PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 8 TAHUN 2021
TENTANG
PENYELENGGARAAN PENILAIAN KESIAPAN PENERAPAN SNI ISO/IEC 27001 MENGGUNAKAN INDEKS KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang : a. bahwa untuk mempersiapkan penerapan SNI ISO/IEC 27001, penyelenggara sistem elektronik dapat melakukan penilaian berdasarkan indeks keamanan informasi;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Penyelenggaraan Penilaian Kesiapan Penerapan SNI ISO/IEC 27001 Menggunakan Indeks Keamanan Informasi;

Mengingat : 1. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);

2. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);

3. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan

Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);

4. 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);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG PENYELENGGARAAN PENILAIAN KESIAPAN PENERAPAN SNI ISO/IEC 27001 MENGGUNAKAN INDEKS KEAMANAN INFORMASI .

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 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.
3. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersedian, dan kenirsangkalan informasi.
4. Indeks Keamanan Informasi yang selanjutnya disebut Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di organisasi.
5. Asesor Indeks KAMI adalah orang yang diberikan tugas dan tanggung jawab untuk melakukan verifikasi terhadap hasil penilaian Indeks KAMI.

6. Sertifikat Indeks KAMI adalah bukti tertulis yang dikeluarkan oleh Badan Siber dan Sandi Negara bagi PSE yang telah memenuhi kriteria yang ditetapkan.
7. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan sandi.

Pasal 2

Penyelenggaraan penilaian kesiapan penerapan SNI ISO/IEC 27001 menggunakan Indeks KAMI meliputi:

a. penilaian mandiri berdasarkan Indeks KAMI;
b. pengajuan permohonan verifikasi hasil penilaian mandiri;
c. verifikasi hasil penilaian mandiri; dan
d. penetapan verifikasi hasil penilaian Indeks KAMI.

Pasal 3

(1) Penilaian mandiri berdasarkan Indeks KAMI sebagaimana dimaksud dalam Pasal 2 huruf a dilaksanakan oleh PSE sesuai dengan Indeks KAMI versi terkini yang ada di situs web resmi BSSN.
(2) Penilaian mandiri sebagaimana dimaksud pada ayat (1) dilakukan dengan mengevaluasi aspek Indeks KAMI paling sedikit meliputi:
    a. tata kelola;
    b. pengelolaan risiko;
    c. kerangka kerja Keamanan Informasi;
    d. pengelolaan aset; dan
    e. teknologi dan Keamanan Informasi.
(3) Tata kelola sebagaimana dimaksud pada ayat (2) huruf a dilakukan dengan mengevaluasi kelengkapan kebijakan, prosedur, fungsi, tugas, dan tanggung jawab pengelolaan Keamanan Informasi.
(4) Pengelolaan risiko sebagaimana dimaksud pada ayat (2) huruf b dilakukan dengan mengevaluasi kebijakan, prosedur manajemen risiko, *risk register*, tugas dan tanggung jawab pengelolaan risiko Keamanan Informasi.

(5) Kerangka kerja Keamanan Informasi sebagaimana dimaksud pada ayat (2) huruf c dilakukan dengan mengevaluasi kelengkapan dokumen keamanan informasi maupun efektivitas penerapannya yang meliputi dokumen:
   a. *business continuity plan*;
   b. *disaster recovery plan*;
   c. pengelolaan insiden Keamanan Informasi;
   d. pengembangan perangkat lunak yang aman;
   e. strategi penerapan Keamanan Informasi; dan
   f. kepatuhan terhadap regulasi Keamanan Informasi.

(6) Pengelolaan aset sebagaimana dimaksud pada ayat (2) huruf d dilakukan dengan:
   a. mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset; dan
   b. memeriksa terkait pengamanan fisik.

(7) Teknologi dan Keamanan Informasi sebagaimana dimaksud pada ayat (2) huruf e dilakukan dengan mengevaluasi kelengkapan, konsistensi, dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Pasal 4

(1) Evaluasi sebagaimana dimaksud dalam Pasal 3 ayat (2) dilakukan dengan:
   a. pemeriksaan kelengkapan dokumen kebijakan dan/atau prosedur; dan
   b. pemeriksaan penerapan dokumen kebijakan dan/atau prosedur.

(2) Setiap pertanyaan pada aspek evaluasi sebagaimana dimaksud dalam Pasal 3 ayat (2) terdiri atas 4 (empat) pilihan jawaban:
   a. tidak dilakukan;
   b. dalam perencanaan;
   c. dalam penerapan atau penerapan sebagian; atau
   d. diterapkan secara menyeluruh.

(3) Tidak dilakukan sebagaimana dimaksud pada ayat (2) huruf a jika PSE tidak memiliki dokumen kebijakan dan/atau prosedur.

(4) Dalam perencanaan sebagaimana dimaksud pada ayat (2) huruf b jika PSE telah menyusun dokumen kebijakan dan/atau prosedur tetapi belum ditetapkan.

(5) Dalam penerapan atau penerapan sebagian sebagaimana dimaksud pada ayat (2) huruf c jika PSE telah menetapkan dokumen kebijakan dan/atau prosedur tetapi belum diterapkan secara menyeluruh.

(6) Diterapkan secara menyeluruh sebagaimana dimaksud pada ayat (2) huruf d jika PSE telah menetapkan dan menerapkan secara menyeluruh dokumen kebijakan dan/atau prosedur.

Pasal 5

(1) Pengajuan permohonan verifikasi hasil penilaian mandiri sebagaimana dimaksud dalam Pasal 2 huruf b disampaikan oleh PSE secara tertulis kepada Kepala BSSN.

(2) Permohonan verifikasi sebagaimana dimaksud pada ayat (1) dilengkapi dengan dokumen:
   a. surat permohonan;
   b. kelengkapan pengajuan verifikasi penilaian Indeks KAMI;
   c. daftar ketersediaan dokumen;
   d. Indeks KAMI yang telah diisi oleh PSE; dan
   e. informasi narahubung PSE.

(3) Format dokumen permohonan sebagaimana dimaksud pada ayat (2) huruf a, huruf b, dan huruf c tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Badan ini.

Pasal 6

(1) Verifikasi hasil penilaian mandiri sebagaimana dimaksud dalam Pasal 2 huruf c dilakukan setelah permohonan

sebagaimana dimaksud dalam Pasal 5 ayat (2) dinyatakan lengkap.

(2) Verifikasi sebagaimana dimaksud pada ayat (1) dilaksanakan melalui tahap:
   a. verifikasi kelengkapan dokumen kebijakan dan/atau prosedur; dan
   b. verifikasi penerapan dokumen kebijakan dan/atau prosedur.

(3) Verifikasi sebagaimana dimaksud pada ayat (2) menghasilkan skor akhir yang menunjukkan tingkat kesiapan PSE dalam pemenuhan kriteria SNI ISO/IEC 27001.

(4) Tingkat kesiapan sebagaimana dimaksud pada ayat (3) terdiri atas:
   a. baik;
   b. cukup baik;
   c. pemenuhan kerangka kerja dasar; dan
   d. tidak layak.

(5) Tingkat kesiapan sebagaimana dimaksud pada ayat (4) diberikan sesuai kategorisasi Sistem Elektronik yang dimiliki oleh PSE meliputi:
   a. Sistem Elektronik kategori strategis;
   b. Sistem Elektronik kategori tinggi; dan
   c. Sistem Elektronik kategori rendah.

(6) PSE yang memiliki Sistem Elektronik kategori strategis sebagaimana dimaksud pada ayat (5) huruf a diberikan nilai tingkat kesiapan:
   a. baik, jika mendapatkan skor akhir penilaian Indeks KAMI pada rentang 610 (enam ratus sepuluh) sampai dengan 645 (enam ratus empat puluh lima);
   b. cukup baik, jika mendapatkan skor akhir penilaian Indeks KAMI pada rentang 536 (lima ratus tiga puluh enam) sampai dengan 609 (enam ratus sembilan);
   c. pemenuhan kerangka kerja dasar, jika mendapatkan skor akhir penilaian Indeks KAMI pada rentang 334 (tiga ratus tiga puluh empat) sampai dengan 535 (lima ratus tiga puluh lima); dan

d. tidak layak, mendapatkan skor akhir penilaian Indeks KAMI pada rentang 0 (nol) sampai dengan 333 (tiga ratus tiga puluh tiga).

(7) PSE yang memiliki Sistem Elektronik kategori tinggi sebagaimana dimaksud pada ayat (5) huruf b diberikan nilai tingkat kesiapan:

a. baik, jika mendapatkan skor akhir penilaian Indeks KAMI pada rentang 584 (lima ratus delapan puluh empat) sampai dengan 645 (enam ratus empat puluh lima);

b. cukup baik, jika mendapatkan skor akhir penilaian Indeks KAMI pada rentang 456 (empat ratus lima puluh enam) sampai dengan 583 (lima ratus delapan puluh tiga);

c. pemenuhan kerangka kerja dasar, jika mendapatkan skor akhir penilaian Indeks KAMI pada rentang 273 (dua ratus tujuh puluh tiga) sampai dengan 455 (empat ratus lima puluh lima); dan

d. tidak layak, mendapatkan skor akhir penilaian Indeks KAMI pada rentang 0 (nol) sampai dengan 272 (dua ratus tujuh puluh dua).

(8) PSE yang memiliki Sistem Elektronik kategori rendah sebagaimana dimaksud pada ayat (5) huruf c diberikan nilai tingkat kesiapan:

a. baik, jika mendapatkan skor akhir penilaian Indeks KAMI pada rentang 175 (seratus tujuh puluh lima) sampai dengan 312 (tiga ratus dua belas);

b. cukup baik, jika mendapatkan skor akhir penilaian Indeks KAMI pada rentang 313 (tiga ratus tiga belas) sampai dengan 535 (lima ratus tiga puluh lima);

c. pemenuhan kerangka kerja dasar, jika mendapatkan skor akhir penilaian Indeks KAMI pada rentang 175 (seratus tujuh puluh lima) sampai dengan 312 (tiga ratus dua belas); dan

d. tidak layak, mendapatkan skor akhir penilaian Indeks KAMI pada rentang 0 (nol) sampai dengan 174 (seratus tujuh puluh empat).

Pasal 7

(1) Verifikasi sebagaimana dimaksud dalam Pasal 6 dilakukan oleh tim Asesor Indeks KAMI BSSN.
(2) Tim Asesor Indeks KAMI sebagaimana dimaksud pada ayat (1) ditetapkan oleh Kepala BSSN.

Pasal 8

(1) Penetapan verifikasi hasil penilaian Indeks KAMI sebagaimana dimaksud dalam Pasal 2 huruf d disusun dalam bentuk laporan yang memuat:
    a. tingkat kesiapan PSE dalam menerapkan SNI ISO/IEC 27001; dan
    b. deskripsi kekuatan, kelemahan, dan rekomendasi seluruh aspek Indeks KAMI.
(2) Laporan sebagaimana dimaksud pada ayat (1) disampaikan oleh BSSN kepada PSE.
(3) Laporan sebagaimana dimaksud pada ayat (2) disertai dengan Sertifikat Indeks KAMI bagi PSE yang memperoleh nilai tingkat kesiapan baik atau cukup baik.

Pasal 9

Pendanaan kegiatan verifikasi penilaian Indeks KAMI dibebankan pada:

a. anggaran pendapatan dan belanja negara;
b. anggaran pendapatan dan belanja daerah; dan/atau
c. sumber pendanaan lainnya yang sah dan tidak mengikat.

Pasal 10

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 25 Agustus 2021

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN

Diundangkan di Jakarta
pada tanggal 27 Agustus 2021

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

ttd.

BENNY RIYANTO

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2021 NOMOR 975

LAMPIRAN
PERATURAN BADAN SIBER DAN SANDI NEGARA
NOMOR 8 TAHUN 2021
TENTANG
PENYELENGGARAAN PENILAIAN KESIAPAN PENERAPAN SNI ISO/IEC 27001 MENGGUNAKAN INDEKS KEAMANAN INFORMASI

FORMAT SURAT PERMOHONAN VERIFIKASI HASIL PENILAIAN MANDIRI INDEKS KAMI

[Nama PSE]
[Alamat PSE]
[Nomor Telepon dan Surel PSE]

[Nama Kota, Tanggal]

Nomor :
Sifat :
Lampiran :

Kepada Yth.
Kepala Badan Siber dan Sandi Negara
di Tempat

Dengan Hormat,
Dengan ini kami mengajukan permohonan untuk verifikasi hasil penilaian mandiri Indeks Keamanan Informasi (Indeks KAMI) dengan ruang lingkup asesmen sebagai berikut:
Nama PSE :
Nama Sistem Elektronik:
Ruang Lingkup :

untuk melengkapi permohonan ini, kami lampirkan dokumen sebagai berikut:
1. Kelengkapan Pengajuan Verifikasi Penilaian Indeks KAMI
2. Indeks KAMI yang telah diisi oleh PSE

Demikian disampaikan, untuk koordinasi lebih lanjut, dapat menghubungi Sdr/Sdri..... /(no HP/WA). Atas perhatian dan kerjasamanya diucapkan terima kasih.

Pimpinan Perusahaan

(.....)

KELENGKAPAN PENGAJUAN VERIFIKASI PENILAIAN INDEKS KAMI

KELENGKAPAN PENGAJUAN VERIFIKASI PENILAIAN INDEKS KAMI

1. GAMBARAN UMUM

   a. Nama Penyelenggara Sistem Elktronik (PSE)

      .....

   b. Nama Sistem Elektronik
      .....

   c. Sektor Sistem Elektronik
      .....

   d. *Uniform Resource Locator (URL) website*
      .....

   e. Deskripsi model bisnis

      .....

      .....

      .....

   f. Deskripsi singkat fungsi Sistem Elektronik dan proses bisnis Sistem Elektronik

      .....

      .....

      .....

   g. Keterangan Data Pribadi yang diproses

      .....

      .....

      .....

2. RUANG LINGKUP

a. Nama Sistem
.....

b. Unit Kerja/Bagian/Divisi Terkait
.....

c. Lokasi diisi lokasi yang termasuk dalam ruang lingkup. Misal Data Center, Kantor Pusat)

No	Nama Lokasi	Alamat
1		
2		
3		

d. Aset TI kritikal

1) Informasi (*apa saja yang penting dilindungi kerahasiaan/keutuhan/ ketersediaannya*)

.....
.....
.....

2) Aplikasi Utama

.....
.....
.....

3) Server Utama

.....
.....
.....
.....

e. *Data Center* / Server Utama disimpan dalam ruangan khusus?

□ Ya □ Tidak

f. *Data Recovery Center* (DRC) tersedia?

□ Ya □ Tidak

Jika Ya, siapa pengelola fasilitas DRC:

□ Dikelola oleh internal Instansi/Lembaga □ Dikelola vendor (*outsourced*)

DAFTAR KETERSEDIAAN DOKUMEN (KEBIJAKAN/PROSEDUR)

No	Nama Kebijakan	Cakupan Dokumen	Ada/Tidak
1	Kebijakan Keamanan Informasi	Menyatakan komitmen manajemen/ pimpinan instansi/lembaga menyangkut pengamanan informasi yang didokumentasikan dan disahkan secara formal. Kebijakan keamanan informasi dapat mencakup antara lain: • Definisi, sasaran dan ruang lingkup keamanan informasi • Persetujuan terhadap kebijakan dan program keamanan informasi • Kerangka kerja penetapan sasaran kontrol dan kontrol • Struktur dan metodologi manajemen risiko • Organisasi dan tanggungjawab keamanan informasi	
2	Organisasi, peran dan tanggungjawab keamanan informasi	Uraian tentang organisasi yang ditetapkan untuk mengelola dan mengkoordinasikan aspek keamanan informasi dari suatu instansi/lembaga serta uraian peran dan tanggungjawabnya. Organisasi pengelola keamanan informasi tidak harus berbentuk unit kerja terpisah	
3	Panduan Klasifikasi Informasi	Berisi tentang petunjuk cara melakukan klasifikasi informasi yang ada di instansi/lembaga dan disusun dengan memperhatikan nilai penting dan kritikalitas informasi bagi penyelenggaraan pelayanan publik, baik yang dihasilkan secara intenal maupun diterima dari pihak eksternal. Klasifikasi informasi dilakukan dengan mengukur dampak gangguan operasional, jumlah kerugian uang, penurunan reputasi dan legal manakala terdapat ancaman menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi.	
4	Kebijakan Manajemen Risiko TIK	Berisi metodologi / ketentuan untuk mengkaji risiko mulai dari identifikasi aset, kelemahan, ancaman dan dampak kehilangan aspek kerahasiaan, keutuhan dan ketersediaan informasi termasuk jenis mitigasi risiko dan tingkat penerimaan risiko yang disetujui oleh pimpinan.	

5	Kerangka Kerja Manajemen Kelangsungan Usaha (*Business Continuity Management*)	Berisi komitmen menjaga kelangsungan pelayanan publik dan proses penetapan keadaan bencana serta penyediaan infrastruktur TIK pengganti saat infrastruktur utama tidak dapat beroperasi agar pelayanan publik tetap dapat berlangsung bila terjadi keadaan bencana/k darurat. Dokumen ini juga memuat tim yang bertanggungjawab (ketua dan anggota tim), lokasi kerja cadangan, skenario bencana dan rencana pemulihan ke kondisi normal setelah bencana dapat diatasi/berakhir.	
6	Kebijakan Penggunaan Sumber daya TIK	Berisi aturan penggunaan komputer (desktop/laptop/modem atau *email* dan internet).	

No	**Nama Prosedur/ Pedoman**	**Cakupan Dokumen**	**Ada/Tidak**
1	Pengendalian Dokumen	Berisi proses penyusunan dokumen, wewenang persetujuan penerbitan, identifikasi perubahan, distribusi, penyimpanan, penarikan dan pemusnahan jika tidak digunakan, daftar dan pengendalian dokumen eksternal yang menjadi rujukan	
2	Pengendalian Rekaman	Berisi pengelolaan rekaman yang meliputi: identifikasi rekaman penting, kepemilikan, pengamanan, masa retensi, dan pemusnahan jika tidak digunakan lagi	
3	Audit Internal SMKI	Proses audit internal: rencana, ruang lingkup, pelaksanaan, pelaporan dan tindak lanjut hasil audit serta persyaratan kompetensi auditor	
4	Tindakan Perbaikan & Pencegahan	Berisi tatacara perbaikan/pencegahan terhadap masalah/gangguan/insiden baik teknis maupun non teknis yang terjadi dalam pengembangan, operasional maupun pemeliharaan TI	

5	Pelabelan, Pengamanan, Pertukaran & *Disposal* Informasi	Aturan pelabelan, penyimpanan, distribusi, pertukaran, pemusnahan informasi/daya "rahasia" baik *softcopy* maupun *hardcopy*, baik milik instansi maupun informasi pelanggan/mitra yang dipercayakan kepada Instansi	
6	Pengelolaan *Removable Media* & *Disposal* Media	Aturan penggunaan, penyimpanan, pemindahan, pengamanan media simpan informasi (*tape*/*hard disk*/*Flashdisk*/CD) dan penghapusan informasi ataupun penghancuran media	
7	Pemantauan (*Monitoring*) Penggunaan Fasilitas TIK	Berisi proses *monitoring* penggunaan CPU, *storage*, *email*, internet, fasilitas TIK lainnya dan pelaporan serta tindak lanjut hasil *monitoring*	
8	*User Access Management*	Berisi proses dan tatacara pendaftaran, penghapusan dan *review* hak akses *user*, termasuk administrator, terhadap sumber daya informasi (aplikasi, sistem operasi, *database*, internet, *email* dan internet)	
9	*Teleworking*	Pengendalian dan pengamanan penggunaan hak akses secara *remote* (misal melalui modem atau jaringan). Siapa yang berhak menggunakan dan cara mengontrol agar penggunaannya aman.	
10	Pengendalian instalasi software & Hak Kekayaan Intelektual	Berisi daftar *software* standar yang diijinkan di Instansi, permintaan pemasangan dan pelaksana pemasangan termasuk penghapusan *software* yang tidak diijinkan	
11	Pengelolaan Perubahan (*Change Management*) TIK	Proses permintaan dan persetujuan perubahan aplikasi/infrastruktur TIK, serta pengkinian konfigurasi/*database*/versi dari aset TIK yang mengalami perubahan.	
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi	Proses pelaporan & penanganan gangguan/insiden baik menyangkut ketersediaan layanan atau gangguan karena penyusupan/pengubahan informasi secara tidak berwenang. Termasuk analisis penyebab dan eskalasi jika diperlukan tindak lanjut ke aspek legal.	

KEPALA BADAN SIBER DAN SANDI NEGARA,

ttd.

HINSA SIBURIAN