PERATURAN BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA
NOMOR 10 TAHUN 2023
TENTANG
PENGUKURAN TINGKAT KEMATANGAN KEAMANAN SIBER

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 22 ayat (7) Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Pengukuran Tingkat Kematangan Keamanan 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 Republik Indonesia 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 PENGUKURAN TINGKAT KEMATANGAN KEAMANAN SIBER.

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 bersifat teknis maupun sosial.
2. Kematangan Keamanan Siber adalah kondisi yang menggambarkan kapabilitas dan kemajuan organisasi

dalam menerapkan, meningkatkan, dan menjalankan Keamanan Siber secara efektif dan efisien.

3. Tingkat Kematangan Keamanan Siber yang selanjutnya disebut Tingkat Kematangan adalah level hasil penilaian Kematangan Keamanan Siber.
4. 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.
5. Penyelenggara IIV adalah Instansi Penyelenggara Negara, badan usaha, dan/atau organisasi yang memiliki dan/atau mengoperasikan IIV.
6. Peristiwa Siber adalah kejadian pada sistem elektronik yang dapat diobservasi dan dapat memberikan indikasi terhadap terjadinya insiden siber.
7. Kementerian atau Lembaga adalah Instansi Penyelenggara Negara yang bertugas mengawasi dan mengeluarkan pengaturan terhadap sektornya.
8. Badan Siber dan Sandi Negara dan yang selanjutnya disebut Badan adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang Keamanan Siber dan sandi.
9. Kerangka Kerja Pelindungan IIV yang selanjutnya disebut Kerangka Kerja adalah seperangkat konsep dasar yang digunakan sebagai pedoman dalam menyusun, menerapkan, dan mengkomunikasikan aktivitas pengelolaan Keamanan Siber pada lingkup sektor IIV.

Pasal 2

Ruang lingkup Peraturan Badan ini meliputi:

a. pelaksanaan pengukuran Tingkat Kematangan;
b. pelaporan hasil pengukuran Tingkat Kematangan; dan
c. verifikasi hasil pengukuran Tingkat Kematangan.

Pasal 3

(1) Pelaksanaan pengukuran Tingkat Kematangan sebagaimana dimaksud dalam Pasal 2 huruf a dilakukan oleh Penyelenggara IIV secara mandiri.
(2) Pelaksanaan pengukuran Tingkat Kematangan sebagaimana dimaksud pada ayat (1) dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
(3) Pengukuran Tingkat Kematangan sebagaimana dimaksud pada ayat (2) dilaksanakan terhadap domain pada Kerangka Kerja.
(4) Domain pada Kerangka Kerja sebagaimana dimaksud pada ayat (3) meliputi:
    a. identifikasi;
    b. proteksi;
    c. deteksi; dan
    d. penanggulangan dan pemulihan.

(5) Domain identifikasi sebagaimana dimaksud pada ayat (4) huruf a terdiri atas kategori kegiatan paling sedikit meliputi:
   a. mengidentifikasi peran dan tanggung jawab organisasi;
   b. menyusun strategi, kebijakan, dan prosedur pelindungan IIV;
   c. mengelola aset informasi;
   d. menilai dan mengelola risiko keamanan siber; dan
   e. mengelola risiko rantai pasok.

(6) Domain proteksi sebagaimana dimaksud pada ayat (4) huruf b terdiri dari kategori kegiatan paling sedikit meliputi:
   a. mengelola identitas, autentikasi, dan kendali akses;
   b. melindungi aset fisik;
   c. melindungi data;
   d. melindungi aplikasi;
   e. melindungi jaringan; dan
   f. melindungi sumber daya manusia.

(7) Domain deteksi sebagaimana dimaksud pada ayat (4) huruf c terdiri dari kategori kegiatan paling sedikit meliputi:
   a. mengelola deteksi Peristiwa Siber;
   b. menganalisis anomali dan Peristiwa Siber; dan
   c. memantau Peristiwa Siber berkelanjutan.

(8) Domain penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (4) huruf d terdiri dari kategori kegiatan paling sedikit meliputi:
   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.

Pasal 4

(1) Pelaksanaan pengukuran Tingkat Kematangan sebagaimana dimaksud dalam Pasal 3 dilakukan dengan menggunakan instrumen penilaian.

(2) Instrumen penilaian sebagaimana dimaksud pada ayat (1) disusun oleh Badan.

(3) Instrumen penilaian sebagaimana dimaksud pada ayat (2) memuat indikator evaluasi penerapan domain kerangka kerja dan kategori kegiatan sebagaimana dimaksud dalam Pasal 3 ayat (4) sampai dengan ayat (8).

(4) Instrumen penilaian sebagaimana dimaksud pada ayat (3) dimuat di situs web resmi Badan.

(5) Kementerian atau Lembaga dapat menetapkan instrumen penilaian lain dengan mengacu pada instrumen penilaian yang disusun oleh Badan.

Pasal 5

(1) Pelaksanaan pengukuran Tingkat Kematangan sebagaimana dimaksud dalam Pasal 4 menghasilkan kategori Tingkat Kematangan.

(2) Kategori Tingkat Kematangan sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. level 1 (satu), dengan nilai kematangan pada rentang indeks 0 (nol) – 1,50 (satu koma lima nol) dinamakan level awal;
   b. level 2 (dua), dengan dengan nilai kematangan pada rentang indeks 1,51 (satu koma lima satu) – 2,50 (dua koma lima nol) dinamakan level berulang;
   c. level 3 (tiga), dengan nilai kematangan pada rentang indeks 2,51 (dua koma lima satu) – 3,50 (tiga koma lima nol) dinamakan level terdefinisi;
   d. level 4 (empat), dengan nilai kematangan pada rentang indeks 3,51 (tiga koma lima satu) – 4,50 (empat koma lima nol) dinamakan level terkelola; dan
   e. level 5 (lima), dengan nilai kematangan pada rentang indeks 4,51 (empat koma lima satu) – 5,0 (lima koma nol) dinamakan level inovatif.

(2) Kategori Tingkat Kematangan level 1 (satu) sebagaimana dimaksud pada ayat (2) huruf a dengan kriteria:
   a. menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi awal;
   b. penerapan Keamanan Siber belum memiliki prosedur yang terorganisir;
   c. penerapan Keamanan Siber bersifat informal;
   d. Keamanan Siber tidak dilakukan secara konsisten dan berkelanjutan; dan
   e. dokumen manajemen risiko dan dokumen kontrol belum disusun.

(3) Kategori Tingkat Kematangan level 2 (dua) sebagaimana dimaksud pada ayat (2) huruf b dengan kriteria:
   a. menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang berulang;
   b. penerapan Keamanan Siber sudah memiliki prosedur yang terorganisir;
   c. penerapan Keamanan Siber bersifat informal;
   d. Keamanan Siber dilakukan secara berulang namun belum konsisten dan belum berkelanjutan; dan
   e. dokumen manajemen risiko dan dokumen kontrol sudah disusun namun belum ditetapkan.

(4) Kategori Tingkat Kematangan level 3 (tiga) sebagaimana dimaksud pada ayat (2) huruf c dengan kriteria:
   a. menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang telah terdefinisi dengan baik;
   b. penerapan Keamanan Siber telah terorganisir dengan jelas;
   c. penerapan Keamanan Siber bersifat formal;
   d. Keamanan Siber dilakukan secara berulang dan konsisten serta direviu secara berkala; dan
   e. dokumen manajemen risiko dan dokumen kontrol sudah disusun dan sudah ditetapkan.

(5) Kategori Tingkat Kematangan level 4 (empat) sebagaimana dimaksud pada ayat (2) huruf d dengan kriteria:

a. menggambarkan kondisi penerapan Keamanan Siber dalam tahap implementasi yang telah terkelola dengan baik.
b. penerapan Keamanan Siber telah terorganisir dengan baik namun belum dilakukan proses otomatisasi;
c. penerapan Keamanan Siber bersifat formal;
d. Keamanan Siber dilakukan secara berulang dan implementasi perbaikan dilakukan berkelanjutan; dan
e. dokumen manajemen risiko dan dokumen kontrol sudah disusun dan sudah ditetapkan.

(6) Kategori Tingkat Kematangan level 5 (lima) sebagaimana dimaksud pada ayat (2) huruf e dengan kriteria:
a. menggambarkan kondisi penerapan Keamanan Siber telah diimplementasikan secara optimal;
b. penerapan Keamanan Siber telah terorganisir dengan baik dan telah dilakukan proses otomatisasi;
c. penerapan Keamanan Siber bersifat formal;
d. Keamanan siber dilakukan secara berulang dan konsisten serta telah terintegrasi;
e. keamanan siber menjadi bagian budaya organisasi secara menyeluruh; dan
f. dokumen manajemen risiko dan dokumen kontrol sudah ditetapkan.

Pasal 6

(1) Pelaporan hasil pengukuran Tingkat Kematangan sebagaimana dimaksud dalam Pasal 2 huruf b disampaikan oleh Penyelengara IIV kepada Kementerian atau Lembaga paling sedikit 1 (satu) kali dalam 1 (satu) tahun sesuai dengan ketentuan yang ditetapkan oleh Kementerian atau Lembaga.
(2) Pelaporan sebagaimana dimaksud pada ayat (1) disampaikan dengan menyertakan:
a. surat penyampaian hasil pengukuran Tingkat Kematangan;
b. hasil penilaian mandiri yang telah diotorisasi oleh pejabat yang berwenang mewakili Penyelenggara IIV;
c. bukti pendukung; dan
d. informasi narahubung.
(3) Kementerian atau Lembaga wajib menginformasikan pelaporan hasil pengukuran Tingkat Kematangan sebagaimana dimaksud pada ayat (1) kepada Kepala Badan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
(4) Dalam hal Kementerian atau Lembaga sebagai Penyelenggara IIV, pelaporan hasil pengukuran Tingkat Kematangan disampaikan oleh Kementerian atau Lembaga kepada Badan.

Pasal 7

(1) Kementerian atau Lembaga melakukan verifikasi hasil pengukuran Tingkat Kematangan berdasarkan pelaporan sebagaimana dimaksud dalam Pasal 6 ayat (1).

(2) Badan melakukan verifikasi hasil pengukuran Tingkat Kematangan berdasarkan pelaporan sebagaimana dimaksud dalam Pasal 6 ayat (4).

Pasal 8

(1) Verifikasi hasil pengukuran Tingkat Kematangan sebagaimana dimaksud dalam Pasal 7 dilakukan dengan metode paling sedikit:
   a. penelaahan dokumen;
   b. wawancara;
   c. observasi lapangan; dan
   d. pemeriksaan kesesuaian antara hasil penilaian mandiri dan bukti dukungnya.
(2) Dalam melakukan verifikasi sebagaimana dimaksud pada ayat (1), Kementerian atau Lembaga dapat mengikutsertakan Badan.

Pasal 9

(1) Kementerian atau Lembaga wajib menyampaikan hasil verifikasi pengukuran Tingkat Kematangan sebagaimana dimaksud dalam Pasal 8 kepada Badan dan Penyelenggara IIV.
(2) Penyampaian hasil verifikasi pengukuran Tingkat Kematangan sebagaimana dimaksud pada ayat (1) dilakukan paling lambat bulan Januari tahun berikutnya.
(3) Hasil verifikasi sebagaimana dimaksud pada ayat (2) sesuai dengan format yang tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 10

Dalam hal Badan melakukan verifikasi pengukuran Tingkat Kematangan sebagaimana dimaksud dalam Pasal 7 ayat (2), Badan menyampaikan hasil verifikasi kepada Kementerian atau Lembaga paling lambat bulan Januari tahun berikutnya.

Pasal 11

(1) Ketentuan mengenai pengukuran Tingkat Kematangan yang diatur dalam Peraturan Badan ini menjadi acuan dalam hal Kementerian atau Lembaga akan menetapkan peraturan tentang pengukuran Tingkat Kematangan di lingkup sektor.
(2) Dalam menetapkan peraturan mengenai pengukuran Tingkat Kematangan sebagaimana dimaksud pada ayat (1), Kementerian atau Lembaga berkoordinasi dengan Badan.

Pasal 12

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 16 Oktober 2023

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 3 November 2023

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

ttd.

ASEP N. MULYANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2023 NOMOR 875

LAMPIRAN
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 10 TAHUN 2023
TENTANG PENGUKURAN TINGKAT KEMATANGAN KEAMANAN SIBER

FORMAT HASIL VERIFIKASI PENGUKURAN
TINGKAT KEMATANGAN KEAMANAN SIBER

Nama Kota, Tanggal

Nomor :
Sifat :
Lampiran :

Kepada Yth.
Kepala Badan Siber dan Sandi Negara/Penyelenggara IIV
Di Tempat

Dengan Hormat,
Dengan ini kami menyampaikan hasil verifikasi pengukuran Tingkat Kematangan Keamanan Siber pada Sektor ... yang merupakan cerminan hasil pengukuran tingkat kematangan keamanan siber pada Penyelenggara IIV sebagai berikut :
1. Nama Penyelenggara IIV
2. Nama Penyelenggara IIV
3. dst

Berikut terlampir dokumen hasil verifikasi pengukuran tingkat kematangan keamanan siber dan profil kematangan keamanan siber sektor ...
Demikian disampaikan, atas perhatian dan kerjasamanya diucapkan terima kasih

Pimpinan Instansi/Perusahaan,

(.....)

HASIL VERIFIKASI
PENGUKURAN TINGKAT KEMATANGAN KEAMANAN SIBER

I. Gambaran Umum
1. Nama Penyelenggara IIV
2. Nama Sistem Elektronik
3. Sektor
4. Deskripsi model bisnis
5. Deskripsi singkat fungsi Sistem Elektronik dan proses bisnis Sistem Elektronik
6. Keterangan Data Pribadi yang diproses

II. Ruang Lingkup Pengukuran
Pengukuran tingkat kematangan keamanan siber meliputi Domain pada kerangka kerja yaitu:
a. Identifikasi;
b. Proteksi;
c. Deteksi; dan
d. Penanggulangan dan pemulihan

III. Metodologi Kegiatan
Metodologi yang digunakan berdasarkan hasil pengisian instrumen penilaian, wawancara/diskusi, dan melihat ketersediaan dokumen keamanan siber.

IV. Pelaksanaan Kegiatan
Pelaksanaan kegiatan menjelaskan pelaksanaan verifikasi hasil pengukuran tingkat kematangan, meliputi kegiatan pelaksanaan penilaian mandiri, waktu pelaksanaan penilaian mandiri, waktu pelaksanaan verifikasi hasil pengukuran dan hal lain terkait pelaksanaan kegiatan

V. Hasil Kegiatan
Hasil kegiatan verifikasi dari pengukuran terhadap domain-domain yang diukur, yang mencerminkan kekuatan dan kekurangan organisasi dalam mewujudkan kematangan keamanan siber, dan rencana aksi yang perlu dilakukan organisasi dalam rangka memperbaiki kekurangan dan mempertahankan serta senantiasa berinovatif untuk menjaga ketahanan dan keamanan siber.

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN