# BERITA NEGARA REPUBLIK INDONESIA

No.1248, 2020 BAPETEN. Keamanan Informasi. Sistem Manajemen


PERATURAN BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA
NOMOR 8 TAHUN 2020
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN BADAN PENGAWAS TENAGA NUKLIR

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA BADAN PENGAWAS TENAGA NUKLIR
REPUBLIK INDONESIA,

Menimbang : a. bahwa dalam rangka melindungi kerahasiaan, integritas, dan ketersediaan aset informasi Badan Pengawas Tenaga Nuklir dari berbagai bentuk ancaman keamanan informasi baik dari dalam maupun luar lingkungan Badan Pengawas Tenaga Nuklir, perlu melakukan pengaturan pengelolaan keamanan informasi di lingkungan Badan Pengawas Tenaga Nuklir;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Badan Pengawas Tenaga Nuklir tentang Sistem Manajemen Keamanan Informasi di Lingkungan Badan Pengawas Tenaga Nuklir;

Mengingat : 1. Undang-Undang Nomor 10 Tahun 1997 tentang Ketenaganukliran (Lembaran Negara Republik Indonesia Tahun 1997 Nomor 23, Tambahan Lembaran Negara

www.peraturan.go.id

Republik Indonesia Nomor 3676);

2. 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);
3. Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Departemen sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Presiden Nomor 145 Tahun 2015 tentang perubahan kedelapan Keputusan Presiden Nomor 103 Tahun 2001 tentang Kedudukan, Tugas, Fungsi, Kewenangan, Susunan Organisasi, dan Tata Kerja Lembaga Pemerintah Non Departemen (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 322);
4. Keputusan Kepala Badan Pengawas Tenaga Nuklir Nomor 01.Rev.2/K.OTK/V-04 sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Badan Pengawas Tenaga Nuklir Nomor 1 Tahun 2019 tentang Perubahan Kedua atas Keputusan Kepala Badan Pengawas Tenaga Nuklir Nomor 01 Rev.2/K-Otk/V-04 Tahun 2004 tentang Organisasi dan Tata Kerja Badan Pengawas Tenaga Nuklir (Berita Negara Republik Indonesia Tahun 2019 Nomor 27);

MEMUTUSKAN:

Menetapkan : PERATURAN BADAN PENGAWAS TENAGA NUKLIR TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN BADAN PENGAWAS TENAGA NUKLIR.

www.peraturan.go.id

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Badan ini yang dimaksud dengan:

1. Aset Informasi adalah aset dalam bentuk data atau dokumen, perangkat lunak, aset fisik, dan aset tak berwujud.
2. Badan adalah Badan Pengawas Tenaga Nuklir.
3. *Chief Information Officer* yang selanjutnya disingkat CIO adalah pejabat pengarah informasi yang dijabat oleh Sekretaris Utama sebagai koordinator penyelenggaraan tata kelola Teknologi Informasi dan Komunikasi di lingkungan Badan.
4. *Chief Information Security Officer* yang selanjutnya disingkat CISO adalah pejabat yang berperan sebagai koordinator dalam pelaksanaan implementasi kebijakan dan standar SMKI di Lingkungan Badan.
5. Keamanan Informasi adalah terjaganya kerahasiaan, keutuhan, dan ketersediaan informasi.
6. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah teknologi untuk mengumpulkan, menyiapkan, menyimpan, mengolah, mengumumkan, menganalisis, mengambil kembali, mengirim atau menerima data dan informasi.
7. Komite TIK adalah komite yang terdiri dari Deputi Perizinan dan Inspeksi, Deputi Pengkajian Keselamatan Nuklir, Manajemen Unit Pengelola TIK, dan Ahli TIK yang dibentuk dengan tujuan untuk memberikan dukungan teknis TIK dalam mendukung pelaksanaan tugas CIO.
8. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen yang meliputi organisasi, perencanaan, penanggung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.

www.peraturan.go.id

9. Tim Keamanan Informasi adalah tim yang dibentuk dalam rangka perlindungan terhadap keamanan informasi Badan.
10. Unit Pemilik Proses Bisnis adalah unit kerja yang memiliki aplikasi sistem informasi dan/atau memiliki alat monitoring pengawasan ketenaganukliran.
11. Unit Pengelola TIK adalah unit kerja yang melakukan pengelolaan teknologi informasi dan komunikasi berupa mengumpulkan, menyiapkan, menyimpan, mengolah, mengumumkan, menganalisis, mengambil kembali, mengirim atau menerima data dan informasi.

Pasal 2

Peraturan Badan ini mengatur kebijakan dan standar SMKI yang digunakan sebagai pedoman dalam melindungi keamanan aset informasi milik Badan.

BAB II

PELAKSANA KEAMANAN INFORMASI

Pasal 3

Kebijakan dan standar SMKI sebagaimana dimaksud dalam Pasal 2 dikoordinasikan oleh Sekretaris Utama selaku CIO dan sekaligus CISO.

Pasal 4

(1) Dalam melaksanakan tugasnya, CISO sebagaimana dimaksud dalam Pasal 3 menetapkan Tim Keamanan Informasi.
(2) Tim Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. CISO;
    b. Unit Pengelola TIK; dan
    c. Unit Pemilik Proses Bisnis

www.peraturan.go.id

Pasal 5

CISO sebagaimana dimaksud dalam Pasal 4 bertanggung jawab untuk:

a. mengkoordinasikan perumusan dan penyempurnaan kebijakan dan standar SMKI di Lingkungan Badan;
b. memelihara dan mengendalikan penerapan kebijakan dan standar SMKI di seluruh area di Lingkungan Badan yang menjadi tujuan sasaran pengendalian;
c. menetapkan target keamanan informasi setiap tahunnya serta menyusun rencana kerja;
d. memastikan efektivitas dan konsistensi penerapan kebijakan dan standar SMKI di Lingkungan Badan serta mengukur kinerja keseluruhan; dan
e. melaporkan kinerja penerapan kebijakan dan standar SMKI di Lingkungan Badan serta pencapaian target kepada Komite TIK.
f. menunjuk pihak yang berkompeten untuk melakukan audit terhadap penerapan kebijakan dan standar SMKI di Lingkungan Badan.

Pasal 6

Unit Pengelola TIK sebagaimana dimaksud dalam Pasal 4 bertanggung jawab untuk:

a. memastikan kebijakan dan standar SMKI di Lingkungan Badan diterapkan secara efektif;
b. memastikan langkah-langkah perbaikan sudah dilakukan berdasarkan saran dan rekomendasi yang diberikan dalam pelaksanaan evaluasi dan/atau audit penerapan kebijakan dan standar SMKI di Lingkungan Badan;
c. memastikan peningkatan kesadaran, kepedulian, dan kepatuhan seluruh pegawai terhadap kebijakan dan standar SMKI di Lingkungan Badan;
d. melaporkan kinerja penerapan kebijakan dan standar SMKI di Lingkungan Badan sesuai ruang lingkup tanggung jawabnya kepada CISO yang akan digunakan sebagai dasar peningkatan keamanan informasi;

www.peraturan.go.id