SOSIALISASI PERMENPAN 59/2020

Keamanan SPBE dalam Evaluasi SPBE

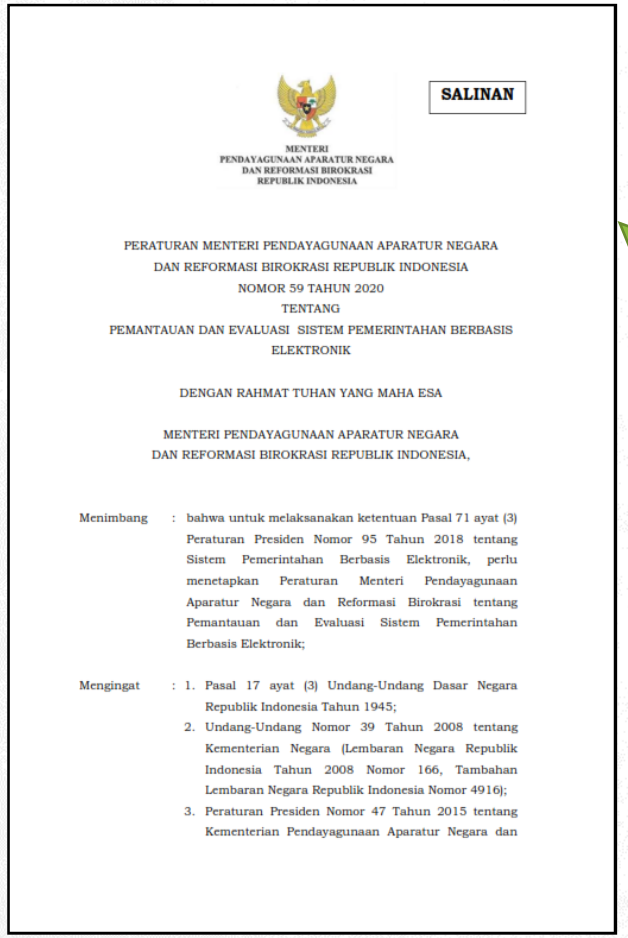
DWI KARDONO, S.Sos., M.A.
Direktur Proteksi Pemerintah
BSSN

19-20 November 2020

AGENDA HARI INI

- Indikator Kematangan Keamanan Informasi
- Tingkat Kematangan Kebijakan Internal Manajemen Keamanan Informasi
- Tingkat Kematangan Penerapan Manajemen Keamanan Informasi
- Tingkat Kematangan Pelaksanaan Audit Keamanan SPBE

DASAR PENGATURAN



SALINAN

MENTERI
PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI
REPUBLIK INDONESIA

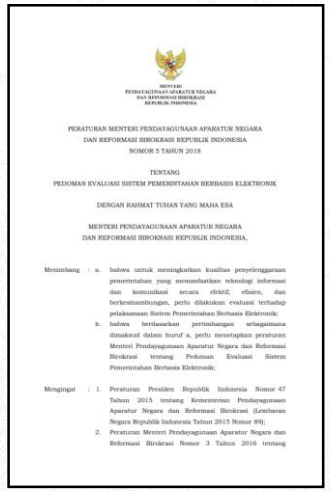
PERATURAN MENTERI PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI REPUBLIK INDONESIA
NOMOR 59 TAHUN 2020
TENTANG
PEMANTAUAN DAN EVALUASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI REPUBLIK INDONESIA,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 71 ayat (3) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat :
1. Pasal 17 ayat (3) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 39 Tahun 2008 tentang Kementerian Negara (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 166, Tambahan Lembaran Negara Republik Indonesia Nomor 4916);
3. Peraturan Presiden Nomor 47 Tahun 2015 tentang Kementerian Pendayagunaan Aparatur Negara dan



PERATURAN MENTERI PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI REPUBLIK INDONESIA
NOMOR 5 TAHUN 2018

TENTANG
PEDOMAN EVALUASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PENDAYAGUNAAN APARATUR NEGARA
DAN REFORMASI BIROKRASI REPUBLIK INDONESIA,

Menimbang : a. bahwa untuk meningkatkan kualitas penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi secara efektif, efisien, dan berkesinambungan, perlu dilakukan evaluasi terhadap pelaksanaan Sistem Pemerintahan Berbasis Elektronik;
b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi tentang Pedoman Evaluasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat : 1. Peraturan Presiden Republik Indonesia Nomor 47 Tahun 2015 tentang Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 89);
2. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 3 Tahun 2016 tentang

Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 59 Tahun 2020 Tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik

Mencabut Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2018 tentang Pedoman Evaluasi Sistem Pemerintahan Berbasis Elektronik

Konsep Kematangan Keamanan Informasi SPBE

PENYUSUNAN KEBIJAKAN

PENERAPAN

AUDIT

Indikator Kematangan Keamanan Informasi SPBE

Tingkat kematangan manajemen keamanan informasi (Information Security Management Maturity Model)

Aspek 1 – Kebijakan Internal Tata Kelola SPBE

Indikator 8

Tingkat Kematangan Kebijakan Internal Manajemen Keamanan Informasi

Aspek 5 – Penerapan Manajemen SPBE

Indikator 22

Tingkat Kematangan Penerapan Manajemen Keamanan Informasi

Aspek 6– Pelaksanaan Audit TIK

Indikator 31

Tingkat Kematangan Pelaksanaan Audit Keamanan SPBE

Tingkat Kematangan Kebijakan Internal Manajemen Keamanan Informasi

Apakah Instansi Pusat/Pemerintah Daerah memiliki kebijakan internal Manajemen Keamanan Informasi?

Tingkat	Kriteria
1	Konsep kebijakan internal terkait Manajemen Keamanan Informasi belum atau telah tersedia.
2	Kebijakan internal terkait Manajemen Keamanan Informasi telah ditetapkan. Kondisi: Kebijakan internal terkait Manajemen Keamanan Informasi belum mengatur secara lengkap mengenai cakupan Manajemen Keamanan Informasi (penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap Keamanan Informasi).
3	Kriteria tingkat 2 telah terpenuhi dan kebijakan internal terkait Manajemen Keamanan Informasi mengatur seluruh cakupan Manajemen Keamanan Informasi secara lengkap (penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap Keamanan Informasi).
4	Kriteria tingkat 3 telah terpenuhi, dan kebijakan internal terkait Manajemen Keamanan Informasi telah mengatur penerapan untuk seluruh unit kerja/perangkat daerah di Instansi Pusat/Pemerintah Daerah. Selain itu, kebijakan internal terkait Manajemen Keamanan Informasi telah direviu dan dievaluasi secara periodik.
5	Kriteria tingkat 4 telah terpenuhi serta hasil reviu dan evaluasi kebijakan internal terkait Manajemen Keamanan Informasi telah ditindaklanjuti dengan kebijakan baru.

Poin Penilaian

Ketersediaan Peraturan mengenai Keamanan Informasi atau Persandian untuk Keamanan Informasi

Dapat berbentuk pengaturan yang sudah ada seperti SMPI/SMKI, Persandian untuk Keamanan Informasi atau pembentukan baru khusus untuk mengatur Keamanan SPBE.

Cakupan pengaturan dari Peraturan mengenai Keamanan Informasi atau Persandian untuk Keamanan Informasi

Yang perlu diatur dalam aturan ini adalah:

- penetapan ruang lingkup pengaturan → apa saja yang diatur, pemberlakuan
- penetapan penanggung jawab → tim dan tupoksi
- perencanaan → penyusunan program, pendokumentasian, manajemen risiko, BCP
- dukungan pengoperasian → penganggaran
- evaluasi kinerja → langkah monitoring
- perbaikan berkelanjutan → dari hasil rekomendasi audit atau monitoring

Poin Penilaian

Cakupan di mana Peraturan mengenai Keamanan Informasi atau Persandian untuk Keamanan Informasi diterapkan

Peraturan tersebut harus berlaku untuk seluruh unit kerja/perangkat daerah di Instansi Pusat/Pemerintah Daerah

Evaluasi dan tindak lanjut

Peraturan tersebut harus dilakukan reviu dan evaluasi secara periodik. Hasil dari reviu dan evaluasi dapat berupa perubahan peraturan atau tidak ada perubahan karena peraturan masih sesuai dengan kondisi saat ini

Tingkat Kematangan Penerapan Manajemen Keamanan Informasi

Apakah Instansi Pusat/Pemerintah Daerah menerapkan Manajemen Keamanan Informasi?

Tingkat	Kriteria
1	Pengendalian Keamanan Informasi belum atau telah tersedia dalam tahap pembangunan.
2	Pengendalian Keamanan Informasi telah tersedia. Kondisi: Pengendalian Keamanan Informasi telah dilaksanakan pada sebagian unit kerja/perangkat daerah di Instansi Pusat/Pemerintah Daerah.
3	Kriteria tingkat 2 telah terpenuhi dan pengendalian Keamanan Informasi telah dilaksanakan pada seluruh unit kerja/perangkat daerah di Instansi Pusat/Pemerintah Daerah dengan berdasarkan Risiko SPBE.
4	Kriteria tingkat 3 telah terpenuhi dan pengendalian Keamanan Informasi dilakukan melalui strategi Keamanan Informasi yang ditetapkan oleh Tim Koordinasi SPBE Instansi Pusat/Pemerintah Daerah. Selain itu, pengendalian Keamanan Informasi telah dilakukan reviu dan evaluasi secara periodik.
5	Kriteria tingkat 4 telah terpenuhi serta hasil reviu dan evaluasi pengendalian Keamanan Informasi ditindaklanjuti melalui perbaikan penerapan proses pengendalian Keamanan Informasi.

Poin Penilaian

Cakupan penerapan Peraturan mengenai Keamanan Informasi atau Persandian untuk Keamanan Informasi

Peraturan tersebut harus diterapkan untuk seluruh unit kerja/perangkat daerah di Instansi Pusat/Pemerintah Daerah

Evaluasi dan tindak lanjut

Penerapan tersebut harus dilakukan reviu dan evaluasi secara periodik. Hasil dari reviu dan evaluasi harus ditindaklanjuti guna adanya perbaikan berkelanjutan dari Keamanan Informasi atau Persandian untuk Keamanan Informasi SPBE

Tingkat Kematangan Pelaksanaan Audit Keamanan SPBE

Apakah Instansi Pusat/Pemerintah Daerah melaksanakan Audit Keamanan SPBE?

Tingkat	Kriteria
1	Kegiatan Audit Keamanan SPBE belum atau telah dilaksanakan. Kondisi: Kegiatan Audit Keamanan dilaksanakan tanpa perencanaan yang berkesinambungan.
2	Kriteria tingkat 1 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan sesuai dengan perencanaan yang berkesinambungan. Kondisi: Kegiatan Audit Keamanan dilaksanakan tanpa pedoman Audit Keamanan.
3	Kriteria tingkat 2 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan sesuai dengan pedoman Audit Keamanan. Kondisi: kegiatan Audit Keamanan dilaksanakan oleh auditor TIK/Sistem Keamanan Informasi internal Instansi Pusat/Pemerintah Daerah.
4	Kriteria tingkat 3 telah terpenuhi dan kegiatan Audit Keamanan dilaksanakan oleh auditor TIK/Sistem Keamanan Informasi eksternal yang memiliki sertifikasi auditor TIK/Sistem Keamanan Informasi.
5	Kriteria tingkat 4 telah terpenuhi dan hasil audit Keamanan SPBE telah ditindaklanjuti melalui perbaikan penerapan Keamanan SPBE.

Poin Penilaian

Perencanaan Audit Keamanan SPBE

Audit dilakukan didahului dengan adanya perencanaan

Pelaksanaan Audit dilakukan sesuai dengan Pedoman Audit

BSSN akan menerapkan Pedoman Audit Keamanan SPBE. Pedoman tersebut harus dijadikan panduan oleh Auditor Keamanan Informasi dalam di Instansi Pusat/Pemerintah Daerah maupun eksternal di Instansi Pusat/Pemerintah Daerah untuk melakukan kegiatan audit

Poin Penilaian

Audit dilaksanakan oleh pihak eksternal

Pelaksaan audit oleh Auditor Keamanan Informasi dalam di Instansi Pusat/Pemerintah Daerah tidak menggugurkan kewajiban untuk melaksanakan audit oleh pihak eksternal

Evaluasi dan tindak lanjut

Pelaksanaan audit harus dilakukan reviu dan evaluasi secara periodik. Hasil dari reviu dan evaluasi ditindaklanjuti guna adanya perbaikan berkelanjutan atas pelaksanaan audit serta penerapan Keamanan Informasi atau Persandian untuk Keamanan Informasi SPBE

BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

Jalan Raya Muchtar 70
Duren Mekar,
Bojong Sari, Depok
16518
Tel: +6221 77973360

bssn_ri

@BSSN_RI

@badansiberdansandinegara

Photo Courtesy of Rini Widyantini

Thank You

TERIMA KASIH