****

PERATURAN BADAN SIBER DAN SANDI NEGARA

NOMOR TAHUN 2021

TENTANG

PENYELENGGARAAN PENILAIAN 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;

1. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Badan Siber dan Sandi Negara tentang Penyelenggaraan Penilaian 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 9 Tahun 2020 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2020 Nomor 1464);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN SIBER DAN SANDI NEGARA TENTANG PENYELENGGARAAN PENILAIAN INDEKS KEAMANAN INFORMASI.

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. Sistem Manajemen Pengamanan Informasi yang selanjutnya disingkat SMPI adalah pengaturan kewajiban bagi Penyelenggara Sistem Elektronik dalam penerapan manajemen pengamanan informasi berdasarkan asas risiko.
4. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersedian, dan kenirsangkalan informasi.
5. Indeks Keamanan Informasi yang selanjutnya disebut Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di organisasi.
6. Asesor Indeks KAMI adalah orang yang diberikan tugas dan tanggung jawab untuk melakukan verifikasi terhadap hasil penilaian Indeks KAMI.
7. Sertifikat Indeks KAMI adalah bukti tertulis yang dikeluarkan oleh Badan Siber dan Sandi Negara bagi Penyelenggara Sistem Elektronik yang telah memenuhi kriteria yang ditetapkan.
8. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan sandi.
9. Penyelenggaraan penilaian Indeks KAMI merupakan kegiatan untuk menilai tingkat kesiapan PSE dalam menerapkan SNI ISO/IEC 27001.
10. Penyelenggaraan penilaian Indeks KAMI sebagaimana dimaksud pada ayat (1) meliputi:
11. penilaian mandiri berdasarkan Indeks KAMI;
12. pengajuan permohonan verifikasi hasil penilaian mandiri;
13. verifikasi hasil penilaian mandiri; dan
14. penetapan verifikasi hasil penilaian Indeks KAMI.
15. Penilaian mandiri berdasarkan Indeks KAMI sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a dilaksanakan oleh PSE sesuai dengan Indeks KAMI versi terkini yang ada di situs web resmi BSSN.
16. Penilaian mandiri sebagaimana dimaksud pada ayat (1) dilakukan dengan mengevaluasi aspek Indeks KAMI paling sedikit meliputi:
17. tata kelola;
18. pengelolaan risiko;
19. kerangka kerja keamanan informasi;
20. pengelolaan aset; dan
21. teknologi dan keamanan informasi.
22. Tata kelola sebagaimana dimaksud pada ayat (2) huruf a dilakukan dengan mengevaluasi kelengkapan kebijakan, prosedur, fungsi, tugas, dan tanggung jawab pengelolaan keamanan informasi.
23. 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.
24. Kerangka kerja keamanan informasi sebagaimana dimaksud pada ayat (2) huruf c dilakukan dengan mengevaluasi kelengkapan dokumen keamanan informasi maupun efektifitas penerapannya yang meliputi dokumen *business continuity plan*, *disaster recovery plan*, pengelolaan insiden keamanan informasi, pengembangan perangkat lunak yang aman, strategi penerapan keamanan informasi, dan kepatuhan terhadap regulasi keamanan informasi.
25. Pengelolaan aset sebagaimana dimaksud pada ayat (2) huruf d dilakukan dengan mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut serta memeriksa terkait pengamanan fisik.
26. Teknologi dan keamanan informasi sebagaimana dimaksud pada ayat (2) huruf e dilakukan dengan mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.
27. Evaluasi aspek Indeks KAMI sebagaimana dimaksud dalam Pasal 3 ayat (2) dilakukan dengan:
28. pemeriksaan kelengkapan dokumen kebijakan dan/atau prosedur; dan
29. pemeriksanaan penerapan dokumen kebijakan dan/atau prosedur.
30. Masing-masing pertanyaan pada setiap aspek Indeks KAMI sebagaimana dimaksud dalam Pasal 3 ayat (2) terdiri atas 4 (empat) pilihan jawaban:
31. tidak dilakukan;
32. dalam perencanaan;
33. dalam penerapan atau penerapan sebagian; dan
34. diterapkan secara menyeluruh.
35. Tidak dilakukan sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf a jika PSE tidak memiliki dokumen kebijakan dan/atau prosedur.
36. Dalam perencanaan sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b jika PSE telah menyusun dokumen kebijakan dan/atau prosedur tetapi belum ditetapkan.
37. Dalam penerapan atau penerapan sebagian sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf c jika PSE telah menetapkan dokumen kebijakan dan/atau prosedur ~~dan telah ditetapkan secara formal akan~~ tetapi belum diterapkan secara menyeluruh oleh PSE.
38. Diterapkan secara menyeluruh sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf d jika PSE telah menetapkan dokumen kebijakan dan/atau prosedur ~~dan telah ditetapkan secara formal~~ serta diterapkan secara menyeluruh oleh PSE.
39. Pengajuan permohonan verifikasi hasil penilaian mandiri sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b disampaikan oleh PSE secara tertulis kepada Kepala BSSN.
40. Permohonan sebagaimana dimaksud pada ayat (1) disampaikan dengan melampirkan:
41. Indeks KAMI yang telah diisi oleh PSE;
42. dokumen kebijakan dan/atau prosedur; dan
43. informasi narahubung PSE.
44. Verifikasi hasil penilaian mandiri sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf c dilakukan setelah permohonan sebagaimana dimaksud dalam Pasal 5 ayat (2) dinyatakan lengkap.
45. Verifikasi sebagaimana dimaksud pada ayat (1) dilaksanakan melalui tahap:
46. verifikasi kelengkapan dokumen kebijakan dan/atau prosedur; dan
47. verifikasi penerapan dokumen kebijakan dan/atau prosedur.
48. Verifikasi sebagaimana dimaksud pada ayat (2) menghasilkan skor akhir yang menunjukkan tingkat kesiapan PSE dalam pemenuhan kriteria SNI ISO/IEC 27001.
49. Tingkat kesiapan sebagaimana dimaksud pada ayat (3) terdiri atas:
50. baik;
51. cukup baik;
52. pemenuhan kerangka kerja dasar; dan
53. tidak layak.
54. Tingkat kesiapan baik sebagaimana dimaksud pada ayat (4) huruf a diperoleh jika:
55. PSE yang memiliki Sistem Elektronik kategori rendah mendapatkan skor akhir penilaian Indeks KAMI pada rentang 536 (lima ratus tiga puluh enam) sampai dengan 645 (enam ratus empat puluh lima);
56. PSE yang memiliki Sistem Elektronik kategori tinggi mendapatkan skor akhir penilaian Indeks KAMI pada rentang 584 (lima ratus delapan puluh empat) sampai dengan 645 (enam ratus empat puluh lima); atau
57. PSE yang memiliki Sistem Elektronik kategori strategis mendapatkan skor akhir penilaian Indeks KAMI pada rentang 610 (enam ratus sepuluh) sampai dengan 645 (enam ratus empat puluh lima).
58. Tingkat kesiapan cukup baik sebagaimana dimaksud pada ayat (4) huruf b diperoleh jika:
59. PSE yang memiliki Sistem Elektronik kategori rendah mendapatkan skor akhir penilaian Indeks KAMI pada rentang 313 (tiga ratus tiga belas) sampai dengan 535 (lima ratus tiga puluh lima);
60. PSE yang memiliki Sistem Elektronik kategori tinggi mendapatkan skor akhir penilaian Indeks KAMI pada rentang 456 (empat ratus lima puluh enam) sampai dengan 583 (lima ratus delapan puluh tiga); atau
61. PSE yang memiliki Sistem Elektronik kategori strategis mendapatkan skor akhir penilaian Indeks KAMI pada rentang 536 (lima ratus tiga puluh enam) sampai dengan 609 (enam ratus sembilan).
62. Tingkat kesiapan pemenuhan kerangka kerja dasar sebagaimana dimaksud pada ayat (4) huruf c diperoleh jika:
63. PSE yang memiliki Sistem Elektronik kategori rendah mendapatkan skor akhir penilaian Indeks KAMI pada rentang 175 (seratus tujuh puluh lima) sampai dengan 312 (tiga ratus dua belas);
64. PSE yang memiliki Sistem Elektronik kategori tinggi mendapatkan skor akhir penilaian Indeks KAMI pada rentang 273 (dua ratus tujuh puluh tiga) sampai dengan 455 (empat ratus lima puluh lima); atau
65. PSE yang memiliki Sistem Elektronik kategori strategis mendapatkan skor akhir penilaian Indeks KAMI pada rentang 334 (tiga ratus tiga puluh empat) sampai dengan 535 (lima ratus tiga puluh lima).
66. Tingkat kesiapan tidak layak sebagaimana dimaksud pada ayat (4) huruf d diperoleh jika:
67. PSE yang memiliki Sistem Elektronik kategori rendah mendapatkan skor akhir penilaian Indeks KAMI pada rentang 0 (nol) sampai dengan 174 (seratus tujuh puluh empat);
68. PSE yang memiliki Sistem Elektronik kategori tinggi mendapatkan skor akhir penilaian Indeks KAMI pada rentang 0 (nol) sampai dengan 272 (dua ratus tujuh puluh dua); atau
69. PSE yang memiliki Sistem Elektronik kategori strategis mendapatkan skor akhir penilaian Indeks KAMI pada rentang 0 (nol) sampai dengan 333 (tiga ratus tiga puluh tiga).
70. Verifikasi sebagaimana dimaksud dalam Pasal 6 dilakukan oleh tim Asesor Indeks KAMI BSSN.
71. Tim Asesor Indeks KAMI sebagaimana dimaksud pada ayat (1) terdiri atas:
    1. pegawai BSSN; dan/atau
    2. pihak lain.
72. Tim Asesor Indeks KAMI sebagaimana dimaksud pada ayat (2) ditetapkan oleh Kepala BSSN.

Asesor Indeks KAMI di tetapkan oleh Kepala BSSN.

1. Penetapan verifikasi hasil penilaian Indeks KAMI sebagaimana dimaksud dalam Pasal 2 ayat (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.

1. Laporan sebagaimana dimaksud pada ayat (1) disampaikan oleh BSSN kepada PSE.
2. Laporan sebagaimana dimaksud pada ayat (2) disertai dengan Sertifikat Indeks KAMI bagi PSE yang memperoleh tingkat kesiapan baik atau cukup baik.

Pendanaan kegiatan verifikasi penilaian Indeks KAMI dibebankan pada anggaran pendapatan belanja negara dan/atau anggaran pendapatan belanja daerah.

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

KEPALA BADAN

PEMBINAAN HUKUM NASIONAL

KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

REPUBLIK INDONESIA,

WIDODO EKATJAHJANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN NOMOR