RANCANGAN

PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR... TAHUN...
TENTANG
PERLINDUNGAN INFRASTRUKUR INFORMASI KRITIS NASIONAL

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang :

a. bahwa Pemerintah melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan Informasi Elektronik dan Transaksi Elektronik yang mengganggu ketertiban umum;
b. bahwa gangguan terhadap infrastruktur informasi kritis nasional dapat menimbulkan kerugian dan dampak yang serius terhadap kepentingan umum, pelayanan publik, pertahanan dan keamanan, serta perekonomian nasional;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan b, perlu ditetapkan Peraturan Badan Siber dan Sandi Negara tentang Perlindungan infrastruktur informasi kritis nasional;

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. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor

189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);

3. Peraturan Presiden Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara sebagaimana telah diubah degan Peraturan Presiden Nomor 133 Tahun 2017 tentang Perubahan Atas Peraturan Presiden Nomor 53 Tahun 2017 (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 100).

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG PERLINDUNGAN INFRASTRUKTUR INFORMASI KRITIS NASIONAL

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:

1. Infrastruktur Kritis Nasional adalah Infrastruktur baik fisik maupun non fisik yang memiliki fungsi sangat penting dalam menunjang hajat hidup orang banyak yang apabila terjadi gangguan, kerusakan, dan/atau kehancuran pada infrastruktur tersebut dapat berdampak pada pertahanan dan keamanan nasional, ekonomi nasional, kesehatan, keselematan publik, penyelenggaraan negara, pelayanan publik, merusak reputasi negara dan hilangnya kepercayaan publik, maupun dampak lain berupa kombinasi dari hal-hal tersebut.
2. Infrastruktur Informasi Kritis Nasional adalah Sistem Elektronik dengan kategori strategis yang meliputi teknologi informasi, teknologi operasional, dan data elektronik strategis, baik berdiri sendiri maupun saling bergantung dengan sistem elektronik lainnya dalam menunjang suatu infrastruktur kritis nasional yang apabila terjadi gangguan, kerusakan, dan/atau kehancuran pada infrastruktur tersebut dapat berdampak pada pertahanan dan keamanan nasional, ekonomi nasional, kesehatan, keselematan publik, penyelenggaraan negara, pelayanan publik, merusak

reputasi negara dan hilangnya kepercayaan publik, maupun dampak lain berupa kombinasi dari hal-hal tersebut

3. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/ atau menyebarkan Informasi Elektronik.
4. Informasi Elektronik adalah satu atau sekumpulan data elektronik, 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.
5. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/ atau menyebarkan informasi.
6. Teknologi Operasional adalah suatu teknik baik meliputi perangkat keras dan perangkat lunak yang memiliki fungsi dapat mendeteksi, menyebabkan perubahan secara langsung, dan/atau dapat mengontrol perangkat fisik atau suatu proses.
7. Data Elektronik Strategis adalah data elektronik yang berdampak strategis terhadap kelancaran penyelenggaraan negara, dan pertahanan dan keamanan negara.
8. Keamanan Siber adalah keamanan komputer atau sistem komputer terhadap akses, tindakan atau aktivitas melalui sistem komputer atau komputer, yang dapat membahayakan, merusak dan berdampak buruk terhadap keamanan, ketersediaan, kerahasiaan atau integritas sistem komputer atau komputer.
9. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam layanan Sistem Elektronik dan/atau pelanggaran kepatuhan terhadap kebijakan keamanan siber yang berlaku pada penyelenggara Sistem Elektronik.
10. Instansi Pengawas dan Pengatur Sektor yang selanjutnya disebut IPPS adalah instansi yang bertugas mengawasi

pelaksanaan tugas sektor dan mengeluarkan pengaturan terhadap sektor tersebut.

11. Badan Siber dan Sandi Negara yang selanjutnya disebut BSSN adalah Lembaga Pemerintah non Kementerian yang berada di bawah dan bertanggung jawab kepada Presiden melalui Menteri yang menyelenggarakan koordinasi, sinkronisasi, dan pengendalian penyelenggaraan Pemerintah di bidang politik, hukum dan keamanan.
12. Penyelenggara Infrastruktur Informasi Kritis Nasional adalah lembaga pemerintah, badan usaha, dan atau organisasi yang memiliki dan mengoperasikan Infrastruktur Informasi Kritis Nasional.

Pasal 2

Pengaturan Perlindungan Infrastruktur Informasi Kritis Nasional bertujuan untuk:

a. menjaga keberlangsungan penyelenggaraan Infrastruktur Informasi Kritis Nasional secara aman, andal, dan terpercaya;
b. mencegah gangguan dan/atau kegagalan beroperasinya lnfrastruktur Informasi Kritis Nasional akibat serangan siber, bencana alam, dan/atau ancaman/kerentanan lainnya; dan
c. mengurangi risiko terjadinya Insiden Siber dan menjamin pemulihan dari dampak Insiden Siber yang terjadi.

Pasal 3

Ruang lingkup Perlindungan Infrastruktur Informasi Kritis Nasional meliputi:

a. identifikasi Infrastruktur Informasi Kritis Nasional;
b. strategi dan rencana aksi Perlindungan Infrastruktur Informasi Kritis Nasional;
c. penerapan standar Keamanan Siber;
d. pengelolaan risiko Keamanan Siber;
e. penanggulangan dan pemulihan Insiden Siber;
f. berbagi informasi ancaman siber;
g. peningkatan kapasitas sumber daya manusia Keamanan Siber;
h. edukasi dan pembentukan budaya Keamanan Siber;
i. keberlangsungan bisnis penyelenggaraan Infrastruktur Informasi Kritis Nasional;
j. evaluasi tingkat kematangan penerapan Perlindungan Infrastruktur Informasi Kritis Nasional; dan

k. kerja sama.

BAB II
IDENTIFIKASI INFRASTUKTUR INFORMASI KRITIS NASIONAL

Bagian Kesatu
Identifikasi Sektor Infrastruktur Kritis Nasional

Pasal 4

(1) Sektor Infrastruktur Kritis Nasional meliputi:
   a. penegakan hukum;
   b. energi dan sumber daya mineral;
   c. transportasi;
   d. keuangan dan perbankan;
   e. kesehatan;
   f. teknologi informasi dan komunikasi;
   g. pangan (pertanian);
   h. pertahanan dan industri strategis;
   i. layanan darurat (sosial);
   j. sumber daya air; dan
   k. pemerintah.

(2) Ketentuan lebih lanjut mengenai identifikasi dan penetapan sektor Infrastruktur Kritis Nasional diatur dalam Peraturan Badan Siber dan Sandi Negara.

(3) Ketentuan lebih lanjut mengenai penentuan dan penetapan, serta fungsi dan tugas Instansi Pengawas dan Pengatur Sektor diatur dalam Peraturan Badan Siber dan Sandi Negara.

Bagian Kedua
Identifikasi Infrastruktur Informasi Kritis nasional

Pasal 5

(1) Setiap Penyelenggara Infrastruktur Informasi Kritis Nasional yang berada di lingkup sektor Infrastruktur Kritis Nasional wajib melakukan identifikasi terhadap infrastruktur informasi kritis miliknya secara berkala berdasarkan kriteria sebagai berikut :
   a. memiliki Infrastruktur Informasi Kritis meliputi:
      i) teknologi informasi,
      ii) teknologi operasional, dan

iii) data elektronik strategis.

b. berdampak pada salah satu atau kombinasi pada aspek:
   i) pertahanan dan keamanan nasional,
   ii) ekonomi nasional,
   iii) kesehatan nasional,
   iv) keselamatan publik,
   v) penyelenggaraan negara,
   vi) pelayanan publik, dan
   vii) merusak reputasi negara dan hilangnya kepercayaan publik.
c. kriteria lain yang didefinisikan oleh masing-masing IPPS.

(2) Penyelenggara Infrastruktur Informasi Kritis Nasional wajib melaporkan hasil identifikasi Infrastruktur Informasi Kritis yang dikelolanya kepada IPPS dan BSSN.

(3) BSSN bersama dengan IPPS melakukan verifikasi atas laporan Penyelenggara Infrastruktur Informasi Kritis Nasional dan menetapkan Infrastruktur Informasi Kritis Nasional.

(4) Dalam hal Penyelenggara Infrastruktur Informasi Kritis Nasional tidak melakukan identifikasi terhadap Infrastruktur Informasi Kritis miliknya, maka BSSN dan IPPS dapat melakukan identifikasi langsung terhadap Infrastruktur Informasi Kritis tersebut.

(5) Untuk menunjang proses identifikasi sebagaimana dimaksud dalam ayat (3), BSSN dan IPPS dapat melakukan identifikasi interdependensi antar Infrastruktur Informasi Kritis pada sektor Infrastruktur Kritis Nasional binaannya dan juga lintas sektor.

(6) Interdependensi sebagaimana dimaksud pada ayat (5) menggambarkan hubungan saling ketergantungan antar Infrastruktur Informasi Kritis Nasional di masing-masing sektor Infrastruktur Kritis Nasional dan juga lintas sektor.

(7) Ketentuan lebih lanjut mengenai mekanisme identifikasi, kriteria, prosedur pelaporan, dan penilaian risiko terhadap Infrastruktur Informasi Kritis Nasional diatur dalam Peraturan Badan Siber dan Sandi Negara.

BAB III
PENYELENGGARAAN PERLINDUNGAN INFRASTRUKTUR INFORMASI KRITIS NASIONAL

Bagian Kesatu
Strategi Dan Rencana Aksi Perlindungan Infrastruktur Informasi Kritis Nasional

Pasal 6

(1) BSSN menyusun dan menetapkan rencana strategis perlindungan Infrastruktur Informasi Kritis Nasional untuk jangka waktu 5 (lima) tahun.
(2) Rencana strategis sebagaimana dimaksud pada ayat (1) dievaluasi paling sedikit 1 (satu) kali dalam setahun.
(3) Setiap Instansi Pengatur dan Pengawas Sektor menyusun peta jalan perlindungan Infrastruktur Informasi Kritis untuk jangka waktu 5 (lima) tahun dengan mengacu pada rencana strategis perlindungan Infrastruktur Informasi Kritis Nasional.
(4) Evaluasi terhadap peta jalan perlindungan Infrastruktur Informasi Kritis Nasional dilakukan dalam hal terjadi perubahan atas rencana strategis perlindungan Infrastruktur Informasi Kritis Nasional.

Bagian Kedua
Penerapan Standar Keamanan Siber

Pasal 7

(1) Penyelenggara Infrastruktur Informasi Kritis Nasional wajib menyelenggarakan Perlindungan Infrastruktur Informasi Kritis Nasional secara andal, aman dan bertanggung jawab.
(2) Penyelenggara Infrastruktur Informasi Kritis Nasional wajib menerapkan standar keamanan minimal SNI ISO/IEC 27001 versi terkini dan/atau standar keamanan lain yang ditetapkan oleh IPPS dan/atau BSSN

Bagian Ketiga
Pengelolaan Risiko Keamanan Siber

Pasal 8

(1) Setiap Penyelenggara lnfrastruktur Informasi Kritis Nasional menerapkan pengelolaan risiko keamanan siber secara efektif dalam rangka perlindungan Infrastruktur Informasi Kritis Nasional miliknya.
(2) Penerapan pengelolaan risiko keamanan siber sebagaimana dimaksud pada ayat (1) minimal mempertimbangkan hal-hal sebagai berikut:
    a. kepatuhan terhadap peraturan perundangan yang berlaku di Indonesia;
    b. kesesuaian dengan kebijakan yang ada seperti rencana strategis dan peta jalan yang ditetapkan oleh IPPS;
    c. kecukupan proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko pada Perlindungan Infrastruktur Informasi Kritis Nasional yang disusun oleh IPPS; dan
    d. sistem pengendalian intern yang berlaku di penyelenggara Infrastruktur Informasi Kritis Nasional.
(3) Penerapan pengelolaan risiko harus dilakukan secara terintegrasi dalam setiap tahapan Perlindungan Infrastruktur Informasi Kritis Nasional sejak proses perencanaan, pengadaan, pengembangan, operasional, pemeliharaan, hingga penghentian dan penghapusan Infrastruktur Informasi Kritis Nasional.
(4) BSSN bersama dengan IPPS melakukan pengawasan secara aktif terhadap penerapan pengelolaan risiko sebagaimana dimaksud pada ayat (2).
(5) Penyelenggara Infrastruktur Informasi Kritis Nasional melaporkan hasil penerapan pengelolaan risiko kepada IPPS secara berkala setiap 2 (dua) tahun sekali.
(6) Mekanisme pelaporan dapat diatur lebih lanjut oleh masing-masing IPPS.
(7) BSSN bersama IPPS melakukan evaluasi pengelolaan risiko dan pemantauan mitigasi risiko secara berkala setiap 2 (dua) tahun sekali.
(8) Ketentuan lebih lanjut mengenai mekanisme evaluasi pengelolaan risiko dan pemantauan mitigasi risiko

sebagaimana dimaksud dalam ayat (7) diatur dalam Peraturan Badan Siber dan Sandi Negara.

Bagian Keempat
Penanggulangan dan Pemulihan Insiden Siber

Pasal 9

(1) Setiap penyelenggara Infrastruktur Informasi Kritis Nasional wajib melakukan penanganan, penanggulangan, tanggap insiden, dan pemulihan pasca Insiden Siber terhadap Infrastruktur Informasi Kritis Nasional yang dikelolanya.
(2) Penyelenggara Infrastruktur Informasi Kritis Nasional melaporkan setiap bentuk penanganan, penanggulangan, tanggap insiden dan pemulihan pasca Insiden Siber kepada IPPS dan ditembuskan kepada BSSN.

Pasal 10

(1) Pengelolaan persiapan penanganan, penanggulangan, tanggap insiden, dan pemulihan Insiden Siber dilakukan oleh Penyelenggara Infrastruktur Informasi Kritis Nasional dengan:
    a. menyusun mekanisme manajemen krisis siber;
    b. menyusun kerangka kerja penanganan, penanggulangan, tanggap insiden, dan pemulihan Insiden Siber termasuk menyiapkan sumber daya yang diperlukan pada saat proses penanganan;
    c. melakukan dan turut berpartisipasi aktif dalam simulasi penanganan Insiden Siber dan pemulihan di internal sektor Infrastruktur Kritis Nasional dan lintas sektor Infrastruktur Kritis Nasional;
    d. melakukan evaluasi kematangan penanganan insiden siber.
(2) Ketentuan lebih lanjut mengenai mekanisme penyusunan dan penetapan manajemen krisis sebagaimana dimaksud dalam pasal (1) huruf (a) diatur lebih lanjut dalam Peraturan Badan Siber dan Sandi Negara.
(3) Ketentuan lebih lanjut mengenai Pengelolaan persiapan penanganan, penanggulangan, tanggap insiden, dan pemulihan Insiden Siber sebagaimana dimaksud dalam

pasal (1) huruf (b) diatur lebih lanjut dalam Peraturan Badan Siber dan Sandi Negara.

Pasal 11

(1) Simulasi penanganan Insiden Siber di internal sektor Infrastruktur Kritis Nasional minimal dilaksanakan setiap 1 (satu) tahun sekali dan dikoordinasikan oleh IPPS dari masing-masing sektornya.
(2) Simulasi penanganan Insiden Siber pada lintas sektor minimal dilaksanakan setiap 1 (satu) tahun sekali dan dikoordinasikan oleh BSSN.

Pasal 12

(1) BSSN dapat menetapkan aksi penanggulangan dan pemulihan pada Infrastruktur Informasi Kritis Nasional jika terjadi Insiden Siber skala nasional.
(2) Insiden Siber skala nasional yang dimaksud pada ayat (1) adalah kegagalan teknologi pada Infrastruktur Informasi Kritikal Nasional yang mengakibatkan gangguan luas pada layanan IIKN, terganggunya stabilitas nasional dan/atau menimbulkan korban jiwa masyarakat.
(3) Aksi penanggulangan dan pemulihan pada Infrastruktur Informasi Kritis Nasional sebagaimana dimaksud pada ayat (1), dikoordinasikan oleh Tim Penanggulangan dan Pemulihan Insiden Siber/CSIRT Nasional.
(4) Ketentuan lebih lanjut mengenai CSIRT Nasional diatur dalam Peraturan Badan Siber dan Sandi Negara.

Bagian Keenam
Berbagi Informasi Ancaman, Celah Keamanan dan Insiden Siber

Pasal 13

(1) Masing-masing sektor Infrastruktur Kritis Nasional dapat membentuk pusat analisis dan berbagi informasi dengan melibatkan BSSN, IPPS, Penyelenggara Infrastruktur Informasi Kritis Nasional, Instansi, institusi, dan asosiasi yang terkait pada sektor dimaksud.

(2) Pusat analisis dan berbagi informasi sebagaimana dimaksud pada ayat (1) dilakukan untuk memelihara kesadaran berbagi informasi ancaman, celah keamanan, dan Insiden Siber beserta mitigasinya, serta kerja sama lainnya pada sektor dimaksud.
(3) Berbagi informasi sebagaimana dimaksud pada ayat (2) dilakukan dengan skema yang ditentukan oleh IPPS pada sektor dimaksud.

Bagian Ketujuh
Peningkatan Kapasistas Sumber Daya Manusia Keamanan Siber

Pasal 14

(1) Setiap Penyelenggara Infrastruktur Informasi Kritis Nasional wajib melakukan peningkatan kapasitas sumber daya manusia dibidang Keamanan Siber.
(2) Peningkatan kapasitas sumber daya manusia sebagaimana dimaksud pada ayat (1) disesuaikan dengan peta jalan Perlindungan Infrastruktur Informasi Kritis Nasional yang disusun oleh IPPS.

Pasal 15

(1) Peningkatan kapasitas sumber daya manusia sebagaimana dimaksud dalam Pasal 14 ayat (1) dapat dilakukan dengan meningkatkan kuantitas sumber daya manusia yang memiliki kompetensi di bidang Keamanan Siber dan/atau meningkatkan kualitas kompetensi di bidang Keamanan Siber yang dikuasai.
(2) Peningkatan kapasitas sebagaimana dimaksud pada ayat (1) dilakukan diantaranya melalui:
    a. rekrutmen sumber daya manusia di bidang Keamanan Siber;
    b. peningkatan program pelatihan, materi, dan sarana pembelajaran dan aktualisasi sumber daya manusia; dan
    c. transfer ilmu pengetahuan antar-sumber daya manusia dalam suatu sektor.
(3) Peningkatan kapasitas sebagaimana dimaksud pada ayat (1) diawasi pelaksanaannya oleh IPPS.

Pasal 16

(1) Setiap pengelola Infrastruktur Informasi Kritis dan tenaga ahli pada Penyelenggara Infrastruktur Informasi Kritis Nasional wajib merupakan pekerja tetap pada Penyelenggara Infrastruktur Informasi Kritis Nasional.
(2) Setiap pengelola dan tenaga ahli pada Penyelenggara Infrastruktur Informasi Kritis Nasional wajib terikat pada perjanjian kerahasiaan informasi.

Bagian Kedelapan
Edukasi dan Pembentukan Budaya Keamanan Siber

Pasal 17

(1) Setiap Penyelenggara Infrastruktur Informasi Kritis Nasional melakukan kegiatan kesadaran Keamanan Siber.
(2) Kegiatan kesadaran Keamanan Siber sebagaimana dimaksud pada ayat (1) dilakukan pada tingkat pimpinan, pekerja, maupun pihak lain yang terkait dan/atau melakukan pengelolaan pada Infrastruktur Informasi Kritis Nasional.
(3) Peningkatan kesadaran Keamanan Siber sebagaimana dimaksud pada ayat (1) disesuaikan dengan peta jalan Perlindungan Infrastruktur Informasi Kritis Nasional yang disusun oleh IPPS.
(4) BSSN dan IPPS dapat melakukan evaluasi terkait kegiatan peningkatan keasadaran Keamanan Siber pada Penyelenggara Infrastruktur Informasi Kritis Nasional.

Pasal 18

Kegiatan kesadaran Keamanan siber sebagaimana dimaksud dalam Pasal 17 ayat (1) termasuk tetapi tidak terbatas pada:

a. merumuskan dan menerapkan strategi, sasaran strategi, dan peta jalan (*roadmap*) kesadaran keamanan siber;
b. melakukan sosialisasi, workshop, dan diseminasi informasi terkait kesadaran keamanan siber;
c. memberikan masukan pada pimpinan mengenai hal-hal yang berkaitan dengan keamanan siber; dan
d. penyampaian informasi pada pihak eksternal dilakukan sesuai dengan klasifikasi keamanan siber dengan

pembedaan kriteria atas tingkatan jabatan penerima informasi;

e. evaluasi tingkat kesadaran keamanan siber di lingkungan Penyelenggara Infrastruktur Informasi Kritis Nasional.

Bagian Kesembilan
Keberlangsungan Bisnis Penyelenggaraan Infrastruktur Informasi Kritis Nasional

Pasal 19

(1) Setiap Penyelenggara Infrastruktur Informasi Kritis Nasional wajib memiliki kerangka kerja keberlangsungan bisnis dan pemulihan bencana penyelenggaraan Infrastruktur Informasi Kritis Nasional
(2) Kerangka kerja keberlangsungan bisnis dan pemulihan becana penyelenggaraan Infrastruktur Informasi Kritis Nasional sebagaimana dimaksud pada ayat (1) diperlukan untuk memastikan keberlangsungan operasional Infrastruktur Informasi Kritis minimal pada saat kondisi kritis.
(3) Kerangka kerja keberlangsungan bisnis dan pemulihan bencana penyelenggaraan Infrastruktur Informasi Kritis Nasional sebagaimana dimaksud pada ayat (1) disesuaikan dengan peta jalan Perlindungan Infrastruktur Informasi Kritis Nasional yang disusun oleh IPPS.

Pasal 20

Kerangka kerja keberlangsungan bisnis penyelenggaraan Infrastruktur Informasi Kritis Nasional sebagaimana dimaksud dalam Pasal 19 ayat (1) termasuk tetapi tidak terbatas pada:

a. Mengidentifikasi area proses bisnis yang kritis;
b. Mengidentifikasi fungsi-fungsi kritis pada Infrastruktur Informasi Kritis Nasional;
c. Mengidentifikasi keterhubungan antara berbagai area proses bisnis dan fungsi kritis;
d. Menetapkan risiko yang dapat diterima untuk setiap fungsi kritis;
e. Menetapkan rencana aksi yang harus dilakukan untuk mempertahankan operasional Infrastruktur Informasi Kritis Nasional.

Pasal 21

Kerangka kerja pemulihan bencana penyelenggaraan Infrastruktur Informasi Kritis Nasional sebagaimana dimaksud dalam Pasal 19 ayat (1) termasuk tetapi tidak terbatas pada:

a. menetapkan penanggung jawab pengelola Infrastruktur Informasi Kritis nasional pada saat kondisi darurat atau bencana;
b. memastikan kesiapan langkah penanggulangan bencana dengan komposisi SDM, ketersediaan proses kerja dan teknologi yang diperlukan dalam kondisi darurat atau bencana;
c. menentukan mekanisme pemulihan terhadap layanan Infrastruktur Informasi Kritis secara keseluruhan;
d. melakukan uji coba langkah penanggulangan bencana sedikitnya 1 kali dalam 1 tahun dengan hasil capaian yang memenuhi sasaran penyelenggaraan Infrastruktur Informasi Kritis Nasional dalam kondisi darurat atau bencana;
e. wajib melaporkan kondisi kesiapan langkah penanggulangan bencana berikut hasil uji cobanya kepada IPPS.

Bagian Kesepuluh

Evaluasi Kematangan Penerapan Perlindungan Infrastruktur Informasi Kritis Nasional

Pasal 22

(1) Setiap Penyelenggara Infrastruktur Informasi Kritis Nasional melakukan evaluasi kematangan (*maturity level*) hasil penerapan Perlindungan Infrastruktur Informasi Kritis Nasional pada lingkup organisasinya.
(2) Evaluasi kematangan sebagaimana dimaksud pada ayat (1) pada tingkat penyelenggara Infrastruktur Informasi Kritis Nasional disesuaikan dengan peta jalan Perlindungan Infrastruktur Informasi Kritis Nasional yang disusun oleh IPPS
(3) Evaluasi kematangan sebagaimana dimaksud dalam ayat (1) dilakukan dengan melakukan pengukuran tingkat kematangan penerapan Perlindungan Keamanan Siber pada Infrastruktur Informasi Kritis Nasional berdasarkan alat bantu yang disusun oleh BSSN.

(4) Pengukuran tingkat kematangan sebagaimana dimaksud pada ayat (3) dilakukan setiap 2 (dua) tahun sekali oleh asesor Perlindungan Infrastruktur informasi Kritis Nasional.
(5) Ketentuan lebih lanjut mengenai alat ukur, tata cara penilaian evaluasi kematangan, serta kualifikasi asesor diatur dalam peraturan Badan Siber dan Sandi Negara.

Bagian Kesebelas
Kerja Sama

Pasal 23

(1) IPPS, Instansi, dan/atau institusi serta Penyelenggara Infrastruktur Informasi Kritis Nasional dapat melakukan kerja sama nasional dalam rangka menyelenggarakan Perlindungan Infrastruktur Informasi Kritis Nasional.
(2) Kerja sama nasional sebagaimana dimaksud pada ayat (1) dapat diselenggarakan dalam kerangka kemitraan pemerintah dan swasta.
(3) IPPS dapat melakukan kerja sama internasional.
(4) Kerja sama internasional sebagaimana dimaksud pada ayat (3) harus sesuai dengan kebijakan yang ditetapkan pada rencana strategis Perlindungan Infrastruktur Informasi Kritis Nasional.
(5) Kerja sama sebagaimana dimaksud pada ayat (1) dapat dilakukan untuk hal-hal termasuk tetapi tidak terbatas pada:
    a. pertukaran informasi mengenai ancaman terkini;
    b. panduan terbaik tentang perlindungan Infrastruktur Informasi Kritis; dan
    c. peningkatan kapasitas sumber daya manusia di bidang keamanan siber
(3) Setiap bentuk kerjasama yang dilakukan oleh IPPS maupun Penyelenggara Infrastruktur Informasi Kritis Nasional di bidang Keamanan Siber wajib dikoordinasikan kepada BSSN.

BAB IV
KELOMPOK KERJA PERLINDUNGAN INFRASTRUKTUR INFORMASI KRITIS NASIONAL

Bagian Kesatu
Kelompok Kerja Perlindungan Infrastruktur Informasi Kritis Nasional

Pasal 24

(1) Kelompok kerja Perlindungan Infrastruktur Informasi Kritis Nasional bertugas memberikan masukkan dan mengawasi penyelenggaraan Perlindungan Infrastruktur Informasi Kritis Nasional.
(2) Kelompok kerja Perlindungan Infrastruktur Informasi Kritis Nasional sebagaimana dimaksud pada ayat (1) ditetapkan oleh Kepala BSSN.
(3) Kelompok kerja Perlindungan Infrastruktur Informasi Kritis Nasional sebagaimana dimaksud pada ayat (1) dapat terdiri dari:
    a. BSSN;
    b. Perwakilan dari setiap IPPS;
    c. Penyelenggara Infrastruktur Informasi Kritis Nasional;
    d. Lembaga pemerintah yang melakukan fungsi pertahanan dan keamanan, penegakkan hukum, dan pemeliharaan keamanan dan ketertiban masyarakat;
    e. Ahli/pakar keamanan siber; dan
    f. sekretariat komite.
(4) Sekretariat komite sebagaimana dimaksud pada ayat (3) huruf (g) diselenggarakan oleh Direktorat Proteksi Infrastruktur Informasi Kritis Nasional, BSSN.

Pasal 25

(1) Kelompok kerja Perlindungan Infrastruktur Informasi Kritis Nasional sebagaimana dimaksud dalam Pasal 24 berwenang:
    a. membuat dokumen usulan rekomendasi strategi dan rencana aksi nasional Perlindungan Infrastruktur Informasi Kritis Nasional;
    b. melakukan konsolidasi berkala terhadap profil risiko di masing-masing sektor Infrastruktur Kritis Nasional;

c. melakukan kajian efektivitas mitigasi risiko yang bersifat lintas-sektor;
d. melakukan review atas isu-isu nasional keamanan siber, terutama pada sektor Infrastruktur Kritis Nasional;
e. memberikan usulan rekomendasi terhadap aksi nasional Perlindungan Infrastruktur Informasi Kritis Nasional termasuk kebijakan dalam hubungan internasional;

(2) Kelompok kerja Perlindungan Infrastruktur Informasi Kritis Nasional dapat melakukan pertemuan secara berkala setiap 2 (dua) tahun sekali.

(3) Hasil pertemuan dan rekomendasi Kelompok kerja Perlindungan Infrastruktur Informasi Kritis Nasional dilaporkan kepada BSSN

Bagian Kedua
Kewenangan Instansi Pengawas dan Pengatur Sektor dalam Perlindungan Infrastruktur Informasi Kritis Nasional

Pasal 26

Dalam rangka Perlindungan Infrastruktur Informasi Kritis Nasional, IPPS mempunyai tugas dan kewenangan sebagai berikut:

a. merumuskan dan menetapkan kebijakan teknis terutama peta jalan (roadmap) Perlindungan Infrastruktur Informasi Kritis Nasional pada sektor strategis binaannya berdasarkan dokumen rencana strategis Perlindungan Infrastruktur Informasi Kritis Nasional;
b. melalukan pengawasan pelaksanaan kebijakan teknis terkait Perlindungan Infrastruktur Informasi Kritis Nasional pada sektor binaannya;
c. bersama BSSN menetapkan instansi/institusi yang menyelenggarakan Infrastruktur Informasi Kritis Nasional dan data elektronik strategis sebagai bagian dari Perlindungan Infrastruktur Informasi Kritis Nasional pada sektor binaannya;
d. bersama BSSN memetakan intradependensi dan interdependensi Infrastruktur Informasi Kritis Nasional sektor binaannya;
e. melakukan evaluasi pengelolaan risiko dan pemantauan mitigasi risiko pada sektor binaannya;

f. membentuk tim penanganan insiden dan tanggap darurat keamanan informasi pada sektor binaannya dan menetapkan narahubungnya;
g. menyelenggarakan uji kesiapan insiden keaman siber di internal sektor binaannya;
h. melakukan pengukuran tingkat kematangan penerapan Perlindungan Informasi Infrastruktur Kritis Nasional pada Sektor binaanya yang dilakukan setiap 2 (dua) tahun;
i. mempromosikan budaya keamanan informasi pada sektor strategis binaannya;
j. memberikan persetujuan, melakukan pengawasan, dan menerima laporan kerja sama internasional yang dilaksanakaan oleh sektor binaannya;
k. membentuk pusat analisis dan pertukaran informasi pada sektor binaannya; dan
l. hal lain sesuai dengan ketentuan peraturan perundang-undangan

BAB V
KETENTUAN PENUTUP

Pasal 27

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

KEPALA BADAN SIBER DAN SANDI NEGARA,

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal

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

WIDODO EKATJAHJANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2019 NOMOR