



SALINAN

**SEKRETARIS JENDERAL
DEWAN PERWAKILAN RAKYAT
REPUBLIK INDONESIA**

**PERATURAN SEKRETARIS JENDERAL
DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA
NOMOR 4 TAHUN 2023**

**TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI**

DENGAN RAHMAT TUHAN YANG MAHA ESA

**SEKRETARIS JENDERAL
DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA,**

- Menimbang
- a. bahwa Peraturan Sekretaris Jenderal Nomor 19 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia belum mengadopsi standar ISO 27001:2022 tentang Sistem Manajemen Keamanan Informasi sehingga belum sesuai dengan perkembangan dan kebutuhan organisasi;
 - b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia tentang Sistem Manajemen Keamanan Informasi;
- Mengingat
- 1. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

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. Peraturan Presiden Nomor 26 Tahun 2020 tentang Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 39) sebagaimana telah diubah dengan Peraturan Presiden Nomor 16 Tahun 2023 tentang Perubahan atas Peraturan Presiden Nomor 26 Tahun 2020 tentang Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 30);
4. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
5. 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);
6. Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia Nomor 12 Tahun 2020 tentang Rencana Induk Teknologi Informasi dan Komunikasi Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia Tahun 2020-2024;

7. Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia Nomor 3 Tahun 2023 tentang Perubahan Kedua atas Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia Nomor 6 Tahun 2021 tentang Organisasi dan Tata Kerja Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia;
8. Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia Nomor 9 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) di Lingkungan Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia;

MEMUTUSKAN :

Menetapkan : PERATURAN SEKRETARIS JENDERAL DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI.

Pasal 1

Sistem Manajemen Keamanan Informasi di lingkungan Dewan Perwakilan Rakyat Republik Indonesia berpedoman pada standar ISO 27001:2022.

Pasal 2

- (1) Penyelenggara Sistem Manajemen Keamanan Informasi dilaksanakan oleh:
 - a. manajemen puncak;
 - b. *Chief Information Security Officer* yang selanjutnya disingkat CISO;
 - c. manajer keamanan informasi; dan
 - d. petugas keamanan informasi.
- (2) Manajemen puncak sebagaimana dimaksud pada ayat (1) huruf a dilaksanakan oleh 1 (satu) orang pejabat pimpinan tinggi madya.
- (3) CISO sebagaimana dimaksud pada ayat (1) huruf b dilaksanakan oleh 1 (satu) orang pejabat pimpinan tinggi pratama di bidang teknologi dan informasi.
- (4) Manajer keamanan informasi sebagaimana dimaksud pada ayat (1) huruf c dilaksanakan oleh 1 (satu) orang pejabat administrator.
- (5) Susunan penyelenggara keamanan informasi sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia.

Pasal 3

Manajemen puncak sebagaimana dimaksud dalam Pasal 2 huruf a bertugas memimpin memantau serta memberikan masukan terkait dengan penerapan Sistem Manajemen Keamanan Informasi.

Pasal 4

- (1) CISO sebagaimana dimaksud dalam Pasal 2 huruf b bertugas mengkoordinasikan penerapan strategi dan memantau serta memberikan masukan terkait dengan penerapan Sistem Manajemen Keamanan Informasi di Dewan Perwakilan Rakyat Republik Indonesia.
- (2) Dalam pelaksanaan tugas sebagaimana dimaksud pada ayat (1), CISO menyusun dokumen antara lain:
 - a. ruang lingkup;
 - b. pernyataan kesesuaian (*Statement of Applicability*);
 - c. petunjuk teknis *Disaster Recovery Plan*; dan
 - d. petunjuk teknis risiko informasi teknologi (*Information Technology Risk*).
- (3) Dokumen sebagaimana dimaksud pada ayat (3) ditetapkan dengan Keputusan Sekretaris Jenderal.

Pasal 5

Manajer keamanan informasi sebagaimana dimaksud dalam Pasal 2 huruf c bertugas membantu CISO dalam mengkoordinasikan, memantau serta memberikan masukan terkait dengan penerapan Sistem Manajemen Keamanan Informasi.

Pasal 6

Petugas keamanan informasi sebagaimana dimaksud dalam Pasal 2 huruf d bertugas melaksanakan penerapan strategi sistem manajemen keamanan informasi

Pasal 7

Ketentuan lebih lanjut mengenai pelaksanaan sistem manajemen keamanan informasi sebagaimana dimaksud dalam Pasal 1 tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia ini.

Pasal 8

Ketentuan teknis mengenai penerapan sistem manajemen keamanan informasi sesuai ISO 27001:2022 ditetapkan dengan Keputusan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia.

Pasal 9

- (1) Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia melaksanakan pemantauan dan evaluasi melalui:
 - a. internal audit; dan
 - b. eksternal audit.
- (2) Internal audit dan eksternal audit sebagaimana dimaksud pada ayat (1) dilaksanakan minimal 1 (satu) tahun sekali.

Pasal 10

Pada saat Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia ini mulai berlaku, Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia Nomor 19 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi dicabut dan dinyatakan tidak berlaku.

Pasal 11

Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia ini berlaku sejak tanggal ditetapkan.

Ditetapkan di Jakarta,
pada tanggal 31 Maret 2023
SEKRETARIS JENDERAL,

ttd.

INDRA ISKANDAR

Salinan Sesuai Dengan Aslinya
SEKRETARIAT JENDERAL DEWAN PERWAKILAN RAKYAT
REPUBLIK INDONESIA
Biro Hukum dan Pengaduan Masyarakat

ttd.

Arini Wijayanti, S.H., M.H.

LAMPIRAN
PERATURAN SEKRETARIS JENDERAL
DEWAN PERWAKILAN RAKYAT
REPUBLIK INDONESIA NOMOR 4
TAHUN 2023 TENTANG SISTEM
MANAJEMEN KEAMANAN INFORMASI

KETENTUAN PELAKSANAAN
SISTEM MANAJEMEN KEAMANAN INFORMASI

A. DEFINISI

Dalam Peraturan ini yang dimaksud dengan:

1. Dewan Perwakilan Rakyat Republik Indonesia yang selanjutnya disingkat DPR RI adalah sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia;
2. Sekretariat Jenderal DPR RI adalah aparatur pemerintah yang di dalam menjalankan tugas dan fungsinya berada di bawah dan bertanggungjawab langsung kepada Pimpinan DPR RI;
3. Sekretaris Jenderal adalah Sekretaris Jenderal DPR RI;
4. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE;
5. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah teknologi informasi dan komunikasi berbasis elektronika yang digunakan untuk melakukan pengambilan, pengumpulan, pengolahan, penyimpanan, penyebaran, dan penyajian informasi;
6. Sistem Informasi adalah serangkaian perangkat keras, perangkat lunak, aplikasi, sumber daya manusia, serta prosedur dan atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi informasi yang berguna untuk mencapai suatu tujuan;

7. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah suatu sistem manajemen yang meliputi kebijakan, 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 DPR RI.
8. Perangkat Lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan perintah berupa data yang telah diprogram, disimpan, dan diformat secara digital.
9. Aplikasi adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan pada DPR RI yang berbasis situs web, *desktop* dan/atau *mobile*.
10. Perangkat Keras adalah perangkat & peralatan berwujud fisik yang digunakan untuk mendukung Aplikasi dan jaringan komunikasi dalam menjalankan kegiatan operasionalnya.
11. Keamanan Informasi adalah terjaganya kerahasiaan, keutuhan, dan ketersediaan informasi.
12. Infrastruktur adalah Perangkat Keras, Perangkat Lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, Aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya
13. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan Keamanan Informasi dengan menggunakan 2 (dua) prinsip yaitu enkripsi dan dekripsi.
14. Pusat Data adalah suatu fasilitas yang digunakan untuk menempatkan sistem elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.

15. *Chief Information Security Officer* yang selanjutnya disingkat CISO adalah pejabat yang berperan sebagai koordinator dalam pelaksanaan implementasi kebijakan dan standar SMKI di Sekretariat Jenderal DPR RI.
16. Pengguna adalah Anggota DPR RI, Pegawai Sekretariat Jenderal DPR RI, Tenaga Ahli, Staf Administrasi Anggota DPR RI, Tenaga Sistem Pendukung, dan atau pihak ketiga yang diberikan hak mengakses sistem TIK di lingkungan Sekretariat Jenderal DPR RI.
17. Pihak Ketiga adalah semua unsur di luar Pengguna dan unit pemilik proses bisnis Sekretariat Jenderal DPR RI yang bukan bagian dari pegawai Sekretariat Jenderal DPR RI seperti *Supplier/Vendor, Internet provider*, atau *IT support provider* Fasilitas dan peralatan lainnya.
18. Penyelenggara SMKI adalah tim yang bertugas merencanakan, mengimplementasikan, dan mengontrol proses dalam pelaksanaan SMKI.
19. Manajemen adalah petinggi dari Penyelenggara SMKI seperti Manajemen Puncak dan CISO di DPR RI.
20. Regulator adalah kementerian dan/atau lembaga yang berwenang menerbitkan peraturan terkait SMKI.

B. Maksud dan Tujuan

1. Maksud ditetapkannya SMKI ini adalah:
 - a. sebagai acuan terwujudnya standarisasi kerangka kerja pelaksanaan pengelolaan SMKI di lingkungan DPR RI;
 - b. sebagai pedoman bagi pelaksanaan SMKI dalam menyusun dan menetapkan prosedur operasional sehingga terjadi keselarasan pada tataran strategis, taktis, dan operasional dalam penyelenggaraan SMKI di lingkungan DPR RI.

2. Tujuan ditetapkan SMKI ini adalah:

- a. untuk memberikan kerangka kerja dalam implementasi SMKI dengan mengamankan sumber daya informasi yang disediakan dan melindungi informasi dari akses secara tidak berwenang, memelihara kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi;
- b. mengoptimalkan pengelolaan risiko penggunaan TI, dengan mencegah dan mengurangi dampak insiden SMKI sehingga dapat memelihara dan meningkatkan reputasi DPR RI;
- c. menjaga aspek kerahasiaan, integritas dan ketersediaan dari informasi DPR RI.

C. Konteks Organisasi

1. Konteks Internal dan Konteks Eksternal

Sekretariat Jenderal DPR RI wajib mempertimbangkan konteks baik internal maupun eksternal yang mempengaruhi proses penyediaan layanan kepada Pengguna layanan TI yang mana konteks tersebut merupakan penerjemahan isu yang ada di Klausul ISO 27001. Dalam penyelenggaraan proses layanan TI di Sekretariat Jenderal DPR RI, perlu melakukan identifikasi terhadap pihak lain yang terkait dengan proses penyelenggaraan layanan TI kepada Pengguna.

Sekretariat Jenderal DPR RI melakukan identifikasi terhadap isu atau hal-hal yang relevan terhadap pencapaian tujuan SMKI dan yang mungkin dapat mempengaruhi kemampuan Sekretariat Jenderal DPR RI dalam mencapai tujuan tersebut.

Tabel 1. KONTEKS INTERNAL & KONTEKS EKSTERNAL

No	Isu	Faktor	Implikasi	Tantangan
Konteks Internal				
1	Knowledge & Awareness (Skill & competency) Kapasitas unit kerja yang membidangi teknologi dan informasi DPR RI dalam mengembangkan dan meningkatkan pengetahuan internal maupun kesadaran Keamanan Informasi dalam melakukan kegiatan operasional.	Budaya Kerja	Penerapan SMKI termasuk proses bisnis internal biasanya akan bertentangan dengan cara dan budaya kerja di dalam unit kerja yang membidangi teknologi dan informasi. Perubahan pada umumnya akan ditolak oleh pihak internal dan akan menghambat implementasi SMKI.	Peningkatan kesadaran akan pentingnya SMKI perlu dilakukan secara berkelanjutan mulai dari tingkat strategis hingga operasional. Peningkatan kewaspadaan juga diperlukan untuk mengevaluasi efektivitas pelaksanaan SMKI, serta rencana perbaikan yang perlu dilakukan di masa mendatang.
2	Organization & Governance perubahan struktur organisasi (reorganization), tentu akan mempengaruhi budaya organisasi, proses bisnis, peran, tanggung jawab & wewenang, kebijakan & prosedur, kegiatan operasional Keamanan Informasi dan pengembangan kegiatan operasional di masa depan.	Perubahan Struktur Kepemilikan dan Pengelolaan Organisasi Pedoman operasional	Gangguan pada pengambilan keputusan. Kejelasan tugas dan tanggung jawab pembagian pelaksanaan kegiatan operasional dan dukungan layanan operasional Implementasi SMKI tidak efektif dan efisien.	Identifikasi dampak atas perubahan organisasi dan transisi operasional perlu dilakukan termasuk menentukan langkah pengendalian risiko yang mungkin terjadi. Ketersediaan pedoman tentang cara pengelolaan informasi dalam pelaksanaan SMKI.

No	Isu	Faktor	Implikasi	Tantangan
4	Assets & Technology Seiring dengan perkembangan teknologi, sistem/aplikasi masih membutuhkan pengembangan dan perbaikan yang selaras dengan kebutuhan bisnis dan tujuan unit kerja yang membidangi teknologi dan informasi, investasi besar dalam teknologi. Efektivitas mekanisme penanganan aset berdasarkan klasifikasi diperlukan untuk mengelola aset operasional unit kerja yang membidangi teknologi dan informasi yang besar.	<i>Keuangan</i>	Implementasi kontrol teknis Keamanan Informasi membutuhkan biaya tambahan untuk investasi perangkat TI dan operasional, yang realisasinya perlu dikendalikan sehingga pelaksanaannya dilakukan sesuai rencana.	pengembangan unit kerja yang membidangi teknologi dan informasi. Kontrol teknis yang akan diambil dengan sepatutnya mempertimbangan aspek risiko yang tidak dapat diterima oleh unit kerja yang membidangi teknologi dan informasi, sehingga mengendalikan biaya harus direalisasikan.
		Utilisasi sumber daya	Kebutuhan atas utilisasi sumber daya infrastruktur internal yang optimal baik IT maupun non-IT	Pemecahan masalah atas sumber daya manusia dilakukan dengan menjalin kerjasama dengan unit kerja yang membidangi teknologi dan informasi untuk mempertahankan serta mengembangkan potensi Infrastruktur teknologi maupun aset pemrosesan informasi lainnya.
		Perubahan Lokasi Kerja	Perubahan atas pengendalian fisik dan lingkungan kantor karena adanya relokasi kantor	Implementasi standar pengamanan fisik dan lingkungan di lokasi baru

No	Isu	Faktor	Implikasi	Tantangan
		Kebijakan <i>work from home</i>	Peningkatan pengendalian <i>remote access</i> dan <i>teleworking</i> karena adanya tuntutan bekerja dari rumah	Implementasi standar pengamanan <i>remote access</i> dan adanya risiko baru atas Keamanan Informasi sebagai manifestasi dari pelaksanaan bekerja dari rumah
5	Process Perubahan proses bisnis dan persyaratan kepatuhan dalam menjalankan proses bisnis sesuai dengan ketentuan yang ditetapkan oleh unit kerja yang membidangi teknologi dan informasi dan risiko global terhadap <i>outsourcing</i> proses bisnis karena unit kerja yang membidangi teknologi dan informasi bekerja sama dengan Pihak Ketiga dalam mendukung kegiatan operasional sehari-hari mereka.	Politik internal Kinerja Organisasi	Implementasi SMKI biasanya akan bersinggungan antara proses bisnis dengan proses bisnis lainnya di unit kerja yang membidangi teknologi dan informasi. Pengoperasian dan pemrosesan bisnis yang menjunjung prinsip efektivitas dan efisiensi secara berkelanjutan	Penerapan dan pelaksanaan pengendalian SMKI pada proses lintas pemotongan diperlukan untuk memastikan kemudahan pengambilan keputusan serta pemisahan tugas dan tanggung jawab. Ketersediaan mekanisme pengukuran kinerja maupun evaluasi kinerja organisasi baik secara bisnis maupun pengamanan informasi
6	IT Services Jangkauan unit kerja yang membidangi teknologi dan informasi yang luas membutuhkan proses Manajemen operasional yang kompleks dan pemantauan yang cukup untuk memastikan kualitas dan ketersediaan	Kualitas layanan produk Perubahan kegiatan	Kegagalan mencapai tujuan bisnis dan tujuan SMKI guna menjamin layanan yang aman dan berkualitas Beralihnya fokus layanan unit kerja yang membidangi teknologi dan	Pertimbangan Keamanan Informasi secara komprehensif dalam menerapkan kontrol pengamanan dan mutu layanan TI untuk meningkatkan kepercayaan pihak terkait. Mengoptimalkan layanan unit kerja yang membidangi teknologi dan informasi

No	Isu	Faktor	Implikasi	Tantangan
	yang tinggi dalam layanan TI.	operasional	informasi yang memengaruhi sudut pandang operasional dan pengendalian Keamanan Informasi	dengan memperhatikan faktor Keamanan Informasi dan juga menyiapkan Infrastruktur yang konsisten menunjang perkembangan kegiatan operasional. Menyelaraskan perubahan fokus layanan dengan tujuan dan sasaran Keamanan Informasi yang sebelumnya berfokus pada layanan.
7	Information Kecukupan, kelengkapan, dan pemenuhan Keamanan Informasi dalam kegiatan operasional internal.	Konsisten	Pengelolaan informasi yang tidak konsisten dapat menghambat pencapaian tujuan SMKI dan keselarasannya dengan tujuan Lembaga	Melakukan pengukuran, pemantauan, dan mengevaluasi kerangka kerja SMKI untuk memastikan konsistensi dalam implementasi SMKI yang ditentukan.
		Jaminan dan privasi informasi pribadi	Tanggung jawab untuk secara berkelanjutan menjamin privasi dan informasi pribadi Pegawai maupun Pengguna dan pihak eksternal lainnya	Serangkaian sistem manajemen yang menjamin pengelolaan informasi secara berkelanjutan dengan memperhatikan risiko Keamanan Informasi khususnya perlindungan privasi dan informasi pribadi, termasuk pengelolaan akses informasi, penyimpanan maupun penanganan informasi
8	Fasilitas Pendukung Pusat Data (Genset, AC, UPS, Access Door,	Keberlangsungan Fasilitas	Terganggunya Ketersediaan fasilitas pendukung untuk menunjang	Menjaga Ketersediaan fasilitas pendukung untuk menunjang keberlangsungan

No	Isu	Faktor	Implikasi	Tantangan
	APAR, CCTV) Kecukupan, kelengkapan, dan pemenuhan fasilitas pendukung dalam kegiatan operasional Pusat Data.	Pendukung Pusat Data	keberlangsungan operasional kegiatan	kegiatan operasional
Konteks Eksternal				
1	Masyarakat Perubahan perilaku masyarakat dan kebutuhan masyarakat, risiko global terhadap pelanggaran data, pengetahuan, dan kesadaran akan Keamanan Informasi.	Perilaku & Kebutuhan Masyarakat dan Harapan	Masyarakat yang tidak puas / tidak terpercaya kepada penyedia layanan.	Kontrol informasi masyarakat selama operasi bisnis yang berinteraksi dengan pihak lain.
2	Contract of Supplier/ Vendor & Partner Kegagalan Pihak Ketiga dalam menyediakan layanan untuk mendukung kegiatan operasional unit kerja yang membidangi teknologi dan informasi, Risiko hubungan Pihak Ketiga dan proses bisnis <i>outsourcing</i> dalam Keamanan Informasi, pengetahuan, dan kesadaran akan Keamanan Informasi. Kegagalan mitra dalam memberikan	Hubungan Pihak Ketiga	Kekurangan kontrol kepada pihak eksternal yang dapat mempengaruhi pihak yang berkepentingan.	Pengendalian pihak eksternal dalam lingkup implementasi SMKI adalah sebuah keharusan. Penerapan pengendalian dan optimalisasi penyusunan perjanjian Kerjasama dengan mempertimbangkan syarat Keamanan Informasi, memastikan ketersediaan proses review Pihak Ketiga secara berkala.

No	Isu	Faktor	Implikasi	Tantangan
	persyaratan kontrak, risiko pembagian informasi dan penutupan dengan mitra bisnis, pengetahuan, dan kesadaran akan Keamanan Informasi. Persyaratan kontraktual untuk mengatasi Keamanan Informasi.			
3	Social & Environment Lingkungan alam dan lingkungan bisnis yang kompetitif, adanya pendorong dan tren sosial dan lingkungan yang berdampak pada tujuan organisasi, politik, status keuangan negara, isu lingkungan, bencana alam, atau ancaman <i>force majeure</i> lainnya.	<i>Remote Working</i>	Tingginya kebutuhan dan adanya transisi pekerjaan secara <i>remote</i>	Ketersediaan infrastruktur maupun sumber daya penunjang <i>remote working</i> harus dipastikan sesuai dan memenuhi kebutuhan kapasitas Pegawai.
		<i>Environment</i>	Pengendalian yang dilakukan dalam setiap aspek penerapan SMKI harus mempertimbangkan dampaknya terhadap lingkungan sekitar.	Penerapan pengendalian yang akan dilakukan akan mempertimbangkan aspek dan dampak terhadap lingkungan sekitar. Selain memenuhi persyaratan ISO 27001 dan diharapkan mampu memenuhi persyaratan regulasi yang berlaku.
4	Technology Masalah perkembangan teknologi, kebutuhan untuk mengadopsi teknologi baru.	Pengembangan dan Peningkatan Teknologi	Pengembangan TIK secara cepat menyebabkan unit kerja yang membidangi teknologi dan informasi harus terus mengadopsi dan menyesuaikan kapasitasnya dengan kondisi perkembangan dari waktu ke waktu. Penggunaan teknologi	Penggunaan perangkat teknologi informasi dan komputer telah menjadi bagian penting bagi unit kerja yang membidangi teknologi dan informasi. Penggunaan perangkat yang tidak terkendali akan menyebabkan potensi risiko bagi unit kerja yang membidangi teknologi dan informasi

No	Isu	Faktor	Implikasi	Tantangan
			baru semakin populer di masyarakat. Jalur komunikasi dapat menggunakan koneksi jaringan komunikasi data di area publik, termasuk di kantor.	sehingga SMKI harus mampu menunjang kontrol penggunaan teknologi.
5	Regulatory Compliance Persyaratan kepatuhan terhadap peraturan yang relevan, perubahan persyaratan peraturan.	Hukum / Legal	Tanggung jawab atas penyelenggaraan kegiatan bisnis yang sesuai dengan hukum/legal yang berlaku serta adanya risiko pelanggaran atas hukum yang dapat berkontribusi konsekuensi tindakan hukum.	Perhatian terhadap ketentuan yang diwajibkan oleh undang-undang dalam setiap pelaksanaan SMKI. Setidaknya undang-undang tersebut merupakan pemenuhan prioritas persyaratan pelaksanaan SMKI di lingkungan DPR RI.
		Perubahan Regulasi	Ketidakmampuan Sekretariat Jenderal DPR RI memenuhi persyaratan regulasi dari waktu ke waktu karena adanya perubahan regulasi	Pelaksanaan reviu kepatuhan secara berkala dan melakukan penilaian mandiri atas pemenuhan regulasi dalam kegiatan bisnis unit kerja yang membidangi teknologi dan informasi.

2. Pihak Berkepentingan, Kebutuhan, Hubungan, Ketergantungan Pihak Berkepentingan, dan Regulasi Terkait Sekretariat Jenderal DPR RI perlu melakukan identifikasi terhadap pihak-pihak terkait yang dapat mempengaruhi implementasi SMKI. Selain itu, Sekretariat Jenderal DPR RI perlu mengidentifikasi ekspektasi Keamanan Informasi dari pihak-pihak terkait tersebut, terutama yang berkaitan dengan Keamanan Informasi. Ekspektasi pihak-pihak terkait yang telah diidentifikasi dan dapat mempengaruhi Keamanan Informasi di Sekretariat Jenderal DPR RI harus dikelola untuk pemenuhannya.

Tabel 2. Pihak Berkepentingan dan Kebutuhannya

No	Para Pihak	INT/EXT	Kebutuhan dan persyaratan
1	<i>Management</i>	INT	Ketersediaan dan alokasi sumber daya, komunikasi, pencapaian tujuan dan sasaran, pelaporan yang efektif dan efisien, kesadaran, kepemimpinan dan komitmen, reputasi dan citra unit kerja yang membidangi teknologi dan informasi.
2	Penyelenggara SMKI	INT	Kecukupan dan kelengkapan kegiatan operasional, penanganan insiden/masalah, pencapaian target operasional, penyelarasan operasional dan tujuan bisnis.
3	Pegawai	INT	Kejelasan dalam hal tugas dan tanggung jawab serta kelangsungan bisnis, kesadaran, citra unit kerja yang membidangi teknologi dan informasi.
4	<i>Supplier/ Vendor</i> <i>Internet provider</i> <i>IT support provider</i> Fasilitas dan peralatan lainnya	EXT	• Kejelasan dan kesesuaian antara kontrak dengan pembayaran. • Kerjasama sesuai dengan persyaratan kontraktual dan mendukung layanan unit kerja yang membidangi teknologi dan informasi dalam kegiatan usaha. • Kejelasan perjanjian komersial dan pemenuhan persyaratan kontraktual • Pemenuhan dan kepastian keamanan data dan

No	Para Pihak	INT/EXT	Kebutuhan dan persyaratan
			informasi. • Akses yang aman ke aset yang relevan yang disediakan oleh Pemasok/<i>Vendor</i> atau unit kerja yang membidangi teknologi dan informasi. • Pemenuhan persyaratan pekerjaan dan dukungan layanan.
5	Regulator	EXT	• Kepatuhan terhadap peraturan yang relevan seperti perlindungan data pribadi, keamanan data dan informasi dan persyaratan lisensi terkait lainnya. • Ketersediaan pelaporan operasional yang diperlukan oleh regulator. • Hubungan dan komunikasi yang baik. • Berpartisipasi dalam inisiatif pemerintah termasuk dalam peningkatan teknologi finansial nasional dan tata kelola.
6	Lingkungan sekitar	EXT	Mendapatkan Informasi terkait operasional Pusat Data.
7	Masyarakat	EXT	• Ketersediaan layanan. • Keamanan Informasi dan Manajemen data termasuk perlindungan privasi. • Penanganan insiden/masalah. • Komunikasi dan Manajemen hubungan masyarakat yang baik. • Jangka waktu pemenuhan layanan. • Reputasi baik dan kepuasan masyarakat.

Tabel 3. Hubungan dan Ketergantungan antara Pihak yang Berkepentingan

No	Kegiatan	Unit Kerja Yang Membidangi Teknologi dan Informasi	Platform / Fasilitas / Teknologi Pendukung	Pihak yang Berkepentingan (Pihak Ketiga)
1	Alokasi Sumber Daya termasuk SDM, Infrastruktur, dan penunjang lainnya	Membuat perencanaan terkait kebutuhan alokasi sumber daya manusia, Infrastruktur TI, dan peralatan penunjang lainnya seperti gedung, peralatan kerja lainnya Melakukan verifikasi dan meninjau alokasi sumber daya yang dilakukan oleh mitra maupun Pihak Ketiga lainnya	Menyediakan fasilitas integrasi platform sesuai dengan kebutuhan bisnis unit kerja yang membidangi teknologi dan informasi serta <i>requirement</i> keamanan yang digunakan dalam proses integrasi <i>platform</i> .	Menyediakan sumber daya manusia penunjang kegiatan penagihan maupun <i>contact center</i> , peralatan dan gedung operasional maupun penunjang lainnya sesuai dengan kebutuhan unit kerja yang membidangi teknologi dan informasi sesuai perjanjian kerjasama seperti jasa jaringan internet, Infrastruktur dan Perangkat Keras maupun Perangkat Lunak.
2	<i>Project Management</i>	Mendefinisikan kebutuhan dan persyaratan <i>project</i> pengembangan aplikasi yang dimiliki oleh unit kerja yang membidangi teknologi dan informasi. Melakukan proses pemantauan dan verifikasi hasil akhir <i>project</i>	Mendukung <i>project</i> integrasi <i>platform</i> termasuk proses pengembangan dan perubahan kebutuhan implementasi produk dan layanan unit kerja yang membidangi teknologi dan informasi di dalam platform yang dimiliki	Mendukung unit kerja yang membidangi teknologi informasi dalam eksekusi <i>project</i> dengan menyediakan kebutuhan <i>project</i> baik dari sisi infrastruktur TI maupun sumber daya kebutuhan <i>project</i> sesuai persyaratan <i>service level</i> dan perjanjian kerjasama
3	Penentuan/ Pendefinisian Kebutuhan	Mendefinisikan keseluruhan kebutuhan sistem/aplikasi dalam pengembangan sistem/aplikasi (proses	Membantu unit kerja yang membidangi teknologi dan informasi untuk mengidentifikasi kebutuhan dalam proses	Menyediakan fasilitas penunjang proses pendefinisian kebutuhan unit kerja yang membidangi

No	Kegiatan	Unit Kerja Yang Membidangi Teknologi dan Informasi	Platform / Fasilitas / Teknologi Pendukung	Pihak yang Berkepentingan (Pihak Ketiga)
	sistem/Aplikasi	bisnis, fitur dan fungsi)	integrasi platform dan produk/layanan unit kerja yang membidangi teknologi dan informasi.	teknologi dan informasi dari sisi Infrastruktur TI dan sumber daya terkait lainnya sesuai dengan perjanjian kerjasama meliputi kebutuhan jaringan Perangkat Lunak, perangkat keras, dan memastikan kesesuaian kapasitas <i>service delivery</i> dengan pemenuhan kebutuhan unit kerja yang membidangi teknologi dan informasi.
4	Pembuatan dokumentasi sistem/ pengembangan	Menyusun dokumentasi pengembangan, meliputi <i>Business Requirement Document, Feasibility Study Documents, Technical Specification Document</i>	Melakukan analisis kecukupan dan membantu unit kerja yang membidangi teknologi dan informasi dalam proses pemenuhan persyaratan dokumentasi pengembangan yang ditentukan untuk proses integrasi platform.	Menyediakan informasi yang dibutuhkan untuk proses pendefinisian kebutuhan layanan memastikan kemampuan layanan yang diberikan dapat menunjang proses pengembangan aplikasi yang dimiliki Sekretariat Jenderal DPR RI.
5	Pengembangan sistem/aplikasi	Melakukan pengembangan sistem/aplikasi sesuai kebutuhan yang didefinisikan	Membantu unit kerja yang membidangi teknologi dan informasi untuk mengakomodir proses pengembangan	Memberikan dukungan layanan infrastruktur TI baik jaringan maupun server selama proses

No	Kegiatan	Unit Kerja Yang Membidangi Teknologi dan Informasi	Platform / Fasilitas / Teknologi Pendukung	Pihak yang Berkepentingan (Pihak Ketiga)
		Menentukan kebutuhan akses selama proses pengembangan sistem/ aplikasi Menentukan kebutuhan penggunaan data dan informasi untuk kebutuhan pengembangan sistem/aplikasi	sistem/Aplikasi dalam hal kebutuhan integrasi platform	pengembangan, membantu proses penanganan permasalahan yang berhubungan dengan proses penyampaian <i>service</i> infrastruktur dan kegiatan operasional jaringan serta menyediakan proses penanganan permasalahan
6	Pengujian sistem/ aplikasi	Menyusun skenario dan melakukan pengujian atas penambahan / penyesuaian sistem/aplikasi Memverifikasi hasil pengembangan sesuai dengan kebutuhan seluruh user	Menunjang kegiatan pengujian integrasi platform dengan kebutuhan pengembangan unit kerja yang membidangi teknologi dan informasi termasuk ikut serta dalam proses pengujian untuk memverifikasi hasil integrasi platform sesuai dengan kebutuhan unit kerja yang membidangi teknologi dan informasi.	Memberikan dukungan layanan infrastruktur TI baik jaringan maupun server selama proses pengembangan, membantu proses penanganan permasalahan yang berhubungan dengan proses penyampaian <i>service</i> infrastruktur dan kegiatan operasional jaringan serta menyediakan proses penanganan permasalahan

No	Kegiatan	Unit Kerja Yang Membidangi Teknologi dan Informasi	Platform / Fasilitas / Teknologi Pendukung	Pihak yang Berkepentingan (Pihak Ketiga)
7	Deployment sistem/aplikasi	Melakukan verifikasi kecukupan hasil pengembangan dan pengujian sistem / aplikasi dan memberikan persetujuan dalam proses deployment	Melakukan verifikasi kebutuhan deployment dan berkoordinasi dalam hal proses deployment kebutuhan yang berhubungan dengan integrasi antar platform	Memberikan dukungan layanan Infrastruktur TI baik jaringan maupun server selama proses pengembangan, membantu proses penanganan permasalahan yang berhubungan dengan proses penyampaian service Infrastruktur dan jaringan kegiatan operasional dan menyediakan proses penanganan permasalahan
8	Pemeliharaan sistem/aplikasi (perubahan/perbaikan)	Melaksanakan proses perubahan sistem/aplikasi termasuk memberikan permohonan perubahan sistem/aplikasi sesuai dengan kebutuhan bisnis dengan berkoordinasi kepada pihak terkait Menerima pelaporan permasalahan pada sistem/aplikasi dan melakukan eskalasi permasalahan	Membantu unit kerja yang membidangi teknologi dan informasi dalam perbaikan atas permasalahan pada sistem/aplikasi maupun kegiatan operasional sesuai dengan laporan yang diterima	Membantu unit kerja yang membidangi teknologi dan informasi dalam perbaikan atas permasalahan pada sistem/aplikasi maupun kegiatan operasional sesuai dengan laporan yang diterima

No	Kegiatan	Unit Kerja Yang Membidangi Teknologi dan Informasi	Platform / Fasilitas / Teknologi Pendukung	Pihak yang Berkepentingan (Pihak Ketiga)
		Memastikan permasalahan yang dilaporkan telah ditangani dan tidak memiliki dampak kejadian berulang	Menerima eskalasi permasalahan dan menyediakan solusi dan penanganan permasalahan untuk cakupan integrasi platform dan kegiatan operasional terkait	Memberikan dukungan layanan infrastruktur TI baik jaringan maupun server selama proses pengembangan, membantu proses penanganan permasalahan yang berhubungan dengan proses penyampaian <i>service</i> infrastruktur dan kegiatan operasional jaringan serta menyediakan proses penanganan permasalahan
9	Akses infrastruktur, pemeliharaan infrastruktur	Menentukan persyaratan infrastruktur dan kebutuhan serta perencanaan kapasitas infrastruktur Menentukan kebutuhan konfigurasi dan pengelolaan akses Memiliki akses portal/dashboard untuk melakukan pemantauan dan penggunaan infrastruktur (OSS & konten web)	Membantu unit kerja yang membidangi teknologi dan informasi dalam menentukan persyaratan konfigurasi Infrastruktur yang dibutuhkan untuk menunjang proses integrasi platform maupun kebutuhan pengembangan sistem/aplikasi unit kerja yang membidangi teknologi dan informasi.	Memberikan dukungan layanan Infrastruktur TI baik jaringan maupun server selama proses pengembangan, membantu proses penanganan permasalahan yang berhubungan dengan proses penyampaian <i>service</i> infrastruktur dan kegiatan operasional jaringan serta menyediakan proses penanganan permasalahan

No	Kegiatan	Unit Kerja Yang Membidangi Teknologi dan Informasi	Platform / Fasilitas / Teknologi Pendukung	Pihak yang Berkepentingan (Pihak Ketiga)
10	Pengamanan sistem/aplikasi dan database	Menentukan persyaratan pengamanan sistem/aplikasi dan Infrastruktur TI terkait	Menunjang proses dan implementasi persyaratan pengamanan sistem/aplikasi unit kerja yang membidangi teknologi dan informasi dalam proses integrasi platform dan melakukan pemenuhan persyaratan pengamanan informasi	Ikut serta membantu unit kerja yang membidangi teknologi dan informasi untuk mengimplementasikan persyaratan pengamanan sistem/aplikasi dan informasi melalui dukungan layanan yang disediakan oleh Pihak Ketiga sesuai dengan persyaratan pengamanan yang ditentukan oleh unit kerja yang membidangi teknologi dan informasi.
11	Pengelolaan operasional dan akses aplikasi operasional	Menentukan kebutuhan akses dan persyaratan akses termasuk <i>user access matrix</i> untuk aplikasi Melakukan review atas hak akses sistem/aplikasi operasional. Akses sesuai dengan <i>User Access Matrix</i>	Berkewajiban untuk menerapkan persyaratan pengamanan akses pada sistem/aplikasi yang terintegrasi dengan platform teknologi informasi di DPR RI Mengakomodir kebutuhan pengembangan sistem/aplikasi Unit kerja yang membidangi Teknologi Informasi di lingkungan DPR RI dalam proses integrasi dengan cakupan penambahan akses integrasi pada platform yang dimiliki	Memastikan persyaratan pengamanan akses dan pengelolaan akses dapat dilakukan dan disiapkan pada layanan yang digunakan oleh Unit kerja yang membidangi Teknologi Informasi di lingkungan DPR RI

Tabel 4. Syarat Regulasi Terkait Penerapan Keamanan Informasi

No	Regulasi	Deskripsi	Persyaratan	Ringkasan Kepatuhan
1	Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016	Undang-undang ini berlaku bagi setiap orang yang melakukan perbuatan hukum terkait Penggunaan Teknologi Informasi dan Transaksi Elektronik.	• Pasal 9 dan 10: Ketentuan Umum • Pasal 11 (2), Pasal 13 (6) • Pasal 15 dan 16: • Penyelenggara Sistem Elektronik • Pasal 17, 19, 21 dan 22: Transaksi Elektronik • Pasal 23-26: Nama Domain, Hak Kekayaan Intelektual, dan Perlindungan Hak Pribadi • Pasal 27, 30, 31, 33, 34: Tindakan yang dilarang • Pasal 38: Penyelesaian Sengketa	• Ketentuan yang diatur dalam regulasi telah disesuaikan dengan perkembangan dan operasional yang dilakukan Perseroan, termasuk pengelolaan nama domain dan pengelolaan HAKI. • unit kerja yang membidangi teknologi dan informasi mengelola sistem elektronik yang digunakan dalam kegiatan operasional tetapi tidak terbatas pada Pengelolaan Data Pengguna dan sistem/Aplikasi di lingkungan DPR RI, yang meliputi: pengawasan, pemantauan, pemutakhiran, pemeliharaan, dan aktivitas lainnya untuk memastikan bahwa Pegawai dan Pihak Ketiga tidak melakukan tindakan dilarang oleh Pegawai atau Pihak Ketiga. dan prosedur SMKI.
2	Undang-undang Nomor 28 Tahun 2014 tentang Hak Cipta	Undang-undang ini dilaksanakan dengan mengedepankan kepentingan nasional dan memperhatikan keseimbangan antara kepentingan Pencipta,	• Pasal 1: Ketentuan Umum • Pasal 4,6, dan 7: Umum • Pasal 52 dan 53: Sarana Pengendalian Teknologi • Pasal 54: Konten Hak Cipta dan Hak Terkait dalam TI dan Komunikasi	• unit kerja yang membidangi teknologi dan informasi berkomitmen untuk melindungi Hak atas Kekayaan Intelektual dalam semua aktivitas operasional tetapi tidak terbatas pada Aplikasi teknologi informasi di lingkungan DPR RI. • unit kerja yang membidangi teknologi dan informasi menerapkan ketentuan terkait Hak

No	Regulasi	Deskripsi	Persyaratan	Ringkasan Kepatuhan
		Pemegang Hak Cipta, atau Pemilik Hak Terkait, dan masyarakat serta memperhatikan ketentuan dalam perjanjian internasional di bidang Hak Cipta dan Hak Terkait	• Pasal 64: Pendaftaran Ciptaan dan Produk Hak Terkait • Pasal 66 - 73: Tata Cara Pendaftaran	Kekayaan Intelektual dalam dokumen Standar Keamanan Informasi dan dokumen terkait. • unit kerja yang membidangi teknologi dan informasi juga memuat ketentuan terkait Hak Kekayaan Intelektual dalam rangka pembangunan dan atau pengembangan layanan teknologi informasi yang diselenggarakan oleh unit kerja pengelola teknologi informasi, serta ketentuan penggunaan sistem/Aplikasi di lingkungan DPR RI, Kontrak Pegawai, Perjanjian Kerja Sama dengan Pihak Ketiga, serta ketentuan penggunaan sistem/Aplikasi teknologi informasi.
3	Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Ketentuan Penyelenggaraan Sistem dan Transaksi Elektronik	PP baru ini mengatur pengoperasian sistem elektronik dan transaksi secara umum	• Pasal 1: Ketentuan Umum • Pasal 2: Ketentuan Penyelenggara Sistem Elektronik Lingkup Publik • Pasal 4: Persyaratan minimum untuk mengoperasikan sistem elektronik • Pasal 5: ketentuan Penyelenggara sistem elektronik • Pasal 6: Perangkat Keras • Pasal 7 & 8: Perangkat Lunak	• Sekretariat Jenderal DPR RI dimasukkan ke dalam PSE sektor swasta yang dikategorikan dalam PP No. 71 (Sistem Operasi Elektronik oleh Orang, Bisnis, dan Masyarakat) untuk Aplikasi di lingkungan DPR RI • Sekretariat Jenderal DPR RI melalui unit kerja yang membidangi teknologi dan informasi telah memilih ruang lingkup SMKI dan harus mengikuti proses sertifikasi termasuk pemilihan software dan hardware untuk dijadikan standar sebagai PSE. • unit kerja yang membidangi teknologi dan informasi juga telah melakukan seleksi dalam

No	Regulasi	Deskripsi	Persyaratan	Ringkasan Kepatuhan
			• Pasal 8 dan 9 terkait dengan Penyedia Layanan dan Kode Sumber • Pasal 10: Ahli • Pasal 12, 13, 14, 15, 16: Tata Kelola Sistem Elektronik • Pasal 14: Kewajiban Penyelenggara Sistem Elektronik dan pemrosesan Data Pribadi • Pasal 15, 16, 17, dan 18: Penghapusan Informasi Elektronik • Pasal 18 - 28: Menjaga Penyelenggaraan Sistem Elektronik • Pasal 20 & 21: rencana kelanjutan kegiatan untuk mengatasi gangguan • Pasal 29: wajib menyampaikan informasi kepada Pengguna Sistem Elektronik • Pasal 41: Persyaratan Penyelenggaraan Transaksi	pemilihan penyedia perangkat dengan mempertimbangkan keandalan, jaminan produk, dan ketersediaan suku cadang jika diperlukan. • Perjanjian kerjasama yang diatur oleh unit kerja yang membidangi teknologi dan informasi meliputi: a. Manajemen kode sumber yang diberikan kepada unit kerja yang membidangi teknologi dan informasi. b. Ketersediaan SLA yang akan diberikan kepada Pengguna. c. Perjanjian Larangan pengungkapan informasi rahasia • Adanya daftar Risiko terkait dengan Manajemen risiko dan pemilihan tujuan pengendalian Keamanan Informasi. • Terdapat dokumen Persekjen, SOP, dan Juknis terkait implementasi rencana SMKI dan implementasinya, baik dari Manajemen Keamanan Informasi, TI, Manajemen aset, perlindungan informasi & arsip, hingga Manajemen SDM, yang berlaku untuk seluruh Pegawai, unit bisnis terkait dan vendor Pihak Ketiga.

No	Regulasi	Deskripsi	Persyaratan	Ringkasan Kepatuhan
			Elektronik • Pasal 52, 53, dan 54: Pelaksanaan Sertifikasi Elektronik • Paragraf 2 dan 3: Tanda Tangan Elektronik • Paragraf 4: Segel Elektronik • Paragraf 5: Penanda Waktu Elektronik • Paragraf 7: Otentikasi Situs Web • Paragraf 8: Pengawetan Tanda Tangan Elektronik dan / atau Segel Elektronik	• Perlindungan Informasi Identifikasi Pribadi, Hak Cipta Intelektual, Penggunaan Kriptografi, Proses Otentikasi dan Otorisasi yang tepat, Kontrol Akses, Sinkronisasi Waktu, Pelestarian Tanda Tangan Elektronik dan / atau Segel Elektronik harus, dipelihara, dan diterapkan dengan cara yang sesuai dalam Kerangka Keamanan Informasi Sekretariat Jenderal DPR RI. • unit kerja yang membidangi teknologi dan informasi telah menetapkan tujuan ISMS termasuk untuk menjaga operasional terkait dengan Keamanan Informasi dan fasilitas pemrosesan informasinya, sebagai komitmen luas unit kerja yang membidangi teknologi dan informasi dan untuk Lingkup ISMS dalam layanan transaksi Aplikasi Teknologi Informasi. • unit kerja yang membidangi teknologi dan informasi harus menentukan dan mengalokasikan sumber daya yang memadai untuk membangun, menerapkan dan memelihara SMKTI. • Sekretariat Jenderal DPR RI telah membentuk Penyelenggara SMKTI yang bertanggung jawab

No	Regulasi	Deskripsi	Persyaratan	Ringkasan Kebutuhan
				untuk merencanakan, mengoperasikan, dan mengevaluasi Penyelenggara SMK. Kompetensi khusus tentang SMK harus didefinisikan untuk memastikan keahlian yang memadai dalam melaksanakan Kerangka SMK. • Sekretariat Jenderal DPR RI telah membentuk Penyelenggara SMK yang bertanggung jawab untuk merencanakan, mengoperasikan, dan mengevaluasi Penyelenggara SMK. • Kompetensi khusus tentang SMK harus didefinisikan untuk memastikan keahlian yang memadai dalam melaksanakan Kerangka SMK. Tenaga ahli yang akan dipekerjakan oleh Sekretariat Jenderal DPR RI adalah warga negara Indonesia termasuk para vendor yang bekerja sama. • Sekretariat Jenderal DPR RI menerapkan ketentuan terkait pelaksanaan audit internal dan tinjauan Manajemen sebagai alat untuk melakukan penilaian independen terhadap efektivitas penerapan standar ISO 27001, ketentuan terkait pelaksanaan audit internal dan tinjauan Manajemen yang tertuang dalam SOP Audit Internal dan Tinjauan Manajemen.

No	Regulasi	Deskripsi	Persyaratan	Ringkasan Kepatuhan
				- Sekretariat Jenderal DPR RI menerapkan SMKTI untuk melindungi data pribadi dalam sistem elektronik termasuk proses berikut: - akuisisi dan pengumpulan; - memproses dan menganalisis; - penyimpanan; - penampilan, pengumuman, penyampaian, penyebaran, dan / atau pembukaan akses; dan - pemusnahan. - Sekretariat Jenderal DPR RI juga memiliki ketentuan BCM diantaranya untuk Business Continuity Plan Disaster Recovery Plan yang digunakan sebagai acuan dalam memastikan keberlangsungan operasional unit kerja yang membidangi teknologi dan informasi pada saat terjadi gangguan / bencana.
4	Peraturan Menteri Komunikasi dan Informasi Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi	Peraturan Menteri ini mengatur penyelenggaraan SMKTI oleh Penyelenggara Sistem Elektronik untuk Pelayanan Publik berdasarkan asas Risiko.	- Pasal 3: Ketentuan Umum - Pasal 7 - 9: Standar SMKTI - Pasal 10: Pengoperasian Sistem Elektronik - Pasal 11: Sertifikat SMKTI - Pasal 12-15: Badan Sertifikasi - Pasal 16 dan 17: Penerbitan Sertifikat	- unit kerja yang membidangi teknologi dan informasi menerapkan Manajemen Keamanan Informasi sesuai dengan standar dan peraturan yang relevan serta menerapkan kontrol yang diatur dalam persyaratan ISO / IEC 27001. - Tenaga ahli Keamanan Informasi yang akan dipekerjakan oleh Sekretariat Jenderal DPR RI

No	Regulasi	Deskripsi	Persyaratan	Ringkasan Kepatuhan
			• Pasal 18: Pelaporan Hasil Sertifikasi • Pasal 19 dan 20: Pencabutan Sertifikasi • Pasal 21 dan 22: Penilaian Diri • Pasal 24: Pengawasan • Pasal 25 - 27: Sanksi	adalah warga negara Indonesia termasuk para vendor yang bekerja sama. • Penggunaan lembaga sertifikasi yang terakreditasi dituangkan dalam perjanjian kerjasama yang menjelaskan ruang lingkup pekerjaan, hak dan kewajiban serta besaran biaya sertifikasi yang harus dibayarkan. Perjanjian kerja sama juga mengatur ketentuan khusus lainnya sebagai acuan dalam melaksanakan proses sertifikasi. • Sekretariat Jenderal DPR RI menerapkan ketentuan terkait pelaksanaan audit internal dan tinjauan Manajemen sebagai alat untuk melakukan penilaian independen terhadap efektivitas penerapan standar ISO 27001, ketentuan terkait pelaksanaan audit internal dan tinjauan Manajemen yang tertuang dalam SOP Audit Internal dan Tinjauan Manajemen. • Penerapan SMKI berdasarkan Standar SNI & ISO / IEC 27001 (Pasal 7-9). • Badan sertifikasi terakreditasi (Pasal 12 - 15) • Sekretariat Jenderal DPR RI menerapkan SMKI untuk melindungi data pribadi dalam sistem elektronik melalui sistem pembayaran digital termasuk proses berikut:
5	Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang	Ketentuan yang mengatur tentang Perlindungan Data Pribadi dalam Sistem	• Pasal 3 - 6: Perlindungan data pribadi dalam sistem elektronik • Pasal 7 - 11: Akuisisi dan	

No	Regulasi	Deskripsi	Persyaratan	Ringkasan Kepatuhan
	Perlindungan Data Pribadi dalam Sistem Elektronik	Elektronik dilakukan antara lain: a. akuisisi dan pengumpulan; b. memproses dan menganalisis; c. penyimpanan; d. penampilan, pengumuman, penyampaian, dan / atau pembukaan akses; dan e. pemusnahan.	Pengumpulan Data Pribadi • Pasal 12 - 14: Manajemen dan Analisis Data Pribadi • Pasal 15-20: Penyimpanan Data Pribadi • Pasal 21 - 24: Penampilan, Pengumuman, Transmisi, Penyebaran, dan / atau Pembukaan Akses ke Data Pribadi • Pasal 25: Penghancuran Data Pribadi • Pasal 26: Kepemilikan Data Pribadi • Pasal 27: Kewajiban Pengguna • Pasal 28: Kewajiban Penyelenggaraan Sistem Elektronik	a. akuisisi dan pengumpulan. b. memproses dan menganalisis; c. penyimpanan; d. penampilan, pengumuman, penyampaian, penyebaran, dan / atau pembukaan akses; dan e. pemusnahan. • Terdapat Persekjen, SOP dan Juknis yang mengatur Data Pribadi, termasuk data lainnya, dengan membagi kategori data tersebut menjadi rahasia, internal dan publik. • Sistem elektronik yang digunakan unit kerja yang membidangi teknologi dan informasi telah mempertimbangkan: a. memiliki kemampuan interoperabilitas dan kompatibilitas; dan b. menggunakan Perangkat Lunak (<i>software</i>) yang legal. • Data pribadi milik masyarakat dan Pengguna akhir sistem/Aplikasi unit kerja yang membidangi teknologi dan informasi disimpan dalam database di Server yang dilengkapi dengan parameter dan persyaratan keamanan. • Sekretariat Jenderal DPR RI juga memiliki ketentuan BCM diantaranya untuk Business

No	Regulasi	Deskripsi	Persyaratan	Ringkasan Kepatuhan
				Continuity Plan Disaster Recovery Plan yang digunakan sebagai acuan dalam memastikan keberlangsungan operasional unit kerja yang membidangi teknologi dan informasi pada saat terjadi gangguan / bencana. • Perlindungan data pribadi dalam sistem elektronik, termasuk proses pengumpulan, analisis, penyimpanan, penyajian, pembuangan (Pasal 3) • Sistem elektronik untuk menyimpan pengumpulan data pribadi (Pasal 11) • Kebijakan penyimpanan dan penyimpanan data pribadi (Pasal 15)
6	SNI ISO 27001: 2022 SMKI	Standar ini menetapkan persyaratan untuk menetapkan, menerapkan, memelihara, dan terus meningkatkan SMKI dalam konteks Standar Internasional ini juga mencakup persyaratan untuk penilaian dan perlakuan risiko	Pasal 1; Lingkup penerapan standar Pasal 2; Referensi Pasal 3; Istilah dan definisi dalam ISO / IEC 27000 Pasal 4; Hubungan organisasi dan pemangku kepentingan Pasal 5; Kepemimpinan Keamanan Informasi dan dukungan tingkat tinggi untuk kebijakan Pasal 6; Perencanaan SMKI;	Sekretariat Jenderal DPR RI harus menerapkan, mengoperasikan, memelihara, dan meningkatkan kerangka kerja SMKI sesuai ISO 27001: 2022 dengan mempertimbangkan: a. Wajib: • Konteks Organisasi • Kepemimpinan • Perencanaan • Pengesahan • Operasional • Evaluasi kinerja • Peningkatan

No	Regulasi	Deskripsi	Persyaratan	Ringkasan Keputusan
		Keamanan Informasi yang disesuaikan dengan kebutuhan organisasi. Persyaratan yang ditetapkan dalam Standar Internasional ini bersifat umum dan dimaksudkan untuk diterapkan pada semua organisasi, terlepas dari jenis, ukuran, atau sifatnya. Persyaratan apa pun yang ditentukan dalam Klausul 4 hingga 10 tidak boleh dikecualikan jika organisasi menyatakan kesesuaian dengan Standar ini	perkiraan risiko; pengendalian risiko Pasal 7; Mendukung SMKI Pasal 8; Menjadikan SMKI operasional Pasal 9; Tinjau kinerja sistem Pasal 10; Tindakan perbaikan	b. Mencakup: • Persekjen SMKI dan Surat Keputusan Junkis SMKI • Manajemen Keamanan Informasi • Keamanan sumber daya manusia • Manajemen aset • Kontrol akses • Kriptografi • Keamanan fisik dan lingkungan • Keamanan operasional • Keamanan jaringan • Pengadaan, pengembangan dan pemeliharaan sistem • Hubungan dengan pemasok • Manajemen insiden Keamanan Informasi • Aspek Keamanan Informasi di BCM • Kepatuhan
7	UU Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi	Peraturan ini menyatakan penerapan data perindungan pribadi terkait dengan penerpaan teknologi informasi	• Bab 3: Jenis Data Pribadi • Bab 4 : Hak Subjek Data Pribadi • Bab 5 : Pemrosesan Data Pribadi • Bab 6 : Kewajiban Pengendali	Sudah adanya ketentuan pada Persekjen SMKI, Surat Keputusan Junkis SMKI terkait dengan ketentuan kontrol yang harus diterapkan dalam menjaga perlindungan data pribadi.

No	Regulasi	Deskripsi	Persyaratan	Ringkasan Kepatuhan
			Data Pribadi dan Prosesor Data Pribadi Dalam Pemrosesan Data Pribadi - Bab 7 : Transfer Data Pribadi - Bab 8 : Sanksi Administratif	
8	Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik	Peraturan ini menyatakan penerapan Keamanan Informasi pada sistem pemerintahan berbasis elektronik	- Bab 2 : Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik - Bab 3 : Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik	Sudah adanya ketentuan pada Persekjen SMKI, Juknis SMKI terkait dengan ketentuan Pedoman dan standar teknis yang harus diterapkan dalam menjaga perlindungan data pribadi.

3. Kewajiban Sekretaris Jenderal dalam SMKI

Sekretaris Jenderal DPR RI wajib memastikan perlindungan informasi dalam melaksanakan tugas pokok dan fungsi Sekretariat Jenderal DPR RI melalui kegiatan menetapkan, menerapkan, memelihara, dan terus meningkatkan SMKI sesuai standar.

Sekretaris Jenderal DPR RI mengarahkan semua pegawai menerapkan dan mematuhi persyaratan yang dalam SMKI baik berupa kebijakan, standar, maupun prosedur.

D. Kepemimpinan dan Komitmen

Dalam melaksanakan pengelolaan SMKI, Sekretaris Jenderal berkomitmen untuk:

- a. menetapkan dan menjalankan kebijakan, standar, dan prosedur Keamanan Informasi DPR RI.
- b. menetapkan dan menjalankan struktur organisasi formal lengkap dengan tugas dan tanggung jawabnya untuk mengelola SMKI.
- c. menetapkan dan menjalankan proses formal dan berkesinambungan untuk mengelola proses Manajemen risiko untuk memastikan pengendalian dari risiko Keamanan Informasi yang relevan dan realistis.
- d. memantau dan meninjau operasional SMKI melalui peninjauan SMKI setiap tahun sekali.
- e. melakukan audit internal SMKI paling sedikit setiap tahun sekali.
- f. melakukan tinjauan Manajemen (*management review*) SMKI paling sedikit setiap tahun sekali.
- g. menetapkan dan mengimplementasikan tindakan peningkatan secara berkesinambungan.
- h. menyediakan seluruh sumber daya yang dibutuhkan untuk membentuk, mengimplementasikan, memelihara dan meningkatkan secara berkesinambungan SMKI.

E. Perencanaan

Pencapaian sasaran SMKI DPR RI menjadi tanggung jawab:

1. seluruh pihak yang terlibat dan masuk ke dalam ruang lingkup implementasi SMKI, dan
2. seluruh pihak yang berkepentingan terhadap SMKI DPR RI.

Pencapaian sasaran SMKI DPR RI diukur setiap tahun oleh *person in charge* (PIC) berdasarkan target dari sasaran yang ditetapkan dan realisasinya sesuai dengan pemetaan sasaran SMKI untuk kemudian dianalisis hal-hal yang menyebabkan tercapai atau tidak tercapainya sasaran-sasaran tersebut. Evaluasi dan pengukuran sasaran SMKI tersebut merupakan penerjemahan isu yang ada di Klausul ISO 27001. Sasaran SMKI sebagaimana dimaksud pada tercantum dalam tabel berikut ini.

Tabel 5. SASARAN SMKI

No	Sasaran	Indikator Pencapaian	Rencana Kerja dan Pengendalian	Sumber Daya	Kontrol dan Check Point	PIC
1	Kebocoran Keamanan Informasi	Tidak ada kebocoran	a. Manajemen User & Password dan hak akses data center b. Penerapan NDA c. Pengendalian IT h/w; s/w serta jaringan d. "Clear desk" policy	SOP	kejadian Kebocoran Keamanan Informasi	a. <i>Information Security Manager</i> b. Koordinator Manajemen Risiko dan Keamanan Sistem Informasi
2	Ketersediaan Fasilitas Pendukung Pusat Data (Genset, AC, UPS, Access Door, APAR, CCTV) untuk kelancaran pelayanan	SLA Data Center	a. Pelaksanaan monitoring ketersediaan fasilitas Pusat Data b. Pelaksanaan pemeliharaan secara berkala pada fasilitas Pusat Data	a. Penyelenggara SMKI b. Laporan hasil monitoring ketersediaan fasilitas Pusat Data c. Laporan hasil pemeliharaan fasilitas Pusat Data secara berkala	Seluruh ketidaksesuaian yang teridentifikasi telah ditindaklanjuti dan diperbaiki	Koordinator Manajemen Aset, Pemasok dan Keamanan Fisik
3	Persekitaran, Prosedur, Juknis, dan Dokumentasi	Seluruh Pegawai mendapatkan	Sosialisasi SMKI	SOP	Bukti Sosialisasi	a. <i>Information Security Manager</i>

No	Sasaran	Indikator Pencapaian	Rencana Kerja dan Pengendalian	Sumber Daya	Kontrol dan Check Point	PIC
		sosialisasi				b. Koordinator Manajemen Risiko dan Keamanan Sistem Informasi
4	Sumber Manusia Daya	Rekrutmen sesuai persyaratan	a. <i>Screening</i> Pegawai b. SOP Rekrutmen dan Terminasi	SOP & Regulasi unit kerja membidangi kepegawaian	Bukti Rekrutmen dan terminasi	Koordinator Manajemen Sumber Daya Manusia
5	Pengelolaan Risiko yang optimal	Realisasi Mitigasi Risiko dari Risk Register	a. Wawancara dan berkorelasi dengan pemilik risiko dan aset dan fungsi Manajemen risiko b. Meninjau proses penilaian risiko yang didokumentasikan c. Mendokumentasikan hasil pemantauan risiko dan mengidentifikasi status risk treatment plan	a. SOP Manajemen Risiko TI b. Dokumen Risk Register	Semua aset fasilitas pemrosesan informasi dan informasi dinilai risiko dan rencana perawatan risiko telah dipertahankan dan diimplementasikan dengan tepat	Koordinator Manajemen Risiko dan Keamanan Sistem Informasi

No	Sasaran	Indikator Pencapaian	Rencana Kerja dan Pengendalian	Sumber Daya	Kontrol dan Check Point	PIC
6	Pengujian <i>Disaster Recovery Plan</i>	Pelaksanaan pengujian <i>Disaster Recovery Plan</i>	a. Membuat scenario pengujian <i>Disaster Recovery Plan</i> b. Melakukan pengujian <i>Disaster Recovery Plan</i> Melakukan evaluasi hasil pengujian <i>Disaster Recovery Plan</i>	a. SK Petunjuk <i>Business Continuity Plan</i> Dokumentasi pengujian <i>Disaster Recovery Plan</i>	Memastikan pengujian <i>Disaster Recovery Plan</i> dilakukan sesuai dengan SK Petunjuk <i>Teknis Business Continuity Plan</i>	<i>Information Security Manager</i>
7	Pemantauan dan pengawasan (audit SMKI) yang berkelanjutan	Seluruh Jumlah area dan kriteria ISO 27001:2022 yang telah dilakukan audit (audit program)	a. Pelaksanaan audit setiap tahun b. Review audit program dan audit plan Perbandingan area dan kriteria SMKI yang di audit setiap tahun	a. Tim Auditor SMKI b. Audit Program c. Audit Plan Audit Report	Semua area dan persyaratan SMKI telah dilakukan audit setiap tahun	a. <i>Information Security Manager</i> b. <i>CISO</i> Manajemen Puncak

F. Dukungan

Sekretariat Jenderal DPR RI dalam implementasi, pemeliharaan, dan peninjauan SMKI, menyediakan sumber daya meliputi anggaran, peralatan, sumber daya manusia, dan sumber daya lainnya yang mungkin diperlukan untuk kinerja SMKI yang efisien. Dalam hal penyediaan sumber daya manusia, Sekretariat Jenderal DPR RI harus menyediakan sumber daya manusia yang memiliki kompetensi dalam pengelolaan SMKI. Sekretariat Jenderal DPR RI wajib menyediakan peningkatan keterampilan/pengetahuan pengelolaan SMKI dalam hal terdapat sumber daya manusia yang belum memenuhi kompetensi pengelolaan SMKI.

Sekretariat Jenderal DPR RI menetapkan komunikasi terkait penerapan SMKI kepada pemangku kepentingan sesuai dengan Matriks komunikasi.

G. Komunikasi Penerapan SMKI

Penerapan SMKI dikomunikasikan kepada pemangku kepentingan sesuai dengan Matriks komunikasi. Matriks komunikasi sebagaimana dimaksud tercantum dalam Tabel 8.

Tabel 8. MATRIKS KOMUNIKASI PENERAPAN SMK

No	Agenda	Periode	Pihak yang dikomunikasikan	Metode komunikasi	Item yang dikomunikasikan	Tanggung jawab
1	Persejken Keamanan Informasi, prosedur dan Juknis	Tahunan / sesuai kebutuhan	- Pegawai - Unit bisnis/departemen Pihak Ketiga	- Email - Dokumentasi - Dokumen Repository/ Shar ePoint - Rapat, sosialisasi - Media komunikasi yang relevan	- Persyaratan Keamanan Informasi - Dokumen SMK - Update tentang persyaratan Keamanan Informasi Sistem Informasi dan kebijakan SMK, standar, dan proses bisnis. - Tujuan SMK - Isu internal & eksternal yang relevan - Persyaratan regulasi	- Koordinator Manajemen Risiko dan Keamanan Sistem Informasi - Koordinator Manajemen Aset, Pemasok dan Keamanan Fisik
2	Rapat Manajemen Strategis / Rapat Kepatuhan Keamanan	Kuartal/ sesuai kebutuhan	- Manajemen/perwakilan Manajemen - Engineering Team/ Development Team - Tech. operation - Departemen terkait	- Rapat - konferensi	- Tinjauan Strategis Keamanan Informasi - Masalah Keamanan Informasi (Sumber Daya, Masalah, Rencana, status Rencana Tindakan, dll.) - Laporan Keamanan Informasi - Masalah/insiden Manajemen Risiko & kepatuhan - Ringkasan rekomendasi - Penetration Testing Follow Up - Kapasitas & pemanfaatan - Pengembangan produk	Information Security Manager

No	Agenda	Periode	Pihak yang dikomunikasikan	Metode komunikasi	Item yang dikomunikasikan	Tanggung jawab
3	Penilaian dan pengawasan risiko Keamanan Informasi	- Per Semester/ minimal 1 tahun - Sesuai kebutuhan untuk urusan pengembangan proyek/produk	- Penyelenggara SMKI - Departemen masing-masing - Pegawai	- Email - Rapat Internal - Media/alat komunikasi - Risk Register dan Risk Treatment Plan	a. Penilaian risiko Keamanan Informasi termasuk risiko aset, ancaman, & kerentanan b. Tingkat risiko c. Status rencana perlakuan risiko d. Hasil pengawasan risiko e. Penilaian risiko proyek	Koordinator Manajemen Risiko dan Keamanan Sistem Informasi
4	Program kepedulian keamanan	Setidaknya setiap tahun atau secara teratur sesuai rencana	- Manajemen/perwakilan Manajemen - Pegawai - Stakeholder yang relevan (jika ada)	a. Presentasi b. Email c. Video material d. Kampanye keamanan melalui wallpaper desktop e. Tempat Penyimpanan Intranet / SharePoint / Dokumen f. Media/alat komunikasi yang relevan	a. Persejken Keamanan Informasi dan prosedur standar b. Kesadaran Keamanan Informasi c. Pengetahuan tentang Keamanan Informasi d. Pelatihan Kompetensi e. Pembaruan / pengingat rutin tentang Keamanan Informasi f. Kepatuhan terhadap kode etik g. Aturan Sekretariat Jenderal DPR RI h. Praktik terbaik untuk Keamanan Informasi i. Ancaman dan kerentanan keamanan baru dan/atau yang sedang berlangsung j. Masalah Keamanan Informasi	a. Koordinator Manajemen Risiko dan Keamanan Sistem Informasi b. Koordinator Manajemen Sumber Daya Manusia

No	Agenda	Periode	Pihak yang dikomunikasikan	Metode komunikasi	Item yang dikomunikasikan	Tanggung jawab
5	Induksi Pegawai	Sesuai kebutuhan sesuai proses rekrutmen	- Pegawai baru - PKWT/magang - Agen operasional (Pihak Ketiga)	a. Dokumen & bahan induksi b. presentasi c. pertemuan d. kontrak kerja	a. Profil Sekretariat Jenderal DPR RI b. Pentingnya Keamanan Informasi c. Program kepedulian Keamanan Informasi d. Kebijakan SMKI, standar, proses bisnis, dan persyaratan yang terkait.	Koordinator Manajemen Sumber Daya Manusia
6	Inisiasi proyek	Berbasis proyek / selama proyek	- Pemasok/vendor Pihak Ketiga - Partner - Tim proyek	a. Dokumen proyek b. Rapat c. Email d. Kontrak/NDA	a. Pentingnya Keamanan Informasi dalam menjalankan proyek b. SMKI unit kerja yang membidangi teknologi informasi c. Sekretariat Jenderal DPR RI dan persyaratan Manajemen proyek	a. Koordinator Manajemen Aset, Pemasok dan Keamanan Fisik b. Unit terkait (Pengguna jasa/barang) c. Koordinator Manajemen Risiko dan Keamanan Sistem Informasi
7	Manajemen / Rencana Kontinuitas Bisnis dan Pusat Pemulihan Bencana	Tahunan/sesuai kebutuhan	- Manajemen - Perwakilan Manajemen Departemen terkait - Pegawai	a. BCM/CP and DRP Documents b. BCP/DRP Test Scenarios/Case c. BCP/DRP Testing Report	a. Persyaratan dalam Business Continuity Plan (BCM) / Disaster Recovery Plan (DRP) b. Risiko Keamanan Informasi dan kelangsungan operasional c. Efektivitas hasil Pengujian BCP / DRP	a. Koordinator Manajemen Risiko dan Keamanan Sistem Informasi b. Koordinator Manajemen Aset, Pemasok dan Keamanan Fisik

No	Agenda	Periode	Pihak yang dikomunikasikan	Metode komunikasi	Item yang dikomunikasikan	Tanggung jawab
						c. Koordinator Manajemen Insiden Keamanan Informasi dan Kelangsungan Bisnis
8	Kinerja Pegawai	Sesuai ketentuan pengelolaan sumber daya manusia (Kebijakan HR/People Experiences)	- Pegawai - Unit bisnis	a. Rapat b. Daftar Periksa Kinerja c. Pelatihan	Evaluasi kinerja & prestasi Pegawai	Koordinator Manajemen Sumber Daya Manusia
9	Review dan evaluasi kinerja Pihak Ketiga / vendor	Tahunan / sesuai kebutuhan	Unit bisnis (Pengguna)	a. Email b. Laporan & dokumentasi evaluasi kinerja Pihak Ketiga / Vendor	a. SLA review b. Kinerja Pihak Ketiga / Vendor dan pemenuhan persyaratan c. Perjanjian kontrak d. Aspek komersial e. Kelanjutan status dan rekomendasi Pihak Ketiga / vendor	Koordinator Manajemen Aset, Pemasok dan Keamanan Fisik
10	Masalah Operasional & Keamanan Informasi / eskalasi masalah	Kapan dan kapan acara tersebut berlangsung	- Masyarakat - Unit bisnis/Pegawai - Vendor Pihak Ketiga	a. Laporan insiden / masalah & alat eskalasi b. Lesson Learned database	a. Insiden/masalah layanan b. Masalah Infrastruktur TI c. Masalah keamanan fisik d. Masalah Keamanan Informasi e. Resolusi masalah / insiden f. Laporan Solusi	a. Koordinator Manajemen Risiko dan Keamanan Sistem Informasi

No	Agenda	Periode	Pihak yang dikomunikasikan	Metode komunikasi	Item yang dikomunikasikan	Tanggung jawab
			• Merchants • Regulasi • Partner bisnis	c. Email d. Call Center e. Telepon f. Media/komunikasi Perangkat Lunak	g. Pemberitahuan insiden / peristiwa Keamanan Informasi h. Deskripsi insiden / peristiwa Keamanan Informasi i. Hasil investigasi j. Respon terhadap insiden / kejadian (tindakan yang telah dilakukan) k. Resolusi & status Pemulihan	b. Koordinator Manajemen Insiden Keamanan Informasi dan Kelangsungan Bisnis c. Koordinator Keamanan fisik
11	Internal Audit/SMKI Surveillances	Tahunan/sesuai kebutuhan	• Unit bisnis • Penyelenggara SMKI	a. Dokumentasi Persiapan Audit & bukti b. Eksekusi Audit Laporan audit	a. Kecukupan dan kelengkapan persyaratan SMKI b. Ketidaksesuaian c. Temuan dan rekomendasi d. Rencana remediasi	a. CISO b. Information Security Manager c. Koordinator Manajemen Audit Internal
12	Tinjauan Manajemen	Tahunan/sesuai kebutuhan	• Unit bisnis • Penyelenggara SMKI	a. Laporan audit b. Tinjauan Manajemen c. Minutes of meetings	a. Temuan Audit / Ketidaksesuaian b. Akar Penyebab dan potensi dampak Ketidaksesuaian c. Umpan balik dari pihak yang berkepentingan d. Masalah Internal dan Eksternal e. Pencapaian tujuan Keamanan Informasi dan hasil pemantauan f. Tindakan Korektif dan Tindakan Pencegahan g. Peningkatan SMKI	a. CISO b. Information Security Manager c. Koordinator Manajemen Audit Internal

No	Agenda	Periode	Pihak yang dikomunikasikan	Metode komunikasi	Item yang dikomunikasikan	Tanggung jawab
13	Tindakan Korektif & Pencegahan Tindak Lanjut & Penutupan	Sesuai rencana dalam audit internal dan hasil tinjauan Manajemen	- Unit bisnis - Penyelenggara SMKI	a. Laporan Audit & Dokumentasi Tindakan Korektif / Pencegahan b. Pemberitahuan Audit c. Email d. Laporan Tindak Lanjut & Penutupan	a. Status Tindakan Korektif dan Tindakan Pencegahan b. Bukti implementasi c. Laporan penutupan	a. CISO b. Information Security Manager c. Koordinator Manajemen Audit Internal
14	Tinjauan kerangka SMKI	Tahunan/sesuai kebutuhan	a. Perwakilan Manajemen b. Penyelenggara SMKI	a. Email b. Rapat/konferensi c. Dokumen d. Sosialisasi	a. Perubahan kerangka SMKI termasuk kebijakan, standar, dan tinjauan proses bisnis yang relevan. b. Pemantauan dan evaluasi SMKI c. Tujuan SMKI d. Keamanan Informasi lainnya yang bersangkutan	Koordinator Manajemen Risiko dan Keamanan Sistem Informasi
15	Laporan regulasi (Kominfo & BSSN)	Seperti yang dipersyaratkan oleh peraturan	a. Perwakilan Manajemen b. Penyelenggara SMKI	a. Workshop b. Pelatihan c. Rapat	a. Daftar Periksa Tinjauan Kepatuhan Pengembangan Produk b. Sosialisasi Persyaratan Peraturan c. Laporan regulasi	Koordinator Manajemen Risiko dan Keamanan Sistem Informasi

H. Tindakan Mengatasi Risiko, Peluang, dan Perubahan

Sekretariat Jenderal DPR RI melakukan penilaian risiko paling sedikit 1 (satu) tahun sekali. Penilaian risiko berisi :

- a. identifikasi risiko Keamanan Informasi; dan
- b. identifikasi segala perubahan yang terjadi terkait dengan Keamanan Informasi sesuai dengan peraturan perundang-undangan.

Adapun yang melakukan penilaian risiko dan menyimpan hasil penilaian risiko SMKI adalah Koordinator Manajemen Risiko dan Keamanan Sistem Informasi. Dalam hal terdapat perubahan signifikan, penilaian risiko dilaksanakan dengan mempertimbangkan kriteria yang ditetapkan. Sekretariat Jenderal DPR RI mengontrol perubahan yang direncanakan dan meninjau konsekuensi dari perubahan yang tidak diinginkan, mengambil tindakan untuk mengurangi dampak apapun sebagaimana diperlukan.

I. Informasi Terdokumentasi

Sekretariat Jenderal DPR RI mengelola dan menerapkan dokumentasi informasi SMKI terhadap:

- a. informasi terdokumentasi yang diperlukan sesuai dengan peraturan perundang-undangan yang berlaku; dan
- b. informasi terdokumentasi yang ditentukan oleh Sekretariat Jenderal DPR RI sebagaimana diperlukan untuk efektivitas pengelolaan SMKI.

Kontrol informasi terdokumentasi dilakukan dengan identifikasi dan pengendalian sesuai peraturan perundang-undangan. Akses terhadap informasi terdokumentasi diberikan berdasarkan:

- a. izin akses informasi terdokumentasi; dan/atau
- b. wewenang melihat dan mengubah informasi terdokumentasi.

J. Pemantauan dan Evaluasi

Sekretariat Jenderal DPR RI melaksanakan pemantauan, pengukuran, analisis dan evaluasi terhadap efektifitas penerapan SMKI. Untuk melaksanakan pemantauan, pengukuran, analisis dan evaluasi, Sekretaris Jenderal perlu membentuk tim audit.

Tim audit dimaksud harus memiliki auditor yang telah memiliki sertifikasi internal auditor. Sekretariat Jenderal DPR RI menyimpan informasi terdokumentasi sebagai bukti hasil pemantauan dan pengukuran.

Pimpinan Sekretariat Jenderal DPR RI melalui perwakilan Manajemen terdiri dari Manajemen puncak penyelenggara SMKI dan CISO penyelenggaran SMKI harus meninjau penerapan SMKI secara terencana dengan interval tertentu guna memastikan kesesuaian, kecukupan, efektifitas dan kesetaraan dengan arahan strategis Pimpinan Sekretariat Jenderal DPR RI. Hasil dari kegiatan tinjauan reviu Manajemen harus didokumentasikan.

K. Peningkatan

Sekretariat Jenderal DPR RI senantiasa melakukan peningkatan kesesuaian, kecukupan dan efektivitas dari penerapan SMKI, dengan mempertimbangkan hasil analisis dan evaluasi serta keluaran dari tinjauan Manajemen untuk menetapkan ada tidaknya kebutuhan atau kesempatan yang dapat dilakukan untuk senantiasa melakukan peningkatan.

Penyelenggara SMKI harus mempertahankan semua input dalam catatan perbaikan yang tersedia untuk Sekretariat Jenderal DPR RI termasuk mengkonsolidasikan input dan meninjau penerapan SMKI untuk perbaikan yang dilakukan.

Untuk perubahan yang dilakukan, Penyelenggara SMKI harus menyiapkan rencana aksi dan mengkomunikasikan hasilnya kepada semua pihak yang berkepentingan/terdampak. Semua perbaikan harus diarahkan dan sesuai dengan tujuan penerapan SMKI dan tujuan organisasi.

SEKRETARIS JENDERAL,

ttd.

INDRA ISKANDAR