dimaksud dalam ayat (3) dilakukan sesuai dengan ketentuan sebagaimana dimaksud dalam Pasal 5.

BAB III
PENYELENGGARAAN MANAJEMEN KRISIS SIBER

Pasal 8

(1) Penyelenggaraan Manajemen Krisis Siber sebagaimana dimaksud dalam Pasal 2 huruf b meliputi:
    a. sebelum Krisis Siber;
    b. saat terjadi Krisis Siber; dan
    c. setelah Krisis Siber.
(2) Penyelenggaraan Manajemen Krisis Siber sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Badan dengan mengikutsertakan PSE.

Pasal 9

Penyelenggaraan Manajemen Krisis Siber sebelum Krisis Siber sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf a diselenggarakan paling sedikit melalui:
a. tanggap Insiden Siber;
b. peringatan dini Krisis Siber; dan
c. penetapan status Krisis Siber.

Pasal 10

(1) Tanggap Insiden Siber sebagaimana dimaksud dalam Pasal 9 huruf a merupakan tindakan untuk merespons Insiden Siber yang terus meningkat dan berpotensi menjadi Krisis Siber.
(2) Pelaksanaan tanggap Insiden Siber sebagaimana dimaksud pada ayat (1) dilakukan secara bertahap oleh Tim Tanggap Insiden Siber organisasi, Tim Tanggap Insiden Siber sektor, dan Tim Tanggap Insiden Siber nasional.
(3) Pelaksanaan tanggap Insiden Siber sebagaimana dimaksud pada ayat (2) dilakukan sesuai dengan ketentuan peraturan perundang-undangan mengenai pengelolaan insiden siber.

Pasal 11

(1) Peringatan dini Krisis Siber sebagaimana dimaksud dalam Pasal 9 huruf b merupakan penyampaian peringatan oleh Tim Tanggap Insiden Siber nasional kepada PSE mengenai terjadinya eskalasi Insiden Siber yang mengarah menjadi Krisis Siber.
(2) Bentuk peringatan dini Krisis Siber sebagaimana dimaksud pada ayat (1) dapat berupa:
    a. notifikasi;
    b. dokumen imbauan keamanan; dan/atau
    c. informasi yang disampaikan melalui media berbagi informasi.
(3) PSE sebagaimana dimaksud pada ayat (1) wajib menindaklanjuti peringatan dini Krisis Siber.
(4) PSE melaporkan hasil tindak lanjut peringatan dini Krisis Siber kepada Tim Tanggap Insiden Siber nasional secara berkala setiap 2 (dua) jam atau sewaktu-waktu jika diperlukan setelah peringatan dini diterima oleh PSE.

Pasal 12

(1) Peringatan dini Krisis Siber sebagaimana dimaksud dalam Pasal 11 ayat (1) dilakukan berdasarkan hasil penilaian potensi Krisis Siber.
(2) Penilaian potensi Krisis Siber sebagaimana dimaksud pada ayat (1) dilakukan oleh Tim Tanggap Insiden Siber nasional terhadap:
    a. Insiden Siber; dan/atau
    b. Peristiwa Siber.
(3) Penilaian potensi Krisis Siber sebagaimana dimaksud pada ayat (2) dilakukan dengan memperhatikan potensi dampak terganggunya dan/atau terhentinya layanan sistem elektronik yang berdampak terhadap keselamatan, keutuhan, dan kedaulatan negara.
(4) Potensi dampak sebagaimana dimaksud pada ayat (3) ditentukan berdasarkan kriteria Krisis Siber paling sedikit:
    a. korban jiwa, hilang, dan terluka;
    b. kerugian finansial;
    c. kondisi keamanan dan ketertiban umum; dan/atau
    d. kerusakan pada infrastruktur informasi vital.
(5) Kriteria Krisis Siber sebagaimana dimaksud pada ayat (4) ditetapkan oleh Kepala Badan.
(6) Tim Tanggap Insiden Siber nasional melaporkan peringatan dini Krisis Siber sebagaimana dimaksud pada ayat (1) dan penilaian potensi Krisis Siber sebagaimana dimaksud pada ayat (2) kepada Kepala Badan

Pasal 13

(1) Penetapan status Krisis Siber sebagaimana dimaksud dalam Pasal 9 huruf c merupakan penetapan atas situasi Insiden Siber yang terus meningkat dan telah memenuhi kriteria Krisis Siber sebagaimana dimaksud dalam Pasal 12 ayat (4).
(2) Status Krisis Siber ditetapkan oleh Presiden berdasarkan usulan dari Kepala Badan.
(3) Berdasarkan penetapan sebagaimana dimaksud pada ayat (2), Presiden membentuk gugus tugas Krisis Siber.

Pasal 14

(1) Penyelenggaraan Manajemen Krisis Siber saat terjadi Krisis Siber sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf b meliputi:
   a. penanggulangan Krisis Siber;
   b. pemulihan Krisis Siber;
   c. pelaporan penanganan Krisis Siber; dan
   d. pengakhiran status Krisis Siber.
(2) Penyelenggaraan Manajemen Krisis Siber saat terjadi Krisis Siber sebagaimana dimaksud pada ayat (1) dilaksanakan oleh gugus tugas Krisis Siber.
(3) Dalam penyelenggaraan Manajemen Krisis Siber sebagaimana dimaksud pada ayat (1) gugus tugas dapat mengikutsertakan PSE.

Pasal 15

(1) Penanggulangan Krisis Siber sebagaimana dimaksud dalam Pasal 14 ayat (1) huruf a dilaksanakan melalui kegiatan:
   a. identifikasi dan analisis ruang lingkup sistem elektronik terdampak Krisis Siber;
   b. isolasi terhadap sistem elektronik terdampak Krisis Siber;
   c. pengumpulan dan preservasi bukti dari sistem elektronik terdampak Krisis Siber;
   d. investigasi dan eradikasi penyebab Krisis Siber;
   e. penguatan sistem yang tidak terdampak Krisis Siber; dan
   f. koordinasi dengan Pemangku Kepentingan dalam rangka penerapan protokol komunikasi Krisis Siber dan pengendalian informasi kepada publik.
(2) Dalam melaksanakan penanggulangan Krisis Siber, gugus tugas mengacu pada rencana kontingensi Krisis Siber yang telah ditetapkan oleh Kepala Badan sebagaimana dimaksud dalam Pasal 5.
(3) Selain mengacu pada rencana kontingensi Krisis Siber sebagaimana dimaksud pada ayat (2), gugus tugas dapat menggunakan acuan lain sesuai dengan kebutuhan dalam melaksanakan penanggulangan Krisis Siber.
(4) Gugus tugas dalam melaksanakan penanggulangan Krisis Siber mengikutsertakan PSE yang terdampak.
(5) Pengumpulan dan preservasi bukti sebagaimana dimaksud pada ayat (1) huruf c dilaksanakan dengan kehati-hatian agar tidak merusak bukti.
(6) Protokol komunikasi Krisis Siber dan pengendalian informasi kepada publik sebagaimana dimaksud pada ayat (1) huruf f dilaksanakan dengan mempertimbangkan paling sedikit:
   a. peran, tanggung jawab, dan kewenangan pihak yang terlibat dalam komunikasi;
   b. batasan konten yang disampaikan sesuai peran, tanggung jawab, dan kewenangan pihak yang terlibat dalam komunikasi; dan
   c. media utama dan/atau alternatif yang digunakan.

Pasal 16

(1) Pemulihan Krisis Siber sebagaimana dimaksud dalam Pasal 14 ayat (1) huruf b merupakan upaya pemulihan sistem elektronik terdampak.
(2) Pemulihan sistem elektronik terdampak sebagaimana dimaksud pada ayat (1) dilaksanakan oleh PSE.
(3) Pemulihan sistem elektronik terdampak sebagaimana dimaksud pada ayat (1) dilakukan dengan cara:
    a. pengembalian data dan sistem terdampak; atau
    b. penggunaan sumber daya cadangan dan/atau alternatif.
(4) Setelah upaya pemulihan sistem elektronik terdampak sebagaimana dimaksud pada ayat (3), PSE melakukan kegiatan pengujian ulang terhadap fungsi vital dan fungsi pendukung untuk memastikan capaian pemulihan terpenuhi.
(5) Capaian pemulihan sebagaimana dimaksud pada ayat (4) dinilai berdasarkan:
    a. waktu pemulihan di bawah batas waktu maksimal yang ditetapkan berdasarkan rencana kontingensi Krisis Siber;
    b. jumlah data yang terpulihkan sesuai dengan batas jumlah data minimal yang ditetapkan berdasarkan rencana kontingensi Krisis Siber; dan/atau
    c. fungsi vital dan fungsi pendukung yang terpulihkan sesuai dengan batas fungsi vital dan fungsi pendukung minimal yang ditetapkan berdasarkan rencana kontingensi Krisis Siber.
(6) Gugus tugas melakukan koordinasi dan supervisi kepada PSE yang melaksanakan pemulihan sistem elektronik terdampak dan pengujian ulang terhadap fungsi vital dan fungsi pendukung untuk memastikan capaian pemulihan terpenuhi sebagaimana dimaksud pada ayat (3), ayat (4), dan ayat (5).

Pasal 17

(1) Gugus tugas menyusun laporan berkala dan laporan akhir penanganan Krisis Siber.
(2) Laporan berkala sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
    a. kondisi Krisis Siber terkini;
    b. perkembangan penanggulangan Krisis Siber;
    c. perkembangan pemulihan Krisis Siber; dan
    d. rekomendasi tindak lanjut mitigasi.
(3) Laporan akhir sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
    a. hasil analisis dan capaian penanganan Krisis Siber; dan
    b. rekomendasi tindak lanjut penanganan Krisis Siber.
(4) Laporan berkala dan laporan akhir sebagaimana dimaksud pada ayat (1) disampaikan oleh gugus tugas kepada Presiden.

Pasal 18

Pengakhiran status Krisis Siber sebagaimana dimaksud dalam Pasal 14 ayat (1) huruf d merupakan penetapan pengakhiran status Krisis Siber oleh Presiden berdasarkan laporan gugus tugas Krisis Siber.

Pasal 19

(1) Penyelenggaraan Manajemen Krisis Siber setelah Krisis Siber sebagaimana dimaksud dalam Pasal 8 ayat 1 huruf c diselenggarakan paling sedikit meliputi:
    a. penghitungan perkiraan nilai kerusakan dan kerugian akibat Krisis Siber;
    b. penghitungan perkiraan biaya pemulihan akibat Krisis Siber;
    c. penghitungan korban jiwa, hilang, dan terluka; dan
    d. evaluasi penanganan Krisis Siber.
(2) Penyelenggaraan setelah Krisis Siber sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Badan dengan mengikutsertakan PSE.

Pasal 20

(1) Penghitungan perkiraan nilai kerusakan dan kerugian akibat Krisis Siber sebagaimana dimaksud dalam Pasal 19 ayat (1) huruf a merupakan penghitungan terhadap:
    a. nilai aset yang rusak;
    b. kerugian ekonomi yang timbul akibat adanya aset yang rusak; dan
    c. penurunan tingkat reputasi.
(2) Penghitungan perkiraan nilai aset yang rusak sebagaimana dimaksud pada ayat (1) huruf a dihitung berdasarkan ketentuan manajemen aset yang berlaku di PSE terdampak atau membandingkan nilai aset yang rusak akibat Krisis Siber dengan nilai aset tersebut sebelum terjadinya Krisis Siber.
(3) Penghitungan perkiraan kerugian ekonomi sebagaimana dimaksud pada ayat (1) huruf b dihitung berdasarkan dampak ekonomi yang seharusnya diperoleh ketika sistem elektronik berfungsi dengan baik.
(4) Penghitungan perkiraan penurunan tingkat reputasi sebagaimana dimaksud pada ayat (1) huruf c didasarkan pada persepsi publik.

Pasal 21

Penghitungan perkiraan biaya pemulihan akibat Krisis Siber sebagaimana dimaksud dalam Pasal 19 ayat (1) huruf b merupakan penghitungan perkiraan biaya yang dibutuhkan untuk mengembalikan sistem elektronik seperti sebelum Krisis Siber.

Pasal 22

Penghitungan korban jiwa, hilang, dan terluka sebagaimana dimaksud dalam Pasal 19 ayat (1) huruf c merupakan penghitungan jumlah secara keseluruhan korban jiwa, hilang, dan terluka.

Pasal 23

(1) Evaluasi penanganan Krisis Siber sebagaimana dimaksud dalam Pasal 19 ayat (1) huruf d merupakan kegiatan untuk menilai proses penanganan Krisis Siber yang telah dilaksanakan sesuai dengan rencana kontingensi Krisis Siber.
(2) Hasil evaluasi penanganan Krisis Siber sebagaimana dimaksud pada ayat (1) menjadi dasar untuk perbaikan rencana kontingensi Krisis Siber dan sebagai bahan pertimbangan dalam pengambilan kebijakan Keamanan Siber.

BAB IV
KETENTUAN PENUTUP

Pasal 24

Rencana kontingensi Krisis Siber harus ditetapkan paling lambat 12 (dua belas) bulan setelah Peraturan Badan ini ditetapkan.

Pasal 25

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 44