



BADAN SIBER DAN SANDI NEGARA
DEPUTI BIDANG KEAMANAN SIBER DAN SANDI PEREKONOMIAN
Jalan Raya Muchtar No.70, Kel. Bojongsari Lama, Kec. Bojongsari, Depok 16518
Telepon (021) 77973360, Faksimile (021) 78844104, 77973579
Website: <https://bssn.go.id>, E-mail: humas@bssn.go.id

Yth. Pimpinan Perusahaan Sektor Industri.

SURAT EDARAN

NOMOR 79 TAHUN 2025

TENTANG

PEDOMAN PENERAPAN KEAMANAN SIBER PADA SEKTOR INDUSTRI
UNTUK MENDUKUNG TRANSFORMASI DIGITAL INDUSTRI DI INDONESIA

A. Umum

Seiring dengan pesatnya laju transformasi digital di sektor industri nasional, pemanfaatan teknologi informasi dan teknologi operasional menjadi krusial untuk meningkatkan efisiensi, produktivitas, dan daya saing. Peningkatan konektivitas dan ketergantungan pada sistem elektronik, seperti *Industrial Control Systems* (ICS) yang mulai terhubung dengan jaringan teknologi informasi, turut membuka celah terhadap berbagai bentuk ancaman dan insiden siber. Ancaman ini berpotensi mengganggu proses bisnis, menyebabkan kerugian finansial, hingga membahayakan kepentingan nasional.

Menyikapi tantangan tersebut, Pemerintah melalui Badan Siber dan Sandi Negara (BSSN) telah menetapkan serangkaian kerangka kerja dan peraturan sebagai landasan dalam penyelenggaraan keamanan siber nasional. Kerangka kerja ini mencakup kewajiban penerapan Sistem Manajemen Pengamanan Informasi (SMPI), implementasi kerangka kerja perlindungan siber yang sistematis, serta pengukuran tingkat kematangan keamanan siber secara berkala.

Di sisi lain, dalam rangka mendorong agenda nasional Making Indonesia 4.0, Kementerian Perindustrian telah menggunakan instrumen *Indonesia Industry 4.0 Readiness Index* (INDI 4.0) untuk mengukur tingkat kesiapan industri dalam bertransformasi menuju Industri 4.0. Asesmen INDI 4.0 yang mencakup pilar-pilar strategis seperti manajemen, sumber daya manusia, dan teknologi, akan memiliki nilai dan kredibilitas yang lebih tinggi apabila ditopang oleh fondasi keamanan siber yang kokoh. Penerapan keamanan siber yang andal tidak hanya berfungsi sebagai mekanisme pertahanan, tetapi juga sebagai akselerator yang memastikan bahwa setiap investasi pada teknologi Industri 4.0 terlindungi dan dapat beroperasi secara berkelanjutan. Dengan demikian, penerapan keamanan siber secara langsung meningkatkan nilai dan ketahanan capaian skor INDI 4.0 suatu perusahaan.

Oleh karena itu, untuk menyelaraskan upaya perlindungan ruang siber dengan agenda transformasi digital industri, serta untuk memastikan bahwa peningkatan konektivitas diiringi dengan peningkatan ketahanan, dipandang perlu untuk menerbitkan Surat Edaran. Pedoman ini bertujuan untuk memberikan panduan teknis dan strategis yang terstruktur dan komprehensif bagi seluruh pelaku industri di Indonesia dalam mengimplementasikan keamanan siber secara efektif dan efisien.

B. Maksud dan Tujuan

1. Maksud

Pedoman ini dimaksudkan untuk menjadi acuan standar bagi para pelaku industri di Indonesia dalam merencanakan, menerapkan, mengukur, dan meningkatkan postur keamanan siber organisasinya.

2. Tujuan

Tujuan dari ditetapkannya pedoman ini adalah untuk :

- a. Menyediakan kerangka kerja implementasi keamanan siber yang selaras dengan peraturan perundang-undangan.

- b. Meningkatkan postur keamanan dan ketahanan siber pada setiap entitas di sektor industri.
- c. Mendukung terwujudnya ekosistem transformasi digital industri yang aman, andal, dan terpercaya.

C. Ruang Lingkup

Ruang lingkup Surat Edaran ini meliputi :

1. Kategorisasi sistem elektronik;
2. Penerapan kerangka kerja perlindungan sistem elektronik; dan
3. Pengukuran tingkat kematangan keamanan siber.

D. Dasar

Pedoman ini disusun dengan merujuk pada kerangka peraturan yang telah ditetapkan oleh Badan Siber dan Sandi Negara (BSSN), meliputi:

1. Peraturan BSSN Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik;
2. Peraturan BSSN Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Badan Siber dan Sandi Negara.

E. Pengertian

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 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. Kerangka Kerja Pelindungan Sistem Elektronik adalah seperangkat konsep dasar yang digunakan sebagai pedoman dalam menyusun, menerapkan, dan mengomunikasikan, aktivitas pengelolaan keamanan siber pada Sistem Elektronik.

4. Peristiwa Siber adalah adalah kejadian pada sistem elektronik yang dapat diobservasi dan dapat memberikan indikasi terhadap terjadinya Insiden Siber.
5. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya sistem elektronik.

F. Pelaksanaan Kegiatan

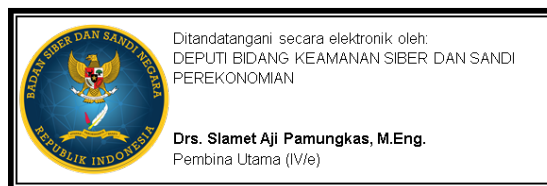
Pelaksanaan kegiatan penerapan keamanan siber bagi sektor industri mengacu pada tahapan sistematis yang diatur lebih lanjut dalam Lampiran yang merupakan bagian tidak terpisahkan dari pedoman ini.

G. Penutup

Demikian pedoman ini ditetapkan untuk dapat diterapkan oleh seluruh pemangku kepentingan di sektor industri. Keberhasilan implementasi pedoman ini, yang mencakup aspek teknis, prosedural, dan sumber daya manusia, merupakan faktor krusial dalam menjaga keamanan ruang siber nasional dan mengakselerasi program transformasi digital industri Indonesia.

Ditetapkan di Depok

Pada tanggal 4 September 2025



Tembusan :

1. Direktur Jenderal Industri Kecil, Menengah, dan Aneka, Kementerian Perindustrian;
2. Direktur Jenderal Industri Logam, Mesin, Alat Transportasi, dan Elektronika, Kementerian Perindustrian;

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Besar Sertifikat Elektronik (BSrE), Badan Siber dan Sandi Negara

3. Direktur Jenderal Industri Agro, Kementerian Perindustrian;
4. Direktur Jenderal Industri Kimia, Farmasi, dan Tekstil, Kementerian Perindustrian;
5. Direktur Jenderal Ketahanan, Perwilayahan dan Akses Industri Internasional, Kementerian Perindustrian;
6. Kepala Badan Standardisasi dan Kebijakan Jasa Industri, Kementerian Perindustrian.

LAMPIRAN SURAT EDARAN
NOMOR 79 TAHUN 2025
TENTANG PEDOMAN PENERAPAN KEAMANAN SIBER
PADA SEKTOR INDUSTRI UNTUK MENDUKUNG
TRANSFORMASI DIGITAL INDUSTRI DI INDONESIA

I. TAHAP I : KATEGORISASI SISTEM ELEKTRONIK

Langkah awal yang perlu dilaksanakan oleh setiap Penyelenggara Sistem Elektronik (PSE) adalah melakukan inventarisasi dan kategorisasi terhadap sistem elektronik yang dimiliki dan/atau dioperasikan.

1. Inventarisasi Sistem Elektronik

Penyelenggara Sistem Elektronik melakukan pendataan terhadap aset sistem elektronik yang dimiliki. Sistem elektronik diinventarisasi ke dalam formulir inventarisasi dengan ketentuan sebagai berikut:

- a. kolom (1) berisi nomor urut
- b. kolom (2) berisi nama sistem elektronik
- c. kolom (3) berisi deskripsi sistem elektronik terkait definisi, fungsi, tujuan, dan data yang dikelola dari layanan sistem elektronik
- d. kolom (4) berisi metode akses terhadap sistem elektronik dengan pilihan isian Publik atau Privat
- e. kolom (5) berisi lokasi penyimpanan sistem elektronik dengan pengisian *co-location* atau *on-premise*
- f. kolom (6) berisi unit pengelola yang bertanggung jawab terhadap sistem elektronik

Contoh pengisian formulir inventarisasi sistem elektronik sebagai berikut :

Tabel 1.1 Format dan Contoh Pengisian Inventarisasi Sistem Elektronik

<i>Formulir Inventarisasi Sistem Elektronik</i>					
NO	NAMA SISTEM ELEKTRONIK	DESKRIPSI SINGKAT	METODE AKSES	LOKASI	UNIT PENGELOLA
(1)	(2)	(3)	(4)	(5)	(6)
1.	Sistem ERP	Sistem elektronik terintegrasi yang digunakan untuk mengelola dan mengotomatisasi berbagai proses bisnis utama dalam organisasi. ERP menghubungkan berbagai fungsi seperti keuangan, sumber daya manusia, produksi, logistik, pemasaran, dan layanan pelanggan ke dalam satu platform, sehingga memungkinkan pertukaran data secara real-time dan meningkatkan efisiensi operasional. Adapun data yang dikelola yaitu data keuangan & akuntansi, SDM, Produksi & Operasional, data logistik dan supply chain	Privat	On-premise	Divisi TI
dst		...	...	...	

2. Kategori Sistem Elektronik

Kategorisasi Sistem Elektronik dilakukan terhadap seluruh sistem elektronik yang sudah terinventarisasi pada tahap sebelumnya. Kategorisasi sistem elektronik ini dilakukan berdasarkan asas risiko ke dalam 3 (tiga) kategori, yaitu:

- a. Strategis : Sistem elektronik yang gangguannya berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.

- b. Tinggi : Sistem elektronik yang dampaknya terbatas pada kepentingan sektor dan/atau daerah tertentu.
- c. Rendah : Sistem elektronik lainnya yang tidak termasuk dalam kategori strategis dan tinggi.

3. Pelaksanaan Kategorisasi Sistem Elektronik

Kategorisasi Sistem Elektronik ditentukan berdasarkan Penilaian Mandiri oleh Penyelenggara Sistem Elektronik terhadap Sistem Elektronik yang dimilikinya. Format Penilaian Mandiri Sistem Elektronik sebagai berikut:

FORMAT PENILAIAN MANDIRI KATEGORISASI SISTEM ELEKTRONIK				
Kategorisasi Sistem Elektronik				
Nama Perusahaan :				
Jenis Usaha :				
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis	Status	Bobot Nilai	Data Dukung	
No	Karakteristik Instansi			
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar			
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar			
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus			
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi			

1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna			
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi			
1.7	Tingkat klasifikasi/kekritisian Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa			
1.8	Tingkat kekritisian proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan			
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih			
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan merugikan finansial)			
Total Bobot Nilai				
Kategorisasi Sistem Elektronik				

Keterangan:

Status	Bobot Nilai
A	5
B	2
C	1

Ketentuan Penilaian:

Kategori Sistem Elektronik	Strategis	Tinggi	Rendah
Total Bobot Nilai	36 - 50	16 - 35	10 - 15

Saya yang bertanda tangan di bawah ini menyatakan bahwa data di atas diisi sesuai dengan keadaan sebenarnya.

(Tempat, tanggal bulan tahun)

PIMPINAN UNIT KERJA TI

(Nama)

(Jabatan)

Cara Pengisian :

- Isi identitas pada kolom “Nama Perusahaan” dan “Jenis Perusahaan”.
 - Isi formulir penilaian dengan mengisi kolom “Status”, “Bobot Nilai”, dan “Data Dukung”.
 - Kolom “Status” diisi berdasarkan pilihan A, B, atau C sesuai dengan karakteristik pada instansi anda.
 - Kolom “Bobot Nilai” diisi berdasarkan konversi dari nilai pada kolom “Status”. Nilai konversi sesuai dengan ketentuan pada Tabel Keterangan.
 - Kolom “Data Dukung” diisi dengan nama/judul dari dokumen yang dilampirkan sebagai bukti bahwa benar keadaan perusahaan sesuai dengan status yang di pilih.
 - Kolom “Total Nilai” diisi dengan menjumlahkan skor yang diperoleh dari setiap pertanyaan.
 - Kolom “Kategorisasi Elektronik” diisi berdasarkan ketentuan penilaian pada Tabel Ketentuan Penilaian.
 - Form yang sudah diisi sesuai ketentuan petunjuk pengisian kemudian di tanda tangani oleh Pimpinan Unit Kerja Teknologi Informasi.
4. Penyelenggara Sistem Elektronik perlu menerapkan Kerangka Kerja Pelindungan Sistem Elektronik sesuai dengan penjelasan pada Tahap II Lampiran Surat Edaran ini.

5. Formulir Inventarisasi Sistem Elektronik dan Formulir Kategorisasi Sistem Elektronik dapat diunduh pada *website* BSSN, menu Publikasi.

II. TAHAP II : PENERAPAN KERANGKA KERJA PELINDUNGAN SISTEM ELEKTRONIK

Setelah Kategorisasi Sistem Elektronik ditetapkan, Penyelenggara Sistem Elektronik, perlu menerapkan kontrol keamanan berdasarkan Kerangka Kerja Pelindungan Sistem Elektronik yang mencakup 4 (empat) domain utama.

1. Domain Kerangka Kerja

Kerangka Kerja Pelindungan mencakup 4 (empat) domain utama sebagai berikut :

a. Domain Identifikasi (*Identify*)

Fungsi ini bertujuan mendukung kemampuan organisasi dalam memahami konteks bisnis, sumber daya, dan risiko siber. Aktivitas utamanya meliputi:

- 1) Mengidentifikasi peran serta tanggung jawab organisasi.
- 2) Mengelola aset informasi.
- 3) Menilai dan mengelola risiko keamanan siber.
- 4) Mengelola risiko dari rantai pasok (pihak ketiga).

b. Domain Proteksi (*Protect*)

Fungsi ini bertujuan untuk mencegah, membatasi, atau menahan dampak dari Insiden Siber. Aktivitas utamanya meliputi:

- 1) Mengelola identitas, autentikasi, dan kendali akses.
- 2) Melindungi aset fisik dan data.
- 3) Melindungi aplikasi dan jaringan komunikasi.
- 4) Melindungi sumber daya manusia melalui program pelatihan dan kesadaran keamanan.

c. Domain Deteksi (*Detect*)

Fungsi ini bertujuan untuk mengembangkan kemampuan dalam memantau dan mendeteksi terjadinya Peristiwa Siber secara tepat waktu. Aktivitas utamanya meliputi:

- 1) Mengelola deteksi Peristiwa Siber.
- 2) Menganalisis anomali dan Peristiwa Siber yang terdeteksi.
- 3) Melaksanakan pemantauan keamanan secara berkelanjutan.

d. Domain Penanggulangan dan Pemulihan (*Respond & Recover*)

Fungsi ini bertujuan untuk memastikan organisasi mampu mengambil tindakan yang diperlukan saat Insiden Siber terjadi guna meminimalisir dampak dan memulihkan layanan. Aktivitas utamanya meliputi:

- 1) Menyusun dan menguji rencana penanggulangan insiden dan pemulihan layanan.
- 2) Menganalisis dan melaporkan Insiden Siber kepada pihak terkait.
- 3) Melaksanakan tindakan mitigasi, eradikasi, dan pemulihan sistem.

Meningkatkan postur keamanan berdasarkan hasil investigasi insiden.

2. Penerapan Kerangka Kerja

Penyelenggara sistem elektronik perlu menyelenggarakan perlindungan sistem elektronik untuk mengendalikan keamanan siber melalui penerapan kontrol keamanan sesuai dengan domain kerangka kerja sebagai berikut :

Tabel 1.2 Matriks Kerangka Kerja Pelindungan Sistem Elektronik

Domain		Kategori		Sub-Kategori		Kontrol		Ruang Lingkup
1.	Identifikasi	1.1	Mengidentifikasi peran dan tanggung jawab organisasi	1.1.1	Menetapkan dan mengomunikasikan prioritas untuk misi, tujuan, dan kegiatan pelindungan Sistem Elektronik di organisasi	a	Pimpinan organisasi menetapkan keamanan siber sebagai prioritas di organisasi dalam bentuk kebijakan atau komitmen pimpinan yang sesuai dengan kondisi bisnis/layanan dan operasional organisasi.	Tata Kelola
						b	Penyelenggara Sistem Elektronik mengomunikasikan perihal komitmen keamanan siber di organisasinya dengan pihak-pihak yang terkait dengan bisnis/layanan organisasi (termasuk kepada penyedia pihak ketiga).	Tata Kelola
				1.1.2	Mengidentifikasi ketergantungan organisasi dengan pihak terkait lainnya	a	Penyelenggara Sistem Elektronik mengidentifikasi unit kerja di internal organisasinya, maupun pihak lain di luar organisasinya yang memiliki ketergantungan, baik secara langsung maupun tidak langsung terhadap operasional layanan Sistem Elektronik di organisasinya.	Tata Kelola
				1.1.3	Mengidentifikasi dan mengomunikasikan peran organisasi di dalam sektor	a	Penyelenggara Sistem Elektronik mengidentifikasi dan menetapkan unit kerja atau fungsi yang memiliki tugas dan tanggung jawab dalam menerapkan pelindungan Sistem Elektronik di organisasinya.	Tata Kelola
						b	Penyelenggara Sistem Elektronik mengidentifikasi peran, aktivitas, proses, dan	Tata Kelola

							narahubung dari pemangku kepentingan yang mendukung ekosistem bisnis atau layanan Sistem Elektronik, baik di dalam atau di luar organisasi.	
		1.2	Menyusun strategi, kebijakan, dan prosedur Pelindungan Sistem Elektronik	1.2.1	Menetapkan dan mengomunikasikan kebijakan keamanan siber di lingkungan Penyelenggara Sistem Elektronik	a	Penyelenggara Sistem Elektronik menyusun, menetapkan, dan mengembangkan kebijakan tentang keamanan siber sesuai dengan standar yang berlaku di sektornya dan/atau peraturan perundang-undangan	Tata Kelola
						b	Penyelenggara Sistem Elektronik mengomunikasikan kebijakan kepada seluruh personel yang relevan, serta mengoordinasikan dan menyepakati metode berbagi informasi mengenai kebijakan dan prosedur yang ada di organisasi dengan para pemangku kepentingan eksternal.	Tata Kelola
						c	Penyelenggara Sistem Elektronik meninjau dan merevisi kebijakannya secara berkelanjutan sesuai dengan setiap perubahan dalam peraturan perundang-undangan yang relevan, standar dan/atau pedoman industri yang berlaku di sektornya.	Tata Kelola
				1.2.2	Mengembangkan strategi untuk meningkatkan pelindungan terhadap Sistem Elektronik	a	Penyelenggara Sistem Elektronik senantiasa mengembangkan strategi dalam melindungi aset informasi dengan mempertimbangkan manajemen risiko yang berlaku di organisasi.	Tata Kelola

						b	Penyelenggara Sistem Elektronik harus menetapkan sasaran atau target penerapan keamanan siber pada fungsi dan tingkatan yang relevan.	Tata Kelola
				1.2.3	Menetapkan persyaratan yang dibutuhkan untuk mendukung operasional Sistem Elektronik pada semua keadaan	a	Penyelenggara Sistem Elektronik menyusun kebijakan standar operasional prosedur terhadap setiap layanan yang mendukung Sistem Elektronik baik dalam kondisi normal, jika terjadi insiden siber, dan pasca insiden siber.	Tata Kelola
				1.2.4	Menetapkan kebijakan penggunaan aset informasi bagi pegawai dan pihak ketiga	a	Penyelenggara Sistem Elektronik menyusun kebijakan yang diperlukan untuk menjaga ketersediaan aset informasi, seperti kebijakan penggunaan perangkat pribadi di kantor (<i>bring your own devices</i>), kebijakan instalasi perangkat lunak pada perangkat kantor, kebijakan klasifikasi informasi, dsb.	Tata Kelola
		1.3	Mengelola aset informasi	1.3.1	Mengelola daftar inventaris aset informasi	a	Dokumentasikan dan kelola dengan tepat daftar inventaris aset informasi seperti perangkat keras, perangkat lunak, data, dan layanan TIK yang akan dilindungi, beserta informasi manajemennya (misalnya nama aset, versi, alamat jaringan, nama penanggungjawab, informasi lisensi, dsb).	Tata Kelola & Teknologi
						b	Penyelenggara Sistem Elektronik memastikan pemberian label pada perangkat aset informasi oleh pihak yang berwenang di organisasi.	Tata Kelola

				1.3.2	Memetakan jalur komunikasi dan alur data pada organisasi	a	Penyelenggara Sistem Elektronik menyusun dokumentasi dan mengelola diagram jalur komunikasi jaringan dan aliran data dengan tepat dalam organisasi.	Teknologi		
				1.3.3	Menyusun katalog sistem informasi eksternal yang menggunakan data milik organisasi	a	Dokumentasikan dan kelola dengan tepat daftar sistem informasi eksternal yang menggunakan data atau layanan Sistem Elektronik.	Tata Kelola		
						b	Dokumentasikan dan kelola dengan tepat daftar sistem informasi eksternal yang digunakan oleh Penyelenggara Sistem Elektronik.	Tata Kelola		
				1.3.4	Menyusun prioritas aset informasi berdasarkan klasifikasi, kekritisannya, dan nilai bisnisnya	a	Mengklasifikasikan dan memprioritaskan aset informasi seperti, perangkat keras, perangkat lunak, data, dan layanan TIK lainnya berdasarkan fungsi, kekritisannya, dan nilai bisnis.	Tata Kelola		
				1.3.5	Mengendalikan aset informasi milik organisasi	a	Menentukan metode untuk memastikan ketertelusuran aset informasi seperti membuat catatan mengenai tanggal produksi atau pengadaan aset, kondisi aset, catatan pemakaian, dan pelaporan kepada unit kerja terkait.	Tata Kelola & Teknologi		
						b	Secara aktif memeriksa keterbaharuan dan memperbaharui dari setiap versi perangkat lunak dan perangkat keras yang digunakan oleh organisasi.	Teknologi		
				1.4	Menilai dan mengelola risiko Keamanan Siber	1.4.1	Mengidentifikasi dan mendokumentasikan	a	Identifikasi kerentanan terhadap seluruh aset informasi di organisasi, misalnya melalui <i>penetration testing</i> dan <i>vulnerability assessment</i> , serta dokumentasikan daftar kerentanan yang	Teknologi

				kerentanan terhadap aset informasi.		teridentifikasi tersebut bersama dengan daftar aset terkait.	
			1.4.2	Mengidentifikasi dan mendokumentasikan informasi terkait ancaman dan kerentanan yang diperoleh dari internal maupun eksternal	a	Penyelenggara Sistem Elektronik mengumpulkan informasi termasuk kerentanan dan ancaman dari sumber internal dan eksternal (melalui pengujian internal, informasi dari pihak berwajib, hasil penelitian keamanan, dll.)	Teknologi & Tata Kelola
					b	Menganalisis informasi tersebut apakah termasuk kedalam konteks risiko terhadap aset informasi, dan mendokumentasikannya.	Tata Kelola
			1.4.3	Mengidentifikasi potensi dampak terhadap layanan Sistem Elektronik dan kemungkinan terjadinya dampak tersebut	a	Penyelenggara Sistem Elektronik perlu memeriksa pada setiap fungsi penting organisasi apakah ada risiko keamanan yang diketahui termasuk kedalam kategori membahayakan keselamatan, menimbulkan kerugian, dan mengancam keamanan negara.	Tata Kelola
			1.4.4	Menganalisis nilai risiko terhadap Sistem Elektronik	a	Pertimbangkan ancaman, kerentanan, kemungkinan, dan dampak saat menganalisis risiko.	Tata Kelola
					b	Penyelenggara Sistem Elektronik menentukan level risiko dan prioritas mitigasinya.	Tata Kelola
			1.4.5		a	Berdasarkan hasil penilaian risiko, tentukan dengan jelas rincian tindakan untuk mencegah kemungkinan risiko keamanan, dan	Tata Kelola

					Mengidentifikasi dan menyusun prioritas mitigasi terhadap risiko		dokumentasikan hasil yang terorganisir dari ruang lingkup dan prioritas tindakan.	
						b	Evaluasi hasil penerapan respon risiko secara berkelanjutan.	Tata Kelola
				1.4.6	Menentukan dan mengomunikasikan toleransi risiko organisasi	a	Menentukan tingkat toleransi risiko organisasi berdasarkan hasil penilaian risiko dan kebijakan yang berlaku.	Tata Kelola
				1.4.7	Mengelola hasil penerapan manajemen risiko yang telah ditetapkan	a	Konfirmasi status implementasi manajemen risiko keamanan siber organisasi dan komunikasikan hasilnya kepada pihak yang tepat di dalam organisasi (misalnya pimpinan organisasi).	Tata Kelola
						b	Tetapkan serta terapkan proses untuk mengonfirmasi status penerapan manajemen risiko keamanan pihak terkait.	Tata Kelola
				1.4.8	Melakukan reviu terhadap hasil penerapan manajemen risiko	a	Penyelenggara Sistem Elektronik melakukan reviu terhadap manajemen risiko secara periodik, atau apabila menemukan data atau informasi baru yang berpotensi menambah atau mengubah profil risiko.	Tata Kelola
		1.5	Mengelola risiko rantai pasok	1.5.1	Mengidentifikasi dan menetapkan proses manajemen risiko rantai pasok	a	Merumuskan standar tindakan keamanan yang relevan dengan rantai pasokan dan menyepakati konten dengan mitra bisnis setelah memperjelas ruang lingkup tanggung jawab masing-masing.	Tata Kelola
						b	Hal yang perlu dipertimbangkan dalam proses manajemen risiko rantai pasokan diantaranya	Tata Kelola

							adalah penentuan jenis akses yang diberikan, alasan kebutuhan akses, metode akses, jangka waktu, dan potensi risiko yang terjadi apabila akses tersebut disalahgunakan.	
				1.5.2	Mengidentifikasi pemasok dan mitra pihak ketiga dari setiap aset informasi di Sistem Elektronik	a	Identifikasi peran dan tanggung jawab keamanan siber di pemangku kepentingan pihak ketiga (misalnya, pemasok, pelanggan, atau mitra), dan pihak lainnya yang berhubungan dengan Penyelenggara Sistem Elektronik.	Tata Kelola
						b	Merumuskan dan mengelola persyaratan keamanan yang berlaku untuk anggota/personel pihak ketiga, dan juga pemangku kepentingan lainnya yang terlibat dalam layanan yang disediakan oleh pihak ketiga.	Tata Kelola
				1.5.3	Memastikan poin-poin perjanjian kerja sama yang digunakan untuk pemasok dan mitra pihak ketiga telah sesuai dengan kebijakan	a	Saat menandatangani kontrak dengan pihak ketiga, periksa apakah manajemen pihak ketiga telah dengan benar mematuhi persyaratan keamanan, standar, dan peraturan perundangan yang berlaku, dengan	Tata Kelola
					keamanan siber pada Penyelenggara Sistem Elektronik		keamanan, standar, dan peraturan perundangan yang berlaku, dengan mempertimbangkan tujuan kontrak tersebut dan hasil manajemen risiko.	
						b	Saat menandatangani kontrak dengan pihak ketiga, periksa apakah produk dan layanan yang	Tata Kelola

						disediakan oleh pihak ketiga sesuai dengan persyaratan keamanan yang ada di organisasi.		
				1.5.4	Melakukan pemeriksaan secara periodik terhadap pemasok dan mitra pihak ketiga terkait pemenuhan kewajiban kerja sama dan keamanannya	a	Melakukan penilaian secara berkala melalui audit, hasil pengujian, atau pemeriksaan dari pihak terkait untuk memastikan pihak ketiga memenuhi kewajiban kontraktual mereka.	Tata Kelola
						b	Merumuskan dan menerapkan prosedur untuk mengatasi ketidakpatuhan terhadap persyaratan kontrak yang ditemukan.	Tata Kelola
						c	Mengumpulkan dan menyimpan data dengan aman yang membuktikan bahwa organisasi memenuhi kewajiban kontraktualnya dengan pihak atau individu lain yang relevan, dan mempersiapkannya untuk pengungkapan jika diperlukan dalam rangka penegakan hukum.	Tata Kelola
				1.5.5	Menyiapkan rencana penanggulangan dan pemulihan pada layanan Sistem Elektronik dengan	a	Menyiapkan dan menguji prosedur respons insiden dengan pihak terkait yang terlibat dalam aktivitas respons insiden untuk memastikan tindakan respons dilaksanakan dalam rantai pasokan.	Tata Kelola
					pihak ketiga yang mendukung layanan tersebut	b	Menyusun prosedur keamanan yang akan dijalankan ketika kontrak dengan pihak ketiga selesai. (misalnya, pemutusan hak akses ketika berakhirnya masa kontrak).	Tata Kelola
c	Senantiasa meningkatkan standar langkah-langkah keamanan yang relevan dengan mitra rantai pasok.	Tata Kelola						

2.	Proteksi	2.1	Mengelola identitas, autentikasi, dan kendali akses	2.1.1	Mengelola identitas dan kredensial yang menggunakan layanan Sistem Elektronik	a	Menetapkan dan menerapkan prosedur untuk menerbitkan, mengelola, memeriksa, membatalkan, dan memantau informasi tentang identitas dan kredensial terhadap aset informasi dan personel yang menggunakan Sistem Elektronik.	Tata Kelola & Teknologi
				2.1.2	Mengelola akses jarak jauh terhadap layanan Sistem Elektronik	a	Penyelenggara Sistem Elektronik menyusun prosedur tentang mekanisme identifikasi pengguna layanan, pemberian akses, dan otorisasi terhadap layanan, termasuk pemberian koneksi terhadap pengguna, perangkat IoT, dan/atau <i>server</i> .	Tata Kelola & Teknologi
						b	Tersedianya dan diterapkannya prosedur pencegahan terhadap upaya memasuki perangkat atau jaringan secara tidak sah, dengan menerapkan langkah-langkah seperti menerapkan fungsi untuk penguncian setelah sejumlah upaya masuk yang gagal dan memberikan interval waktu hingga keamanannya dipastikan.	Teknologi
				2.1.3	Mengelola izin akses dan otorisasi layanan Sistem Elektronik	a	Menyusun dan menerapkan prosedur untuk memisahkan hak akses sesuai tugas dan area tanggung jawab (misalnya, pisahkan fungsi untuk pengguna dari fungsi untuk administrator sistem)	Tata Kelola & teknologi

						b	Tersedianya prosedur pembatasan komunikasi oleh perangkat dan server kepada pengguna sesuai dengan tingkat risikonya.	Teknologi
				2.1.4	Memastikan penerapan sistem autentikasi terhadap pengguna, perangkat, dan aset informasi sesuai tingkat risikonya	a	Perangkat, pengguna, dan aset informasi lainnya menggunakan sistem otentikasi tertentu (misalnya, multi-factor authentication) sesuai dengan tingkat risiko nya terhadap sistem.	Tata Kelola & Teknologi
		2.2	Melindungi aset fisik	2.2.1	Menyediakan prosedur operasional perlindungan terhadap aset fisik yang mendukung layanan Sistem Elektronik	a	Menetapkan dan menerapkan prosedur keamanan fisik terhadap akses kontrol yang sesuai seperti mengunci dan membatasi akses ke area tempat perangkat dan <i>server</i> dipasang, menggunakan kontrol masuk dan keluar, otentikasi biometrik, memasang kamera pengintai, dan/atau memeriksa barang bawaan.	Tata Kelola & teknologi
						b	Tersedianya dan diterapkannya prosedur perlindungan fisik seperti menyiapkan catu daya cadangan, fasilitas proteksi kebakaran, dan perlindungan dari resapan air yang mengikuti kebijakan dan standar yang berlaku.	Tata Kelola
						c	Tersedianya prosedur dan sarana pengamanan terhadap perangkat komputer yang digunakan untuk pengolahan data Sistem Elektronik.	Tata Kelola & Teknologi
				2.2.2	Memastikan proses perbaikan dan pemeliharaan aset	a	Tentukan metode untuk melakukan pembaruan keamanan dan sejenisnya pada perangkat dan server. Kemudian, terapkan pembaruan	Tata Kelola & Teknologi

					informasi pada layanan Sistem Elektronik dilakukan, dicatat, dan dikendalikan sesuai prosedur		keamanan tersebut dengan teknologi yang benar dan tepat pada waktunya.	
						b	Dokumentasikan kegiatan pembaruan keamanan pada perangkat organisasi dan laporkan kepada manajemen secara berkala.	Tata Kelola
				2.2.3	Memastikan proses pemeliharaan jarak jauh terhadap aset informasi pada layanan Sistem Elektronik dilakukan dengan persetujuan penanggung jawab layanan Sistem Elektronik dan Didokumentasikan sesuai prosedur	a	Mengidentifikasi perangkat yang memiliki mekanisme pembaruan jarak jauh untuk melakukan pembaruan massal berbagai program perangkat lunak (OS, <i>driver</i> , dan aplikasi) melalui perintah jarak jauh.	Teknologi
						b	Melakukan pemeliharaan perangkat dan <i>server</i> yang telah disetujui dari jarak jauh dan mencatat setiap <i>log</i> masuknya, sehingga akses yang tidak sah dapat dicegah.	Teknologi
				2.2.4	Memastikan lingkungan fisik aset informasi pada layanan Sistem Elektronik dipantau secara berkala untuk mendeteksi potensi ancaman	a	Penyelenggara Sistem Elektronik memastikan lingkungan fisik aset Sistem Elektronik dipantau secara tepat melalui pengaturan, perekaman, dan pemantauan akses fisik terhadap aset Sistem Elektronik. (misalnya cctv, akses kontrol, sensor, dll).	Teknologi
				2.2.5	Memastikan prosedur dan penerapannya senantiasa ditinjau dan	a	Penyelenggara Sistem Elektronik senantiasa melakukan peninjauan, analisis, dan peningkatan terhadap kontrol keamanan yang diterapkan sesuai hasil revidi dari respons	Tata Kelola

					ditingkatkan sesuai perkembangan ancaman		insiden keamanan dan hasil pemantauan, pengukuran, dan evaluasi ancaman internal dan eksternal.	
		2.3	Melindungi data	2.3.1	Pelindungan terhadap data yang tersimpan pada Penyelenggara Sistem Elektronik	a	Jika Penyelenggara Sistem Elektronik bertukar informasi yang perlu dilindungi dengan organisasi lain, maka Penyelenggara Sistem Elektronik perlu meminta organisasi lain tersebut untuk menyetujui persyaratan keamanan untuk perlindungan informasi tersebut.	Tata Kelola
						b	Mengenkripsi informasi dengan tingkat kekuatan keamanan yang sesuai standar keamanan.	Teknologi
				2.3.2	Pelindungan terhadap data yang terkirim dari Penyelenggara Sistem Elektronik	a	Penyelenggara Sistem Elektronik memastikan saluran komunikasi menerapkan enkripsi saat berkomunikasi antara perangkat Sistem Elektronik dan <i>server</i> Sistem Elektronik.	Teknologi
						b	Penyelenggara Sistem Elektronik memastikan kunci enkripsi dikontrol dengan aman sepanjang siklus hidup kunci enkripsi tersebut untuk memastikan pengoperasian yang benar dan data yang ditransmisikan, diterima, dan disimpan dengan aman.	Teknologi
				2.3.3	Memastikan ketersediaan kapasitas ruang	a	Penyelenggara Sistem Elektronik menyediakan sumber daya yang cukup untuk setiap sistem Sistem Elektronik (misalnya ruang	Teknologi

					penyimpanan data yang memadai		penyimpanan, sumber daya, dan sistem redundan).	
						b	Penyelenggara Sistem Elektronik memastikan dilakukannya pemeriksaan kualitas ruang penyimpanan data secara berkala, pendeteksi kegagalan operasional, dan pembaharuan perangkat lunak untuk perangkat penyimpanan data.	Teknologi
				2.3.4	Mengimplementasikan perlindungan dari kebocoran data	a	Saat menangani informasi yang akan dilindungi atau pengadaan perangkat yang memiliki fungsi penting bagi organisasi, pilih perangkat dan server yang dilengkapi dengan perangkat <i>anti-tampering</i> .	Teknologi
						b	Memastikan bahwa jalur komunikasi yang digunakan untuk mengirim informasi telah dilindungi dengan kontrol keamanan yang tepat.	Teknologi
				2.3.5	Mengimplementasikan mekanisme pengecekan integritas data untuk	a	Melakukan pemeriksaan integritas perangkat lunak yang berjalan di perangkat dan <i>server</i>	Teknologi
					verifikasi perangkat lunak, perangkat keras, dan data		pada waktu yang ditentukan oleh organisasi, untuk mencegah pemasangan perangkat lunak yang tidak sah.	
						b	Lakukan pemeriksaan integritas informasi yang akan dikirim, diterima, dan disimpan.	Teknologi

						c	Memperkenalkan mekanisme pemeriksaan integritas untuk memverifikasi integritas perangkat keras.	Teknologi
						d	Konfirmasikan bahwa perangkat keras dan perangkat lunak adalah produk asli dan memiliki sertifikat keamanan.	Teknologi
						e	Pelihara, perbarui, dan kelola informasi seperti asal data, dan riwayat pemrosesan data, di seluruh siklus hidup data.	Tata Kelola & Teknologi
				2.3.6	Memastikan prosedur pencadangan data dilakukan, dipelihara, dan diuji secara berkala	a	Tersedianya dan diterapkannya prosedur pencadangan sistem secara berkala dan pengujian kehandalan komponen untuk memastikan ketersediaan sistem.	Tata Kelola
				2.3.7	Menyediakan kebijakan pemusnahan data	a	Saat akan menghapuskan perangkat dan aset informasi, prosedur penghapusan data yang disimpan dari perangkat dan server serta informasi penting lainnya (misalnya, kunci pribadi dan sertifikat digital), atau dibuat agar tidak dapat dibaca.	Tata Kelola
		2.4	Melindungi aplikasi	2.4.1	Menyediakan prosedur konfigurasi dasar sistem dan kendali perubahan konfigurasi	a	Tersedianya dan diterapkannya prosedur untuk keamanan pada saat pengaturan sistem (misalnya, prosedur penerapan kata sandi, prosedur penerapan izin akses, dsb).	Tata Kelola
						b	Tersedianya dan diterapkannya prosedur untuk melakukan perubahan pengaturan pada perangkat.	Teknologi

						c	Tersedianya dan diterapkannya prosedur pembatasan perangkat lunak yang akan ditambahkan pada perangkat dan <i>server</i> .	Teknologi
				2.4.2	Mengembangkan dan mengimplementasikan rencana manajemen kerentanan.	a	Penyelenggara Sistem Elektronik mengembangkan dan mengimplementasikan rencana manajemen kerentanan yang meliputi mekanisme pengumpulan informasi kerentanan, inventarisasi kerentanan, hingga perbaikan terhadap kerentanan yang ditemukan pada aplikasi.	Teknologi
				2.4.3	Memastikan bahwa lingkungan pengembangan dan pengujian sistem dibedakan dari lingkungan produksi atau operasional	a	Penggunaan lingkungan pengembangan sistem yang berbeda dari lingkungan produksi yang meliputi pemisahan terhadap media penyimpanan, jaringan, lingkungan kerja, dsb.	Tata Kelola
				2.4.4	Mengimplementasikan prosedur pengembangan sistem yang aman	a	Tersedianya dan diterapkannya prosedur pengembangan perangkat lunak yang selalu	Tata kelola dan Teknologi
							memperhatikan aspek keamanan pada setiap tahapan siklus hidup pengembangannya.	
		2.5	Melindungi jaringan	2.5.1	Menerapkan sistem yang dikonfigurasi dengan prinsip fungsionalitas minimum	a	Minimalkan fungsi perangkat dan <i>server</i> dengan memblokir secara fisik dan logis port jaringan, USB, dan <i>port</i> serial yang tidak perlu, yang mengakses secara langsung bagian utama perangkat dan <i>server</i> .	Teknologi

						b	Memastikan <i>removable media</i> terlindungi dan penggunaannya terbatas sesuai dengan kebijakan.	Teknologi
				2.5.2	Menerapkan pelindungan terhadap jaringan komunikasi, akses sistem informasi, dan akses sistem kendali	a	Organisasi menentukan dan menerapkan segmentasi dan/atau pembagian zonasi jaringan komunikasi/internet. (misalnya dibagi menjadi lingkungan pengembangan, pengujian, lingkungan produksi, dan lingkungan lain dalam organisasi)	Teknologi
						b	Jika diperlukan, organisasi juga dapat melakukan isolasi terhadap jaringan yang menghubungkan dengan perangkat penting, misalnya perangkat SCADA atau ICS (<i>Industrial Control System</i>).	Teknologi
				2.5.3	Menggunakan perangkat-perangkat jaringan yang menerapkan fungsi keamanan	a	Memastikan perangkat jaringan mampu menerapkan mekanisme (misalnya, <i>fail safe</i> , <i>load balancer</i> , atau <i>hot swap</i>) yang perlu diimplementasikan untuk mencapai persyaratan ketahanan dalam situasi normal dan situasi yang merugikan.	Teknologi
						b	Memastikan fungsi keamanan pada perangkat jaringan dapat digunakan sesuai dengan kebutuhan dan sertifikat keamanan.	Teknologi
				2.5.4	Memastikan integritas jaringan senantiasa dilindungi	a	Tersedianya prosedur pelindungan terhadap integritas jaringan dengan cara melakukan pengujian dan monitoring terhadap konfigurasi jaringan, seperti pengujian terhadap segmentasi jaringan yang sesuai.	Teknologi

				2.5.5	Menerapkan prosedur dan teknologi pencegahan <i>malware</i>	a	Untuk melindungi ketersediaan data terhadap serangan <i>malware</i> , data organisasi harus di-rekam cadang secara berkala.	Teknologi
						b	Pemindaian/ <i>scanning</i> terhadap <i>removable media</i> yang akan digunakan pada perangkat komputer, <i>notebook</i> , <i>server</i> , atau perangkat pengolah informasi lainnya untuk mencegah masuknya <i>virus</i> dari luar ke dalam perangkat pengolah informasi dan jaringan komunikasi data milik organisasi.	Teknologi
						c	Mengunduh dan menginstalasi update anti malware terbaru, meliputi <i>antivirus</i> , <i>anti-spyware</i> , <i>spam filtering</i> , <i>web content filtering</i> , dan <i>intrusion detection and prevention system</i> .	Teknologi
						d	Meng- <i>update</i> perangkat komputer dengan melakukan <i>upgrade</i> dan <i>patch</i> sistem operasi dan aplikasi.	Teknologi
				2.5.6	Memastikan catatan audit atau log aktivitas ditentukan, didokumentasikan, diimplementasikan, dan ditinjau sesuai dengan kebijakan organisasi	a	Menentukan dan mendokumentasikan subjek atau ruang lingkup rekaman audit/pencatatan <i>log</i> , dan menerapkan dan meninjau catatan tersebut untuk mendeteksi insiden keamanan berisiko tinggi dengan benar.	Tata Kelola

				2.5.7	Memastikan bahwa informasi mengenai perlindungan terhadap teknologi dibagikan hanya kepada pihak tepercaya	a	Berbagi informasi mengenai efektivitas teknologi perlindungan data hanya dengan mitra yang tepat dan terpercaya.	Tata Kelola
		2.6	Melindungi sumber daya manusia	2.6.1	Menerapkan prosedur pengelolaan keamanan terhadap personel	a	Pemeriksaan verifikasi latar belakang terhadap semua calon personel harus dilakukan sebelum bergabung dengan Penyelenggara Sistem Elektronik dengan mempertimbangkan peraturan dan etika yang berlaku serta proporsional dengan kebutuhan bisnis, dan risiko keamanan.	Sumber Daya Manusia
						b	Perjanjian kontrak kerja harus menyatakan tanggung jawab personel dan organisasi untuk keamanan informasi.	Sumber Daya Manusia
						c	Proses pendisiplinan harus diformalkan dan dikomunikasikan untuk mengambil tindakan terhadap personel dan pihak berkepentingan	Organisasi & Sumber Daya Manusia
							lainnya yang telah melakukan pelanggaran kebijakan keamanan informasi.	
						d	Organisasi menetapkan dan mengomunikasikan kendali terhadap seluruh pegawai dan pihak ketiga setelah penghentian atau penggantian jabatan, tugas dan tanggung jawab keamanan informasi.	Sumber Daya Manusia

						e	Perjanjian kerahasiaan yang mencerminkan kebutuhan organisasi untuk perlindungan informasi harus diidentifikasi, didokumentasikan, ditinjau secara teratur dan ditandatangani oleh personel dan pihak berkepentingan terkait lainnya.	Sumber Daya Manusia
						f	Langkah-langkah keamanan harus diterapkan ketika personel bekerja dari jarak jauh untuk melindungi informasi yang diakses, diproses, atau disimpan di luar lokasi organisasi.	Sumber Daya Manusia
						g	Organisasi harus menyediakan mekanisme bagi personel untuk melaporkan kejadian keamanan informasi yang diamati atau dicurigai melalui saluran yang tepat.	Sumber Daya Manusia
				2.6.2	Menyelenggarakan pelatihan dan peningkatan kesadaran keamanan siber	a	Memberikan pelatihan dan pendidikan yang tepat kepada semua individu dalam organisasi dan mengelola catatan sehingga mereka dapat memenuhi peran dan tanggung jawab yang ditugaskan untuk mencegah dan mengatasi	Sumber Daya Manusia
							terjadinya dan tingkat keparahan insiden keamanan.	
						b	Memberikan pelatihan dan pendidikan keamanan yang sesuai kepada anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan yang mungkin terlibat dalam pencegahan dan penanggulangan insiden keamanan. Kemudian,	Sumber Daya Manusia

							kelola catatan pelatihan dan Pendidikan keamanan tersebut.	
						c	Memberikan pelatihan dan pendidikan yang tepat kepada semua individu dalam organisasi dan mengelola catatan sehingga mereka dapat memenuhi peran dan tanggung jawab yang ditugaskan untuk mencegah dan mengatasi terjadinya dan tingkat keparahan insiden keamanan.	Sumber Daya Manusia
						d	Meningkatkan isi pelatihan dan pendidikan tentang keamanan kepada anggota organisasi dan pihak terkait lainnya yang sangat penting dalam manajemen keamanan organisasi.	Sumber Daya Manusia
				2.6.3	Menyusun dan menerapkan kebijakan terkait kompetensi dan keahlian sumber daya manusia keamanan siber yang ada di PSE	a	Organisasi perlu menetapkan kebijakan terkait Kompetensi yang diperlukan dalam pelaksanaan Keamanan Siber diorganisasinya dengan menacu kepada Peta Okupasi Keamanan Siber Nasional Indonesia.	Sumber Daya Manusia
						b	Organisasi perlu menetapkan kebijakan pengembangan kompetensi SDM keamanan siber melalui pelatihan/pendidikan/ <i>workshop</i> .	Sumber Daya Manusia
						c	Organisasi sektor Pemerintah harus meningkatkan keterampilan dan kompetensi teknis dalam keamanan siber serta perilaku personel terhadap keamanan siber secara	Sumber Daya Manusia

							berkala dan sesuai dengan perkembangan teknologi dan pemanfaatan TIK.	
3.	Deteksi	3.1	Mengelola deteksi Peristiwa Siber	3.1.1	Menetapkan peran dan tanggung jawab organisasi pada kebijakan pendeteksian Peristiwa Siber	a	Memperjelas peran dan tanggung jawab organisasi serta penyedia layanan dalam rangka mendeteksi peristiwa keamanan.	Tata Kelola
						b	Penyelenggara Sistem Elektronik menyiapkan sistem dalam organisasi untuk mendeteksi, menganalisis, dan merespons peristiwa keamanan.	Teknologi
				3.1.2	Melaksanakan pendeteksian Peristiwa Siber sesuai persyaratan dan kebijakan yang berlaku	a	Melakukan proses pemantauan peristiwa keamanan siber, sesuai dengan peraturan, arahan, standar industri, dan aturan lainnya yang berlaku.	teknologi
						b	Melakukan pemantauan dan kontrol jaringan pada setiap titik masuk ke jaringan organisasi.	teknologi
				3.1.3	Menguji prosedur pendeteksian Peristiwa Siber secara berkala	a	Penyelenggara Sistem Elektronik melakukan pengujian secara periodik tentang efektivitas perangkat dan prosedur untuk mendeteksi peristiwa keamanan sebagaimana mestinya.	teknologi
				3.1.4	Menyampaikan informasi hasil pendeteksian Peristiwa Siber kepada pihak yang berhak	a	Informasi hasil pendeteksian kejadian keamanan diberitahukan kepada pihak yang terkait sesuai dengan persetujuan manajemen organisasi.	Tata Kelola
						b	Penyelenggara Sistem Elektronik melakukan reviu dan peningkatan prosedur pendeteksian peristiwa keamanan secara berkala.	Tata kelola

		3.2	Menganalisis anomali dan Peristiwa Siber	3.2.1	Menetapkan dan mendokumentasikan ambang batas peringatan terhadap insiden operasional yang diharapkan organisasi terhadap jaringan komputer dan alur data.	a	Penyelenggara Sistem Elektronik menetapkan dan menerapkan prosedur untuk mengidentifikasi dan mengelola ambang batas terhadap operasional jaringan dan arus informasi yang diharapkan antara pengguna, penyelenggara, dan sistem.	Tata Kelola
				3.2.2	Melaksanakan analisis terhadap Peristiwa Siber yang terdeteksi	a	Kejadian keamanan yang terdeteksi dianalisis untuk memahami target dan metode serangan.	Teknologi
						b	Identifikasi peristiwa keamanan secara akurat dengan menerapkan prosedur untuk melakukan analisis korelasi insiden keamanan dan analisis komparatif dengan informasi ancaman yang diperoleh dari luar organisasi.	Teknologi
				3.2.3	Menentukan dampak dari Peristiwa Siber yang terdeteksi	a	Identifikasi dampak peristiwa keamanan, termasuk dampaknya terhadap organisasi lain yang relevan.	Teknologi
				3.2.4	Mendokumentasikan hasil analisis terhadap Peristiwa Siber yang terdeteksi	a	Hasil analisis peristiwa siber didokumentasikan, serta dilaporkan kepada pihak manajemen sesuai ketentuan.	Tata kelola
		3.3.	Memantau Peristiwa Siber berkelanjutan	3.3.1	Menerapkan prosedur pendeteksi kode	a	Gunakan perangkat teknologi yang dapat mendeteksi perilaku abnormal pada sistem dan jaringan. (misalnya perangkat <i>intrusion</i>	Teknologi

					berbahaya dan tak berizin		detection and prevention systems, next-generation firewall, endpoint detection and response, dll)	
						b	Memvalidasi apakah informasi atau file yang diberikan dari dunia maya tidak mengandung kode berbahaya, sebelum tindakan dilakukan.	Teknologi
						c	Memvalidasi integritas dan keaslian informasi yang diberikan dari dunia maya sebelum tindakan dilakukan.	Teknologi
				3.3.2	Memonitor kegiatan personel yang berada di dalam lingkup sistem Sistem Elektronik	a	Memastikan bahwa personel yang berada pada layanan Sistem Elektronik tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem Sistem Elektronik.	Sumber Daya Manusia
				3.3.3	Memonitor kegiatan pihak ketiga yang berada di dalam lingkup sistem Sistem Elektronik	a	Memastikan bahwa pihak ketiga yang berada pada layanan Sistem Elektronik tidak melakukan koneksi, memasang perangkat keras ataupun perangkat lunak yang tidak berizin pada lingkup sistem Sistem Elektronik.	Tata kelola
				3.3.5	Menerapkan teknologi pemindaian kerentanan terhadap sistem Sistem Elektronik	a	Memastikan bahwa seluruh perangkat teknologi pada lingkup Sistem Elektronik telah diuji keamanannya melalui penilaian kerentanan, uji penetrasi, atau audit keamanan.	Teknologi
						b	Penyelenggara Sistem Elektronik memastikan adanya pemeriksaan rutin di perangkat dan server yang dikelola dalam organisasi.	teknologi

4.	Penanggulangan dan pemulihan	4.1	Menyusun perencanaan penanggulangan dan pemulihan insiden siber	4.1.1	Menyusun dan menetapkan rencana tanggap insiden siber yang disetujui oleh pimpinan organisasi	a	Menentukan dan menetapkan prosedur tanggap insiden beserta pembagian peran yang jelas antara pihak manajemen, personel pengelola Sistem Elektronik, dan pihak lainnya yang mencakup tindakan yang harus dilakukan setelah mendeteksi adanya insiden siber.	Tata Kelola
						b	Menyusun dan menetapkan prosedur rencana tanggap insiden siber, mulai dari tahapan persiapan, identifikasi, kontainmen, eradiksi, pemulihan, dan peningkatan berkelanjutan	Tata Kelola
						c	Menentukan skenario insiden keamanan yang mungkin terjadi pada layanan Sistem Elektronik dan menambahkannya pada dokumen rencana tanggap insiden siber.	Tata Kelola
						d	Memastikan rencana tanggap insiden siber dikomunikasikan kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan.	Tata Kelola
				4.1.2	Menyusun dan menetapkan rencana keberlangsungan kegiatan yang disetujui oleh pimpinan organisasi	a	Menentukan dan menetapkan daftar fungsi dan layanan vital bagi penyelenggaraan Sistem Elektronik, beserta daftar pembagian peran dan	Tata Kelola
							tanggung jawab dengan pihak-pihak yang berhubungan dengan operasional layanan Sistem Elektronik.	
						b	Menentukan dan menetapkan strategi, tahapan, beserta target waktu yang dibutuhkan untuk memulihkan dan menjalankan fungsi dan layanan vital secara penuh/kembali normal.	Tata Kelola

						c	Menentukan daftar sumber daya, peralatan, dan personil yang dibutuhkan untuk menjalankan fungsi dan layanan vital.	Tata Kelola
						d	Memastikan rencana keberlangsungan layanan dikomunikasikan kepada pihak-pihak yang berkepentingan dan berhak sesuai ketentuan.	Tata Kelola
				4.1.3	Memastikan rencana tanggap insiden siber dan rencana keberlangsungan kegiatan dilaksanakan dan disimulasikan secara berkala	a	Memastikan rencana tanggap insiden siber dan rencana keberlangsungan kegiatan disimulasikan secara berkala oleh seluruh pihak yang terlibat dalam lingkup Sistem Elektronik. (misalnya dalam kegiatan simulasi kesiapsiagaan insiden siber).	Tata Kelola
				4.1.4	Memastikan personel yang mengelola Sistem Elektronik mengetahui peran dan prosedur penanggulangan dan pemulihan sesuai rencana tanggap insiden	a	Penyelenggara Sistem Elektronik menentukan dan menetapkan personel yang ditugaskan dalam tim tanggap insiden siber.	SDM & Tata Kelola
					siber dan rencana keberlangsungan kegiatan	b	Penyelenggara Sistem Elektronik memastikan personel mengetahui perannya dan urutan pengoperasian bila respons diperlukan.	SDM & Tata Kelola
						c	Penyelenggara Sistem Elektronik mengidentifikasi siapa saja pihak-pihak pihak-pihak terkait dalam proses penanggulangan dan	SDM & Tata Kelola

							pemulihan insiden, misalnya aparat penegak hukum, regulator, maupun tim TTIS nasional.	
						d	Penyelenggara Sistem Elektronik perlu mengembangkan dan mengelola aturan mengenai penerbitan dan distribusi informasi setelah terjadinya insiden keamanan, sehingga informasi organisasi hanya boleh keluar melalui personel yang berwenang saja.	SDM & Tata Kelola
						4.1.5	Memastikan personel yang mengelola Sistem Elektronik memahami prosedur penggunaan rekam cadang.	Tata Kelola
						a	Penyelenggara Sistem Elektronik memastikan personel yang mengelola Sistem Elektronik melakukan prosedur rekam cadang untuk mengamankan aset informasi berupa sistem/data yang tersimpan di dalam sistem Sistem Elektronik, serta memastikan bahwa media yang digunakan untuk menyimpan data tersebut telah diamankan.	
		4.2	Menganalisis dan melaporkan insiden siber	4.2.1	Mengumpulkan informasi kondisi Sistem Elektronik terkini baik dari hasil deteksi internal maupun	a	Penyelenggara Sistem Elektronik memastikan hasil analisis deteksi peristiwa siber diperiksa untuk menilai ada atau tidaknya anomali pada sistem.	Teknologi
					sumber informasi eksternal	b	Penyelenggara Sistem Elektronik mengumpulkan dan menganalisis laporan peristiwa siber yang diterima baik dari pengguna layanan, maupun sumber eksternal organisasi misalnya laporan dari Tim Tanggap Insiden Siber nasional atau mitra pihak ketiga.	Teknologi

				4.2.2	Mengidentifikasi dan menganalisis potensi dampak dari insiden siber	a	Penyelenggara Sistem Elektronik harus mengidentifikasi dan menganalisis potensi dampak insiden siber pada layanan Sistem Elektronik, termasuk organisasi, dan pihak terkait seperti mitra ketiga berdasarkan laporan lengkap insiden siber.	Teknologi
				4.2.3	Memastikan insiden siber dikategorikan sesuai kriteria yang telah ditetapkan	a	Penyelenggara Sistem Elektronik memastikan laporan insiden siber dikumpulkan, dikategorisasikan, dan diprioritaskan sesuai dampak risiko terhadap organisasi.	Tata kelola
				4.2.4	Memastikan bahwa insiden siber dilaporkan kepada pihak yang terkait	a	Penyelenggara Sistem Elektronik memastikan informasi mengenai insiden siber dilaporkan kepada pihak yang berwenang sesuai dengan kriteria yang ditetapkan oleh organisasi dan peraturan perundangan yang berlaku.	Tata Kelola
						b	Penyelenggara Sistem Elektronik memastikan proses koordinasi dengan para pemangku kepentingan dilakukan sesuai dengan rencana tanggap insiden siber (seperti kepada Kementerian atau Lembaga pembina sektor, Tim	Tata Kelola
							Tanggap Insiden Siber nasional, atau mitra pihak ketiga)	
		4.3	Melaksanakan penanggulangan dan pemulihan insiden siber	4.3.1	Memastikan insiden siber diisolasi dan dimitigasi sesuai rencana tanggap insiden siber	a	Penyelenggara Sistem Elektronik harus mengambil langkah-langkah yang diperlukan untuk meminimalkan kerusakan terkait keamanan dan mengurangi dampak yang disebabkan oleh insiden tersebut. Misalnya	Tata Kelola

						melakukan isolasi terhadap jaringan yang terdapat insiden siber.	
					b	Penyelenggara Sistem Elektronik harus mengidentifikasi hal-hal yang perlu diprioritaskan dan ruang lingkup respons yang perlu diambil.	Tata Kelola
					c	Penyelenggara Sistem Elektronik harus mengambil tindakan yang tepat terhadap perangkat yang terpengaruh oleh insiden siber, terutama mengenai fasilitas produksi yang rusak akibat insiden keamanan.	Tata Kelola
					d	Penyelenggara Sistem Elektronik mendokumentasikan hasil mitigasi insiden siber tersebut sebagai bahan pembelajaran berkelanjutan.	Tata Kelola
			4.3.2	Mengumpulkan dan memelihara bukti insiden siber dari Sistem Elektronik terdampak	a	Penyelenggara Sistem Elektronik memastikan informasi mengenai insiden keamanan yang terdeteksi dikategorikan dan disimpan menurut ukuran dampak terkait keamanan, penyebab insiden, dan faktor lainnya yang diperlukan.	Tata Kelola
			4.3.3	Menginvestigasi dan eradikasi penyebab insiden siber	a	Untuk keperluan investigasi dan/atau audit, maka Penyelenggara Sistem Elektronik menerapkan forensik digital terhadap aset informasi yang terdampak insiden keamanan untuk menemukan penyebab insiden.	Tata Kelola & Teknologi
					b	Penyelenggara Sistem Elektronik harus memastikan bahwa seluruh aset informasi yang terdampak insiden siber telah diperiksa setiap	Teknologi

							komponennya untuk menghapus setiap kode berbahaya atau indikasi ancaman lainnya yang terkait insiden siber.	
				4.3.4	Mengoordinasikan dengan pihak terkait dalam rangka eskalasi penanggulangan insiden siber	a	Jika insiden meningkat atau meluas, maka Penyelenggara Sistem Elektronik perlu menyiapkan dan melaksanakan prosedur eskalasi insiden siber, seperti melaporkan kepada tim tanggap insiden siber (TTIS) sektoral dan nasional, serta menyiapkan informasi yang relevan terkait insiden siber tersebut.	Tata Kelola
				4.3.5	Memastikan setiap aset informasi diperiksa keamanannya setelah penanganan insiden siber	a	Penyelenggara Sistem Elektronik melakukan pemeriksaan kepada seluruh aset informasi yang berhubungan dengan Sistem Elektronik untuk memastikan seluruh sistem tersebut telah bersih dari indikasi ancaman atau serangan yang telah terjadi.	Teknologi
				4.3.6	Melaksanakan prosedur pencadangan dan pemulihan sistem dan data sesuai rencana keberlangsungan kegiatan	a	Penyelenggara Sistem Elektronik melaksanakan prosedur pemulihan sistem/data dari media penyimpanan dalam hal terjadi keadaan darurat.	Teknologi
						b	Penyelenggara Sistem Elektronik melaksanakan simulasi terhadap prosedur pemulihan sistem/data dari media penyimpangan rekam cadang secara periodik.	Teknologi

						c	prosedur rekam cadang (<i>back-up</i>) sedapat mungkin dilakukan secara otomatis dengan memanfaatkan perangkat-perangkat penyimpanan yang mempunyai fitur <i>job-schedulling</i> .	Teknologi
						d	Penyelenggara Sistem Elektronik memastikan data yang disimpan pada media penyimpanan rekam cadang diamankan menggunakan enkripsi.	Teknologi
						e	Penyelenggara Sistem Elektronik menentukan waktu pelaksanaan rekam cadang terhadap data organisasi yang disesuaikan dengan tingkat kritikalitas data dan kebutuhan organisasi.	Tata Kelola & Teknologi
						f	Penyelenggara Sistem Elektronik memastikan hasil pelaksanaan rekam cadang data didokumentasikan.	Tata Kelola & Teknologi
				4.3.7	Menentukan dan menerapkan retensi terhadap hasil pencadangan yang sudah tidak terpakai sesuai ketentuan	a	Penyelenggara Sistem Elektronik memastikan media penyimpanan rekam cadang telah disimpan secara aman.	Tata kelola
						b	Pemusnahan terhadap data yang disimpan pada media rekam cadang harus dilaksanakan dengan persetujuan pimpinan organisasi.	Tata Kelola
						c	Pemusnahan data pada media rekam cadang dilakukan dengan melakukan format ulang atas media rekam cadang dan memastikan bahwa data tersebut tidak dapat diakses lagi.	Teknologi

				4.3.8	Pengujian ulang terhadap fungsi vital dan fungsi pendukung untuk memastikan capaian pemulihan terpenuhi.	a	Penyelenggara Sistem Elektronik harus menyusun dan menerapkan prosedur yang bertujuan untuk memastikan seluruh fungsi pada layanan Sistem Elektronik telah beroperasi dengan normal pasca insiden siber.	Tata Kelola
				4.3.9	Memastikan organisasi memiliki dan mengelola strategi komunikasi publik ketika terjadi insiden siber dan setelah penanggulangan serta pemulihan insiden siber	a	Penyelenggara Sistem Elektronik perlu menyusun dan menerapkan strategi komunikasi publik dalam hal mengelola informasi yang perlu disampaikan terkait insiden siber.	Tata Kelola
						b	Penyelenggara Sistem Elektronik memastikan bahwa proses penanganan dan pemulihan insiden dikomunikasikan dengan pihak yang berkepentingan sesuai dengan peraturan perundangan.	Tata Kelola
				4.3.10	Penyampaian informasi penanggulangan dan pemulihan insiden siber kepada pihak terkait	a	Penyelenggara Sistem Elektronik menyusun laporan hasil penanganan insiden siber dan menyampaikannya kepada Kementerian atau Lembaga di masing-masing sektor.	Tata kelola
		4.4	Meningkatkan keamanan setelah terjadinya insiden siber	4.4.1	Meninjau kembali efektifitas Kontrol Keamanan yang telah diterapkan	a	Penyelenggara Sistem Elektronik mengevaluasi kontrol keamanan yang diterapkan apakah masih relevan terhadap spektrum ancaman yang ada atau perlu ada perbaikan dan penambahan.	Tata Kelola
				4.4.2	Mereviu dan/atau memperbarui dokumen	a	Penyelenggara Sistem Elektronik melakukan reviu dan pembaharuan terhadap dokumen	Tata Kelola

					rencana tanggap insiden siber dan rencana keberlangsungan kegiatan secara berkala		rencana tanggap insiden siber dan pemulihan jika terdapat hal-hal yang dapat dijadikan pembelajaran berkelanjutan bagi organisasi.	
						b	Penyelenggara Sistem Elektronik mendokumentasikan kerentanan, ancaman, atau risiko yang baru ditemukan beserta rencana mitigasinya ke dalam dokumen pengelolaan risiko.	Tata Kelola
				4.4.3	Mengumpulkan dan memelihara hasil forensik digital	a	Laporan hasil pelaksanaan forensik digital dikumpulkan dan dipelihara meliputi juga informasi-informasi yang relevan terhadapnya.	Tata kelola
						b	Laporan hasil pelaksanaan forensik digital dapat disampaikan kepada pihak berwajib untuk proses investigasi dan penegakkan hukum sesuai ketentuan yang berlaku.	Tata kelola
				4.4.4	Meninjau efektivitas kinerja penanganan insiden yang dilakukan oleh tim tanggap insiden siber secara berkala	a	Penyelenggara Sistem Elektronik melakukan peninjauan terhadap efektifitas kinerja penanganan insiden yang dilakukan oleh tim tanggap insiden siber secara berkala.	Tata Kelola
						b	Melakukan langkah-langkah perbaikan yang diperlukan terhadap pelaksanaan penanganan insiden siber meliputi dari segi teknologi, tata kelola, atau peningkatan kapasitas SDM.	Tata Kelola

III. TAHAP III : PENGUKURAN TINGKAT KEMATANGAN KEAMANAN SIBER

Untuk menggambarkan kapabilitas dan kemajuan organisasi dalam menerapkan, meningkatkan, dan menjalankan Keamanan Siber secara efektif dan efisien, Penyelenggara Sistem Elektronik perlu melaksanakan pengukuran tingkat kematangan secara mandiri paling sedikit 1 (satu) kali dalam 1 (satu) tahun, menggunakan instrumen penilaian yang ditetapkan oleh BSSN.

1. Proses Pengukuran Mandiri

- a. Pengukuran Tingkat Kematangan dilakukan secara mandiri oleh setiap Penyelenggara Sistem Elektronik.
- b. Kegiatan ini perlu dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
- c. Pengukuran dilakukan terhadap empat domain pada Kerangka Kerja Pelindungan Sistem Elektronik : Identifikasi, Proteksi, Deteksi, serta Penanggulangan dan Pemulihan.
- d. Proses ini menggunakan instrumen penilaian resmi yang disusun oleh BSSN.

2. Level Kategori Kematangan

Hasil pengukuran akan menempatkan organisasi dalam salah satu dari lima kategori tingkat kematangan, yaitu:

- a. Level 1 – Awal : Penerapan keamanan siber masih dalam tahap awal, bersifat informal, belum terorganisir, dan tidak konsisten.
- b. Level 2 – Berulang : Prosedur penerapan keamanan siber sudah ada dan terorganisir, namun masih bersifat informal dan belum dijalankan secara konsisten.
- c. Level 3 – Terdefinisi : Penerapan keamanan siber telah terdefinisi dengan baik, bersifat formal, terorganisir, dan dilaksanakan secara konsisten serta direviu secara berkala.
- d. Level 4 – Terkelola : Penerapan keamanan siber telah terkelola dengan baik dan implementasi perbaikan dilakukan secara berkelanjutan.

- e. Level 5 – Inovatif: Penerapan keamanan siber telah mencapai tingkat optimal, terimplementasi secara menyeluruh, terotomatisasi, dan menjadi bagian dari budaya organisasi.

3. Proses Verifikasi

- a. PSE dapat melakukan proses verifikasi terhadap hasil penilaian mandiri pengukuran tingkat kematangan keamanan siber di organisasinya.
 - b. Proses verifikasi dilakukan melalui beberapa metode, seperti penelaahan dokumen, wawancara, observasi lapangan, dan pemeriksaan kesesuaian antara hasil penilaian dengan bukti pendukung.
 - c. Proses verifikasi dapat dilakukan oleh Kementerian/Lembaga pengatur dan pengawas sektor atau Lembaga Sertifikasi Sistem Pengamanan Informasi yang sudah terdaftar di Badan Siber dan Sandi Negara.
4. Instrumen penilaian kematangan keamanan siber dapat diunduh pada *website* BSSN, menu Publikasi.