BERITA NEGARA REPUBLIK INDONESIA

No.1488, 2020 BSSN. Tim Tanggap Insiden Siber.

PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 10 TAHUN 2020
TENTANG
TIM TANGGAP INSIDEN SIBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : a. bahwa untuk melakukan penanganan insiden siber yang efektif dan efisien guna melindungi kepentingan umum diperlukan tim yang bertanggung jawab dalam menangani insiden siber;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Tim Tanggap Insiden Siber;

Mengingat : 1. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 100) sebagaimana telah diubah dengan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 277);

2. Peraturan Badan Siber dan Sandi Negara Nomor 2 Tahun 2018 tentang Organisasi dan Tata Kerja Badan Siber dan

Sandi Negara (Berita Negara Republik Indonesia Tahun 2018 Nomor 291);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG TIM TANGGAP INSIDEN SIBER.

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. 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.
3. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik.
4. Tim Tanggap Insiden Siber adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
5. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

Pasal 2

(1) Penanganan Insiden Siber dilaksanakan oleh Tim Tanggap Insiden Siber.
(2) Tim Tanggap Insiden Siber sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. Tim Tanggap Insiden Siber nasional;
    b. Tim Tanggap Insiden Siber sektoral;

c. Tim Tanggap Insiden Siber organisasi; dan
d. Tim Tanggap Insiden Siber khusus.

(3) Tim Tanggap Insiden Siber sebagaimana dimaksud pada ayat (2) paling sedikit terdiri atas:
a. ketua;
b. anggota; dan
c. narahubung.

Pasal 3

(1) Tim Tanggap Insiden Siber nasional sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a dibentuk oleh BSSN.
(2) Tim Tanggap Insiden Siber nasional sebagaimana dimaksud pada ayat (1) melakukan pengelolaan penanganan Insiden Siber pada tingkat nasional.
(3) Pengelolaan penanganan Insiden Siber sebagaimana dimaksud pada ayat (2) dilakukan terhadap Insiden Siber yang mengakibatkan gangguan pada keberlangsungan layanan Sistem Elektronik pada:
a. paling sedikit 2 (dua) sektor dengan jumlah organisasi paling sedikit 2 (dua) di setiap sektor; atau
b. lebih dari setengah jumlah organisasi di 1 (satu) sektor.

Pasal 4

Tim Tanggap Insiden Siber nasional sebagaimana dimaksud dalam Pasal 3 bertugas:
a. menyelenggarakan layanan Tim Tanggap Insiden Siber sesuai dengan kebutuhan penanganan Insiden Siber tingkat nasional;
b. menjadi pusat koordinasi penanganan Insiden Siber tingkat nasional;
c. merumuskan panduan teknis penanganan Insiden Siber tingkat nasional;
d. melaksanakan registrasi Tim Tanggap Insiden Siber;
e. menyediakan fasilitas dan mekanisme kerja untuk menerima laporan penanganan Insiden Siber dari pihak

yang menerima layanan;

f. membangun dan mengelola pangkalan data Insiden Siber dari seluruh Tim Tanggap Insiden Siber yang teregister dan informasi mengenai Insiden Siber di tingkat nasional;

g. memberi bantuan atau mengoordinasikan bantuan yang diperlukan dari pihak yang menerima layanan dalam hal penanganan Insiden Siber; dan

h. menjadi narahubung nasional serta mewakili negara di tingkat regional dan internasional.

Pasal 5

(1) Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dibentuk oleh:
   a. kementerian atau lembaga yang berwenang melakukan pengawasan pada sektornya; atau
   b. institusi yang ditunjuk oleh kementerian atau lembaga yang berwenang melakukan pengawasan pada sektornya.

(2) Sektor sebagaimana dimaksud pada ayat (1) meliputi:
   a. sektor administrasi pemerintahan;
   b. sektor energi dan sumber daya mineral;
   c. sektor transportasi;
   d. sektor keuangan;
   e. sektor kesehatan;
   f. sektor teknologi informasi dan komunikasi;
   g. sektor pangan;
   h. sektor pertahanan; dan
   i. sektor lain yang ditetapkan oleh Presiden.

(3) Tim Tanggap Insiden Siber sektoral pada sektor administrasi pemerintahan sebagaimana dimaksud pada ayat (2) huruf a dibentuk oleh BSSN.

(4) Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud pada ayat (1) melakukan pengelolaan penanganan Insiden Siber pada sektornya.

(5) Pengelolaan penanganan Insiden Siber sebagaimana dimaksud pada ayat (4) dilakukan terhadap Insiden Siber yang mengakibatkan gangguan pada

keberlangsungan layanan Sistem Elektronik pada paling sedikit 2 (dua) organisasi dan paling banyak setengah jumlah organisasi di 1 (satu) sektor.

Pasal 6

Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud dalam Pasal 5 bertugas:

a. menyelenggarakan layanan Tim Tanggap Insiden Siber sesuai dengan kebutuhan penanganan Insiden Siber di tingkat sektor;
b. mengoordinasikan penanganan Insiden Siber tingkat sektor dan Insiden Siber tingkat organisasi yang terjadi dalam lingkup sektornya;
c. merumuskan panduan teknis penanganan Insiden Siber tingkat sektor;
d. melakukan koordinasi dengan Tim Tanggap Insiden Siber nasional;
e. memberikan bantuan yang diperlukan kepada pihak yang menerima layanan;
f. menyusun dan menyampaikan laporan penanganan Insiden Siber tingkat sektor dan Insiden Siber tingkat organisasi yang terjadi dalam lingkup sektornya setiap tahun dan/atau sewaktu-waktu jika diperlukan kepada Tim Tanggap Insiden Siber nasional;
g. menyediakan fasilitas dan mekanisme kerja untuk menerima laporan penanganan Insiden Siber dari pihak yang menerima layanan; dan
h. melakukan koordinasi dan/atau kerja sama dengan pihak lain dengan memperhatikan kerahasiaan informasi, perlindungan data, dan sesuai dengan ketentuan peraturan perundangan-undangan.

Pasal 7

(1) Tim Tanggap Insiden Siber organisasi sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf c dibentuk oleh setiap organisasi atau institusi yang menjadi Penyelenggara Sistem Elektronik.

(2) Tim Tanggap Insiden Siber organisasi sebagaimana dimaksud pada ayat (1) melakukan pengelolaan penanganan Insiden Siber pada lingkup organisasi atau institusi.

(3) Pengelolaan penanganan Insiden Siber sebagaimana dimaksud pada ayat (2) dilakukan terhadap Insiden Siber yang mengakibatkan gangguan pada keberlangsungan layanan Sistem Elektronik pada 1 (satu) organisasi.

Pasal 8

Tim Tanggap Insiden Siber organisasi sebagaimana dimaksud dalam Pasal 7 bertugas:

a. menyelenggarakan layanan Tim Tanggap Insiden Siber sesuai dengan kebutuhan penanganan Insiden Siber di organisasinya;
b. mengoordinasikan penanganan Insiden Siber tingkat organisasi;
c. merumuskan panduan teknis penanganan Insiden Siber tingkat organisasi;
d. melakukan koordinasi dengan Tim Tanggap Insiden Siber sektoral atau dengan Tim Tanggap Insiden Siber nasional dalam hal belum tersedianya Tim Tanggap Insiden Siber sektoral;
e. memberikan bantuan yang diperlukan kepada pihak yang menerima layanan;
f. memberikan laporan penanganan Insiden Siber yang telah terjadi kepada pimpinan organisasi dan Tim Tanggap Insiden Siber sektoral atau Tim Tanggap Insiden Siber nasional dalam hal belum tersedianya Tim Tanggap Insiden Siber sektoral; dan
g. melakukan koordinasi dan/atau kerja sama dengan pihak lain dengan memperhatikan kerahasiaan informasi, perlindungan data, dan sesuai dengan ketentuan peraturan perundangan-undangan.

Pasal 9

(1) Tim Tanggap Insiden Siber khusus sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf d dibentuk oleh organisasi pemerintah atau organisasi nonpemerintah.

(2) Tim Tanggap Insiden Siber khusus sebagaimana dimaksud pada ayat (1) melakukan pengelolaan penanganan Insiden Siber untuk kebutuhan yang bersifat khusus.

(3) Kebutuhan yang bersifat khusus sebagaimana dimaksud pada ayat (2) antara lain:
   a. kebutuhan kewilayahan;
   b. kebutuhan komunitas tertentu;
   c. kebutuhan pelanggan berbasis layanan komersial;
   d. kebutuhan pelanggan produk tertentu; dan/atau
   e. kebutuhan kegiatan dalam jangka waktu tertentu.

Pasal 10

Tim Tanggap Insiden Siber khusus sebagaimana dimaksud dalam Pasal 9 bertugas:

a. menyelenggarakan layanan Tim Tanggap Insiden Siber sesuai dengan kebutuhan penanganan Insiden Siber yang menjadi ruang lingkup layanannya;
b. mengoordinasikan penanganan Insiden Siber yang menjadi ruang lingkup layanannya;
c. memberikan bantuan yang diperlukan kepada pihak yang menerima layanan;
d. menyusun panduan teknis penanganan Insiden Siber pada lingkup layanannya;
e. melakukan koordinasi dengan Tim Tanggap Insiden Siber nasional;
f. melaporkan penanganan Insiden Siber kepada Tim Tanggap Insiden Siber nasional; dan
g. melakukan koordinasi dan/atau kerja sama dengan pihak lain dengan memperhatikan kerahasiaan informasi, perlindungan data, dan sesuai dengan ketentuan peraturan perundangan-undangan.

Pasal 11

(1) Pelaksanaan tugas Tim Tanggap Insiden Siber dapat dilakukan melalui koordinasi antar Tim Tanggap Insiden Siber.

(2) Pelaksanaan koordinasi sebagaimana dimaksud pada ayat (1) dilakukan oleh narahubung di setiap Tim Tanggap Insiden Siber.

Pasal 12

(1) Tim Tanggap Insiden Siber sebagaimana dimaksud dalam Pasal 2 menyelenggarakan:
   a. layanan utama; dan
   b. layanan tambahan.

(2) Layanan utama sebagaimana dimaksud pada ayat (1) huruf a dan layanan tambahan sebagaimana dimaksud pada ayat (1) huruf b diselenggarakan berdasarkan standar nasional Indonesia ISO/IEC 27035 atau ketentuan lain sesuai dengan peraturan perundang-undangan.

(3) Layanan utama dan layanan tambahan sebagaimana dimaksud pada ayat (2) diberikan oleh:
   a. Tim Tanggap Insiden Siber nasional kepada pihak yang menerima layanan, meliputi:
      1) Tim Tanggap Insiden Siber sektoral;
      2) Tim Tanggap Insiden Siber organisasi;
      3) Tim Tanggap Insiden Siber khusus; dan
      4) institusi yang menyelenggarakan Sistem Elektronik, namun belum memiliki Tim Tanggap Insiden Siber organisasi dan belum terdapat Tim Tanggap Insiden Siber sektoral yang menaunginya.
   b. Tim Tanggap Insiden Siber sektoral kepada pihak yang menerima layanan, meliputi:
      1) Tim Tanggap Insiden Siber organisasi dalam lingkup sektornya; dan
      2) institusi dalam lingkup sektornya yang menyelenggarakan Sistem Elektronik, namun

belum memiliki Tim Tanggap Insiden Siber organisasi.

c. Tim Tanggap Insiden Siber organisasi kepada pihak yang menerima layanan, meliputi:
   1) Penyelenggara Sistem Elektronik dalam lingkup organisasinya; dan
   2) pengguna teknologi informasi dan komunikasi dalam lingkup organisasinya.
d. Tim Tanggap Insiden Siber khusus kepada pihak yang menerima layanan, meliputi kelompok atau organisasi yang menjadi ruang lingkup layanannya.

Pasal 13

(1) Layanan utama sebagaimana dimaksud dalam Pasal 12 ayat (1) huruf a terdiri atas:
   a. pemberian peringatan terkait keamanan siber; dan
   b. pengelolaan Insiden Siber.
(2) Pemberian peringatan terkait keamanan siber sebagaimana dimaksud pada ayat (1) huruf a merupakan penyebarluasan informasi keamanan siber kepada pihak yang menerima layanan.
(3) Pengelolaan Insiden Siber sebagaimana dimaksud pada ayat (1) huruf b merupakan kegiatan menerima, menanggapi, dan menganalisis Insiden Siber.

Pasal 14

(1) Layanan tambahan sebagaimana dimaksud dalam Pasal 12 ayat (1) huruf b terdiri atas:
   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.

(2) Penanganan kerentanan sistem elektronik sebagaimana dimaksud pada ayat (1) huruf a merupakan kegiatan analisis teknikal yang dilakukan dengan memeriksa kerentanan pada perangkat lunak maupun perangkat keras, serta melakukan proses verifikasi kerentanan yang mungkin dieksploitasi dengan tujuan menyusun rencana untuk memperbaiki kerentanan yang ada.

(3) Penanganan artefak digital sebagaimana dimaksud pada ayat (1) huruf b merupakan kegiatan analisis teknikal yang dilakukan dengan mencari jejak digital berupa objek atau dokumen yang diduga digunakan untuk melakukan tindakan yang tidak sah terhadap Sistem Elektronik.

(4) Pemberitahuan hasil pengamatan potensi ancaman sebagaimana dimaksud pada ayat (1) huruf c merupakan penyampaian kepada pihak yang menerima layanan terkait ancaman terhadap Sistem Elektronik yang dapat muncul akibat perkembangan teknologi, politik, ekonomi, dan perkembangan lainnya.

(5) Pendeteksian serangan sebagaimana dimaksud pada ayat (1) huruf d merupakan kegiatan menganalisis data untuk mendeteksi adanya serangan terhadap Sistem Elektronik.

(6) Analisis risiko keamanan siber sebagaimana dimaksud pada ayat (1) huruf e merupakan teknik untuk mengidentifikasi dan menilai risiko keamanan siber serta merekomendasikan tindak lanjut untuk menghadapi risiko tersebut.

(7) Konsultasi terkait kesiapan penanganan Insiden Siber sebagaimana dimaksud pada ayat (1) huruf f merupakan kegiatan konseling yang dilakukan dengan tujuan memberikan wawasan, pemahaman, dan cara yang perlu dilaksanakan dalam rangka membantu penanganan Insiden Siber.

(8) Pembangunan kesadaran dan kepedulian terhadap keamanan siber sebagaimana dimaksud pada ayat (1) huruf g merupakan kegiatan diseminasi di bidang keamanan siber kepada pihak yang menerima layanan.

Pasal 15

(1) Dalam pelaksanaan layanan Tim Tanggap Insiden Siber sebagaimana dimaksud dalam Pasal 12, diperlukan sumber daya.

(2) Sumber daya sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. sumber daya manusia;
   b. perangkat pendukung; dan
   c. pendanaan.

(3) Sumber daya manusia sebagaimana dimaksud pada ayat (2) huruf a merupakan orang yang memiliki kompetensi di bidang keamanan siber.

(4) Perangkat pendukung sebagaimana dimaksud pada ayat (2) huruf b merupakan perangkat untuk mendukung operasional layanan Tim Tanggap Insiden Siber.

(5) Pendanaan sebagaimana dimaksud pada ayat (2) huruf c berasal dari sumber yang sah.

Pasal 16

Tim Tanggap Insiden Siber sektoral, Tim Tanggap Insiden Siber organisasi, dan Tim Tanggap Insiden Siber khusus sebagaimana dimaksud dalam Pasal 3 huruf b, huruf c, dan huruf d melakukan registrasi kepada Tim Tanggap Insiden Siber nasional sebagaimana dimaksud dalam Pasal 3 huruf a.

Pasal 17

Registrasi sebagaimana dimaksud dalam Pasal 16 memiliki tahapan yang terdiri atas:

a. pengajuan permohonan;
b. validasi berkas permohonan; dan
c. penerbitan surat tanda register.

Pasal 18

(1) Pengajuan permohonan sebagaimana dimaksud dalam Pasal 17 huruf a disampaikan kepada Tim Tanggap Insiden Siber Nasional.

(2) Dalam hal Tim Tanggap Insiden Siber nasional sebagaimana dimaksud pada ayat (1) belum terbentuk di BSSN, permohonan ditujukan kepada pejabat pimpinan tinggi madya yang melaksanakan tugas dan fungsi di bidang penanggulangan dan pemulihan insiden.

(3) Pengajuan permohonan sebagaimana dimaksud pada ayat (1) dilakukan dengan menyampaikan surat permohonan dengan melampirkan berkas yang terdiri atas:
   a. formulir registrasi;
   b. dokumen yang memuat profil Tim Tanggap Insiden Siber sesuai format *request for comment* 2350; dan
   c. dokumen legal yang memuat pembentukan atau pelaksanaan tugas Tim Tanggap Insiden Siber.

(4) Formulir registrasi sebagaimana dimaksud pada ayat (3) huruf a paling sedikit memuat;
   a. jenis Tim Tanggap Insiden Siber;
   b. nama Tim Tanggap Insiden Siber; dan
   c. pihak yang menerima layanan.

Pasal 19

(1) Validasi berkas permohonan sebagaimana dimaksud dalam Pasal 17 huruf b dilakukan dengan memeriksa kelengkapan dan kesesuaian berkas permohonan.

(2) Validasi sebagaimana dimaksud pada ayat (1) dilaksanakan dalam waktu paling lama 30 (tiga puluh) hari kerja sejak berkas permohonan diterima.

(3) Dalam hal hasil validasi sebagaimana dimaksud pada ayat (2) menyatakan berkas permohonan telah lengkap dan sesuai, Tim Tanggap Insiden Siber sektoral, Tim Tanggap Insiden Siber organisasi, dan Tim Tanggap Insiden Siber khusus yang mengajukan permohonan diberikan surat tanda register.

(4) Dalam hal hasil validasi sebagaimana dimaksud pada ayat (2) menyatakan berkas permohonan belum lengkap dan belum sesuai, berkas permohonan dimaksud dikembalikan kepada Tim Tanggap Insiden Siber

sektoral, Tim Tanggap Insiden Siber organisasi, atau Tim Tanggap Insiden Siber khusus yang mengajukan permohonan untuk dilengkapi dan disesuaikan.

Pasal 20

(1) Penerbitan surat tanda register sebagaimana dimaksud dalam Pasal 17 huruf c dilakukan oleh ketua Tim Tanggap Insiden Siber nasional.
(2) Dalam hal Tim Tanggap Insiden Siber nasional belum terbentuk, surat tanda register sebagaimana dimaksud pada ayat (1) ditandatangani oleh pejabat pimpinan tinggi madya yang melaksanakan tugas dan fungsi di bidang penanggulangan dan pemulihan insiden.
(3) 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; dan
    d. tanggal penerbitan surat tanda register.

Pasal 21

Surat tanda register sebagaimana dimaksud dalam Pasal 20 dinyatakan tidak berlaku apabila:

a. terdapat perubahan organisasi yang mengakibatkan perubahan Tim Tanggap Insiden Siber organisasi;
b. terdapat perubahan sektor yang mengakibatkan perubahan Tim Tanggap Insiden Siber sektoral; dan/atau
c. tugas Tim Tanggap Insiden Siber khusus dinyatakan selesai.

Pasal 22

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 15 Desember 2020

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 16 Desember 2020

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

ttd

WIDODO EKATJAHJANA