**SALINAN**

SEKRETARIS JENDERAL
DEWAN PERWAKILAN RAKYAT
REPUBLIK INDONESIA

**PERATURAN**

**SEKRETARIS JENDERAL**

**DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA**

**NOMOR 19 TAHUN 2021**

**TENTANG**

**SISTEM MANAJEMEN KEAMANAN INFORMASI SEKRETARIAT JENDERAL DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA**

**DENGAN RAHMAT TUHAN YANG MAHA ESA**

SEKRETARIS JENDERAL
DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA,

Menimbang

a. bahwa dalam rangka melindungi kerahasiaan, integritas, dan ketersediaan aset informasi Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia dari berbagai bentuk ancaman baik dari dalam maupun luar, perlu menyusun pengaturan manajemen keamanan informasi Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia tentang Sistem Manajemen Keamanan Informasi Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia;

Mengingat : 1. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);

2. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
3. Peraturan Presiden Nomor 26 Tahun 2020 tentang Sekretariat Jenderal Dewan Perwakilan Rakyat Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 39);
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;
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;
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 SEKRETARIAT JENDERAL DEWAN PERWAKILAN RAKYAT REPUBLIK INDONESIA.

## BAB I
## KETENTUAN UMUM

### Pasal 1

Dalam Peraturan Sekretaris Jenderal Dewan Perwakilan Rakyat Republik Indonesia ini yang dimaksud dengan:

1. Dewan Perwakilan Rakyat Republik Indonesia yang selanjutnya disingkat DPR RI adalah sebagaimana dimaksud dalam peraturan perundang-undangan.
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 Dewan DPR RI.
4. Sistem Pemerintahan Berbasis Elektronik selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.

5. Pengguna adalah pegawai Sekretariat Jenderal DPR RI dan atau pihak ketiga serta tidak terbatas pada pengelola teknologi informasi dan komunikasi dan kelompok kerja yang diberikan hak mengakses sistem teknologi informasi dan komunikasi di lingkungan Sekretariat Jenderal DPR RI.
6. 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.
7. 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.
8. Sistem Informasi adalah serangkaian perangkat keras, Perangkat Lunak, sumber daya manusia, serta prosedur dan atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi informasi yang berguna untuk mencapai suatu tujuan.
9. Perangkat Lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan perintah berupa data yang telah diprogram, disimpan, dan diformat secara digital.
10. Keamanan Informasi adalah terjaganya kerahasiaan, keutuhan, dan ketersediaan informasi.
11. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen yang meliputi organisasi, perencanaan, penanggung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan,

mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan Keamanan Informasi.

12. *Chief Information Security Officer* yang selanjutnya disingkat CISO adalah pejabat yang berperan sebagai koordinator dalam pelaksanaan implementasi kebijakan dan standar Sistem Manajemen Keamanan Informasi di lingkungan Sekretariat Jenderal DPR RI.
13. Komite Pengarah TIK adalah komite yang terdiri dari pejabat Pejabat Pimpinan Tinggi Madya dan Pejabat Pimpinan Tinggi Pratama Sekretariat Jenderal DPR RI yang dibentuk dengan tujuan untuk memberikan arahan terhadap pelaksanaan tata kelola TIK Sekretariat Jenderal DPR RI, memberikan dukungan terkait penyusunan kebijakan, standar, dan rencana strategis TIK, serta memberikan rekomendasi perbaikan dari hasil evaluasi layanan TIK.
14. Akun adalah identifikasi Pengguna dengan hak akses memasuki Sistem Informasi TIK yang diberikan oleh Unit Pengelola TIK, bersifat unik dan digunakan bersamaan dengan kata sandi.
15. Administrator adalah sebuah Akun khusus untuk mengelola Sistem Informasi.
16. Aset Informasi adalah aset berwujud dalam bentuk data atau dokumen, perangkat lunak, perangkat komputer, perangkat jaringan dan komunikasi, media yang dapat dipindahkan, perangkat pendukung lainnya, dan aset tak berwujud seperti pengetahuan, pengalaman, keahlian, citra, dan reputasi.
17. Perangkat Jaringan adalah peralatan jaringan komunikasi data.

18. 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.
19. Jaringan Intra adalah jaringan sistem elektronik yang digunakan untuk menghubungkan antar simpul jaringan baik di dalam lingkungan DPR RI maupun interkoneksi antara DPR RI dan instansi lainnya yang dapat dilakukan dengan koneksi jaringan tertutup ataupun terbuka.
20. 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.
21. Pusat Data adalah suatu fasilitas yang digunakan untuk menempatkan sistem elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.
22. Pusat Data Nasional adalah Pusat Data yang memiliki peran melayani keperluan nasional dan keperluan yang bersifat strategis.
23. Unit Pemilik Proses Bisnis adalah unit kerja yang memiliki aplikasi Sistem Informasi yang digunakan di lingkungan Sekretariat Jenderal DPR RI.
24. Unit Pengelola TIK adalah unit kerja yang melakukan pengelolaan teknologi informasi dan komunikasi berupa mengumpulkan, menyiapkan, menyimpan, mengolah, mengumumkan, menganalisis, mengambil

kembali, mengirim atau menerima data dan informasi.

25. Unit Pemilik Aset Informasi adalah unit kerja yang memiliki kewenangan terhadap Aset Informasi yang terdiri dari Unit Pemilik Proses Bisnis dan Unit Pengelola TIK.
26. Aplikasi Berbasis Web adalah aplikasi sistem elektronik yang dapat diakses melalui perambah (*browser*) dan tersambung dengan jaringan internet atau intranet.
27. Aplikasi Berbasis *Mobile* (*mobile apps*) adalah aplikasi sistem elektronik yang digunakan pada perangkat bergerak (*mobile*) untuk mendukung portabilitas Pengguna yang dibangun menggunakan bahasa pemrograman tertentu.

## BAB II
## RUANG LINGKUP SMKI

### Pasal 2

Ruang lingkup Sistem Manajemen Keamanan Informasi meliputi:

a. keamanan data dan informasi;
b. keamanan Aplikasi;
c. keamanan aset Infrastruktur; dan
d. kebijakan Keamanan Informasi yang telah dimiliki.

### Bagian Kesatu
### Keamanan Data dan Informasi

### Pasal3

Data dan informasi mencakup semua jenis data dan informasi elektronik yang dimiliki oleh unit kerja pengelola

data dan informasi dan/atau yang diperoleh dari masyarakat, dan/atau pihak lain.

Pasal4

(1) Keamanan data dan informasi wajib memenuhi standar teknis.

(2) Standar teknis keamanan data dan informasi sebagaimana dimaksud pada ayat (1) terdiri atas terpenuhinya aspek:
   a. kerahasiaan;
   b. keaslian;
   c. keutuhan;
   d. kenirsangkalan; dan
   e. ketersediaan.

Pasal 5

Terpenuhinya aspek kerahasiaan sebagaimana dimaksud dalam Pasal 4 huruf a dilakukan dengan prosedur:

a. menetapkan klasifikasi informasi sebagaimana diatur dalam Peraturan Sekretaris Jenderal yang mengatur tentang sistem klasifikasi keamanan dan akses arsip dinamis;
b. menerapkan enkripsi dengan sistem Kriptografi terhadap data dan informasi yang ditetapkan dengan keputusan Sekretaris Jenderal; dan
c. menerapkan pembatasan akses terhadap data dan informasi sesuai ketentuan yang diatur dalam Peraturan Sekretaris Jenderal tentang Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis.

Pasal 6

Terpenuhinya aspek keaslian sebagaimana dimaksud dalam Pasal 4 huruf b dilakukan dengan prosedur:

a. menyediakan mekanisme verifikasi;
b. menyediakan mekanisme validasi; dan
c. menerapkan sistem *hash function*.

Pasal 7

Terpenuhinya aspek keutuhan sebagaimana dimaksud dalam Pasal 4 huruf c dilakukan dengan prosedur:

a. menerapkan pendeteksian modifikasi; dan
b. menerapkan tanda tangan elektronik tersertifikasi.

Pasal8

Terpenuhinya aspek kenirsangkalan sebagaimana dimaksud dalam Pasal 4 huruf d dilakukan dengan prosedur:

a. menerapkan tanda tangan elektronik tersertifikasi; dan
b. penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.

Pasal9

Terpenuhinya aspek ketersediaan sebagaimana dimaksud dalam Pasal 4 huruf e dilakukan dengan prosedur:

a. menerapkan sistem pencadangan secara berkala;
b. membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses; dan
c. menerapkan sistem pemulihan.

Bagian Kedua

Keamanan Aplikasi

Pasal 10

(1) Pengamanan dilakukan terhadap:
   a. Aplikasi Berbasis *Web*; dan
   b. Aplikasi Berbasis *Mobile* (*mobile apps*).

(2) Pengamanan sebagaimana dimaksud pada ayat (1) dilakukan oleh tim teknis.

(3) Aplikasi sebagaimana dimaksud pada ayat (1) dapat dikategorikan atas:
   a. bersifat strategis;
   b. bersifat tinggi; dan
   c. bersifat rendah.

(4) Aplikasi yang bersifat strategis sebagaimana dimaksud pada ayat (2) huruf a adalah aplikasi yang berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.

(5) Aplikasi yang bersifat tinggi sebagaimana dimaksud pada ayat (2) huruf b adalah aplikasi yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu.

(6) Aplikasi yang bersifat rendah sebagaimana dimaksud pada ayat (2) huruf c adalah aplikasi lainnya yang tidak termasuk pada ayat (2) dan ayat (3).

(7) Tata cara pengkategorian aplikasi sebagaimana dimaksud pada ayat (2) dilakukan berdasarkan ketentuan tentang sistem pengamanan dalam penyelenggaraan sistem elektronik dari lembaga yang membidangi siber dan sandi negara.

Pasal 11

(1) Pengujian aplikasi dilakukan paling sedikit satu kali dalam satu tahun atau sesuai kebutuhan berdasarkan kategorisasi aplikasi sebagaimana dimaksud dalam Pasal 10 ayat (2).

(2) Pengujian aplikasi sebagaimana dimaksud pada ayat (1) yang dilakukan dengan cara:
   a. mengidentifikasi persyaratan minimum keamanan yang belum diterapkan;
   b. memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan;
   c. melakukan pemindaian otomatis dan/atau pengujian penetrasi sistem;
   d. mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan aplikasi; dan
   e. menganalisis kerentanan.

Pasal 12

Standar teknis keamanan Aplikasi Berbasis *Web* sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf a terdiri atas terpenuhinya fungsi:

a. autentikasi;
b. manajemen sesi;
c. persyaratan kontrol akses;
d. validasi input;
e. Kriptografi pada verifikasi statis;
f. penanganan *error* dan pencatatan *log*;
g. proteksi data;
h. keamanan komunikasi;
i. *file*;

j. keamanan *Application Programming Interface* (API) dan *web service*; dan

k. keamanan konfigurasi.

Pasal 13

(1) Terpenuhinya fungsi autentikasi sebagaimana dimaksud dalam Pasal 12 huruf a dilakukan dengan prosedur:

a. menggunakan manajemen kata sandi untuk proses autentikasi;

b. menerapkan verifikasi kata sandi pada sisi server;

c. mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;

d. mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;

e. mengatur mekanisme pemulihan kata sandi;

f. menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme Kriptografi; dan

g. menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.

(2) Terpenuhinya fungsi manajemen sesi sebagaimana dimaksud dalam Pasal 12 huruf b dilakukan dengan prosedur:

a. menggunakan pengendali sesi untuk proses manajemen sesi;

b. menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;

c. mengatur pembuatan dan keacakan kode kunci sesi yang dihasilkan oleh pengendali sesi;

d. mengatur kondisi dan jangka waktu habis sesi;

e. validasi dan pencantuman *session id*;

f. pelindungan terhadap pengiriman kode kunci untuk sesi terautentikasi.

(3) Terpenuhinya fungsi persyaratan kontrol akses sebagaimana dimaksud dalam Pasal 12 huruf c dilakukan dengan prosedur:

a. menetapkan otorisasi Pengguna untuk membatasi kontrol akses;
b. mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi;
c. mengatur antarmuka pada sisi Administrator; dan
d. mengatur verifikasi kebenaran token ketika mengakses data dan informasi.

(4) Terpenuhinya fungsi validasi input sebagaimana dimaksud dalam Pasal 12 huruf d dilakukan dengan prosedur:

a. menerapkan fungsi validasi input pada sisi server;
b. menerapkan mekanisme penolakan input jika terjadi kesalahan validasi;
c. memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi input;
d. melakukan validasi positif pada seluruh input;
e. menggunakan fitur kode dinamis;
f. melakukan pelindungan terhadap akses yang mengandung konten skrip; dan
g. melakukan pelindungan dari serangan injeksi basis data.

(5) Terpenuhinya fungsi Kriptografi pada verifikasi statis sebagaimana dimaksud dalam Pasal 12 huruf e dilakukan dengan prosedur:

a. menggunakan algoritma Kriptografi, modul Kriptografi, protokol Kriptografi, dan kunci

Kriptografi;

b. melakukan autentikasi data yang dienkripsi;

c. menerapkan manajemen kunci Kriptografi; dan

d. membuat angka acak yang menggunakan generator angka acak Kriptografi.

(6) Terpenuhinya fungsi penanganan *error* dan per[illegible]na dimaksud dalam Pasal 12 hur[illegible] prosedur:

a. mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;

b. menggunakan metode penanganan *error* untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;

c. tidak mencantumkan informasi yang dikecualikan dalam pencatatan *log*;

d. mengatur cakupan *log* yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;

e. mengatur pelindungan *log* aplikasi dari akses dan modifikasi yang tidak sah; dan

f. melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

(7) Terpenuhinya fungsi proteksi data sebagaimana dimaksud dalam Pasal 12 huruf g dilakukan dengan prosedur:

a. melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;

b. melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;

c. melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
d. menentukan metode untuk menghapus dan mengekspor data; dan
e. membersihkan memori setelah tidak diperlukan.

(8) Terpenuhinya fungsi keamanan komunikasi sebagaimana dimaksud dalam Pasal 12 huruf h dilakukan dengan prosedur:
a. menggunakan komunikasi terenkripsi;
b. mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi Pengguna;
c. mengatur jenis algoritma yang digunakan dan alat pengujiannya; dan
d. mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.

(9) Terpenuhinya fungsi *file* sebagaimana dimaksud dalam Pasal 12 huruf i dilakukan dengan prosedur:
a. mengatur jumlah *file* untuk setiap Pengguna dan kuota ukuran *file* yang diunggah;
b. melakukan validasi *file* sesuai dengan tipe konten yang diharapkan;
c. melakukan pelindungan terhadap metadata input dan metadata *file*; dan
d. melakukan konfigurasi server untuk mengunduh *file* sesuai ekstensi yang ditentukan.

(10) Terpenuhinya fungsi keamanan *Application Programming Interface* (API) dan *web service* sebagaimana dimaksud dalam Pasal 12 huruf j dilakukan dengan prosedur:
a. melakukan konfigurasi layanan web;

b. memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
c. membuat keputusan otorisasi;
d. menampilkan metode API yang disediakan apabila input Pengguna dinyatakan valid;
e. menggunakan validasi skema dan verifikasi sebelum menerima input;
f. menggunakan metode pelindungan layanan berbasis web; dan
g. menerapkan kontrol antiotomatisasi.

(11) Terpenuhinya fungsi keamanan konfigurasi sebagaimana dimaksud dalam Pasal 12 huruf k dilakukan dengan prosedur:
a. mengkonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan;
b. mendokumentasi, menyalin konfigurasi, dan semua dependensi;
c. menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;
d. memvalidasi integritas aset jika aset aplikasi diakses secara eksternal; dan
e. menggunakan respons aplikasi dan konten yang aman.

Pasal 14

Standar teknis keamanan Aplikasi Berbasis *Mobile* (*mobile apps*) sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf b terdiri atas terpenuhinya fungsi:
a. penyimpanan data dan persyaratan privasi;
b. Kriptografi;

c. autentikasi dan manajemen sesi;
d. komunikasi jaringan;
e. interaksi *platform*;
f. kualitas kode dan pengaturan *build*; dan
g. ketahanan.

Pasal 15

(1) Terpenuhinya fungsi penyimpanan data dan persyaratan privasi sebagaimana dimaksud dalam Pasal 14 huruf a dilakukan dengan prosedur:
   a. menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem;
   b. membatasi pertukaran data dan informasi yang dikecualikan dengan Pihak Ketiga; dan
   c. melindungi data dan informasi yang dikecualikan yang dimasukkan melalui antarmuka Pengguna.

(2) Terpenuhinya fungsi Kriptografi sebagaimana dimaksud dalam Pasal 14 huruf b dilakukan dengan prosedur:
   a. menghindari Penggunaan Kriptografi simetrik dengan *hardcoded key*;
   d. mengimplementasikan metode Kriptografi yang sudah teruji sesuai kebutuhan;
   e. menghindari Penggunaan protokol Kriptografi atau algoritma Kriptografi yang obsolet;
   f. menghindari Penggunaan kunci Kriptografi yang sama; dan
   g. menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.

(3) Terpenuhinya fungsi autentikasi dan manajemen sesi sebagaimana dimaksud dalam Pasal 14 huruf c

dilakukan dengan prosedur:

a. menerapkan autentikasi pada *remote endpoint* terhadap aplikasi yang menyediakan akses Pengguna untuk layanan jarak jauh;
b. memastikan server menyediakan token yang telah ditandatangani menggunakan algoritma yang aman apabila menggunakan autentikasi *stateless* berbasis token;
c. memastikan *remote endpoint* memutus sesi yang ada saat Pengguna *log out*;
d. menerapkan pengaturan sandi pada *remote endpoint;*
e. membatasi jumlah percobaan log in pada *remote endpoint*;
f. menentukan masa berlaku sesi dan masa kadaluarsa token pada *remote endpoint*; dan
g. melakukan otorisasi pada *remote endpoint.*

(4) Terpenuhinya fungsi komunikasi jaringan sebagaimana dimaksud dalam Pasal 14 huruf d dilakukan dengan prosedur:

a. menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolet secara konsisten; dan
b. memverifikasi sertifikat *remote endpoint.*

(5) Terpenuhinya fungsi interaksi platform sebagaimana dimaksud dalam Pasal 14 huruf e dilakukan dengan prosedur:

a. memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan;
b. melakukan validasi terhadap seluruh input dari sumber eksternal dan Pengguna;

c. menghindari Penggunaan *JavaScript* dalam *WebView*;
d. menggunakan protokol *hypertext transfer protocol* secure pada *WebView*; dan
e. mengimplementasikan Penggunaan serialisasi API yang aman.

(6) Terpenuhinya fungsi kualitas kode dan pengaturan *build* sebagaimana dimaksud dalam Pasal 14 huruf f dilakukan dengan prosedur:
a. menandatangani aplikasi dengan sertifikat yang valid;
b. memastikan aplikasi dalam mode rilis;
c. menghapus simbol *debugging* dari *native binary*;
d. menghapus kode *debugging* dan kode bantuan pengembang;
e. mengidentifikasi kelemahan seluruh komponen *third party*;
f. menentukan mekanisme penanganan *error*;
g. mengelola memori secara aman; dan
h. mengaktifkan fitur keamanan yang tersedia.

(7) Terpenuhinya fungsi ketahanan sebagaimana dimaksud dalam Pasal 14 huruf g dilakukan dengan prosedur:
a. mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah;
b. mendeteksi dan merespons *debugger*;
c. mencegah *executable file* melakukan perubahan pada sumber daya perangkat;
d. mendeteksi dan merespons keberadaan perangkat *reverse engineering*;
e. mencegah aplikasi berjalan dalam emulator;

f. mendeteksi perubahan kode dan data di ruang memori;
g. menerapkan fungsi *device binding* dengan menggunakan *property* unik pada perangkat;
h. melindungi seluruh file dan *library* pada aplikasi; dan
i. menerapkan metode *obfuscation*.

Bagian Ketiga
Keamanan Sistem Penghubung Layanan

Pasal 16

(1) Tim teknis melakukan pengamanan terhadap sistem penghubunglayanan.
(2) Pengamanan sistem penghubung layanan sebagaimana dimaksud pada ayat (1) terdiri atas terpenuhinya fungsi:
a. keamanan interoperabilitas data dan informasi;
b. kontrol sistem integrasi;
c. kontrol perangkat integrator;
d. keamanan API dan *web service*; dan
e. keamanan migrasi data.

Pasal 17

(1) Terpenuhinya fungsi keamanan interoperabilitas data dan informasi sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf a dilakukan dengan prosedur:
a. menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik;
b. menerapkan sistem enkripsi data;
c. memastikan data dan informasi selalu dapat diakses sesuai otoritasnya; dan

d. menerapkan sistem *hash function* pada file.

(2) Terpenuhinya fungsi kontrol sistem integrasi sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf b dilakukan dengan prosedur:

a. menerapkan protokol *secure socket layer* atau protokol *transport layer security* versi terkini pada sesi pengiriman data dan informasi;
b. menerapkan *internet protocol security* untuk mengamankan transmisi data dalam jaringan berbasis *transmission control protocol/ internet protocol*;
c. menerapkan sistem *anti distributed denial of service*;
d. menerapkan autentikasi untuk memverifikasi identitas eksternal antar layanan yang terhubung;
e. menerapkan manajemen keamanan sesi;
f. menerapkan pembatasan akses Pengguna berdasarkan otorisasi yang telah ditetapkan;
g. menerapkan validasi input;
h. menerapkan Kriptografi pada verifikasi statis;
i. menerapkan sertifikat elektronik pada *web authentication*;
j. menerapkan penanganan *error*dan pencatatan log;
k. menerapkan proteksi data dan jalur komunikasi;
l. menerapkan pendeteksi virus untuk memeriksa beberapa konten *file*; dan
m. memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.

(3) Terpenuhinya fungsi kontrol perangkat integrator sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf c dilakukan dengan prosedur:

a. menggunakan sistem operasi dan Perangkat Lunak dengan *security patches* terkini;
b. menggunakan anti virus dan *anti-spyware* terkini;
c. mengaktifkan fitur keamanan pada peramban web;
d. menerapkan *firewall* dan *host-based intrusion detection systems*;
e. mencegah instalasi Perangkat Lunak yang belum terverifikasi;
f. mencegah akses terhadap situs yang tidak sah; dan
g. mengaktifkan sistem *recovery* dan *restore* pada perangkat integrator.

(4) Terpenuhinya fungsi keamanan API dan *web service* sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf d dilakukan dengan prosedur:
a. menerapkan *protokol secure socket layer* atau protokol *transport layer security* di antara pengirim dan penerima API;
b. menerapkan protokol *open authorization* untuk menjembatani interaksi antara *resource owner*, *resource server* dan/atau *third party*;
c. menampilkan metode *web service* apabila input Pengguna dinyatakan valid;
d. melindungi layanan *web service* yang menggunakan *cookie* dari *cross-site request forgery*, dan
e. memvalidasi parameter yang masuk oleh penerima untuk memastikan data yang diterima valid dan tidak menyebabkan kerusakan.

(5) Terpenuhinya fungsi keamanan migrasi data sebagaimana dimaksud dalam Pasal 16 huruf e dilakukan dengan prosedur:

a. memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem;
b. melakukan pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data; dan
c. melakukan validasi data ketika proses migrasi data selesai.

Bagian Keempat
Keamanan Jaringan Intra

Pasal 18

(1) Tim teknis melakukan pengamanan terhadap Jaringan Intra.
(2) Standar teknis keamanan Jaringan Intra sebagaimana dimaksud pada ayat (1) diterapkan pada:
a. Jaringan Intra DPR RI; dan
b. Jaringan Intra DPR RI dan instansi lainnya.

Pasal 19

Pengamanan Jaringan Intra sebagaimana dimaksud pada Pasal 18 terdiri atas dipenuhinya:
a. aspek administrasi keamanan Jaringan Intra;
b. kontrol akses dan autentikasi;
c. persyaratan perangkat dan aplikasi keamanan Jaringan Intra;
d. kontrol keamanan *gateway*;
e. kontrol keamanan *access point* pada jaringan nirkabel; dan
f. kontrol konfigurasi *access point* padajaringan nirkabel.

Pasal 20

(1) Terpenuhinya aspek administrasi keamanan Jaringan Intra sebagaimana dimaksud dalam Pasal 19 huruf a dilakukan dengan prosedur:
   a. menyusun dan mengevaluasi dokumen arsitektur Jaringan Intra;
   b. mengidentifikasi seluruh aset Infrastruktur jaringan;
   c. menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra; dan
   d. membuat laporan pengawasan keamanan jaringan secara periodik.

(2) Terpenuhinya kontrol akses dan autentikasi sebagaimana dimaksud dalam Pasal 19 huruf b dilakukan dengan prosedur:
   a. menempatkan perangkat Infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah;
   b. menggunakan autentikasi untuk mengakses Jaringan Intra;
   c. menerapkan pembatasan akses dalam Jaringan Intra;
   d. mematikan atau membatasi *protocol*, *port*, dan layanan yang tidak digunakan;
   e. menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya;
   f. menerapkan fungsi *honeypot* untuk menganalisis celah keamanan berdasarkan jenis serangan;
   g. menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;

h. memberikan kewenangan hanya kepada administrator untuk menginstal Perangkat Lunak dan/atau mengubah konfigurasi sistem dalam Jaringan Intra;

i. menerapkan *secure endpoints*;

j. memblokir layanan yang tidak dikenal; dan

k. menerapkan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses Jaringan Intra.

(3) Terpenuhinya persyaratan perangkat dan aplikasi keamanan Jaringan Intra sebagaimana dimaksud dalam 19 huruf c dilakukan dengan prosedur:

a. menggunakan perangkat *security information and event management* untuk *network logging* dan *monitoring*;

b. menerapkan sistem deteksi dini kerentanan keamanan Perangkat Jaringan;

c. menggunakan perangkat *firewall*;

d. menggunakan perangkat *intrusion detection systems* dan *intrusion prevention systems*;

e. menerapkan *virtual private network* terenkripsi untuk penggunaan akses jarak jauh secara terbatas;

f. menerapkan kontrol *update patching* pada Infrastruktur Jaringan Intra dan sistem komputer;

g. menggunakan perangkat *web application firewall*;

h. menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;

i. memperbarui teknologi keamanan perangkat keras dan Perangkat Lunak untuk meminimalisasi celah peretas;

j. mengunduh Perangkat Lunak melalui *enterprise software distribution system*; dan

k. menerapkan sertifikat elektronik.

(4) Terpenuhinya kontrol keamanan *gateway* sebagaimana dimaksud dalam 19 huruf d dilakukan dengan prosedur:

a. menerapkan *content filtering*;

b. menerapkan *inspection packet filtering* untuk memeriksa *packet* yang masuk pada Jaringan Intra;

c. menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*;

d. memastikan perangkat *gateway* yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik;

e. melaksanakan manajemen *traffic gateway*; dan

f. memastikan *port* tidak dibuka secara *default*.

(5) Terpenuhinya kontrol keamanan *access point* pada jaringan nirkabel sebagaimana dimaksud dalam Pasal 19 huruf e dilakukan dengan prosedur:

a. menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini;

b. menerapkan media *access control* pada *address filtering*;

c. menerapkan pembatasan jangkauan radio transmisi dan Pengguna jaringan;

d. menerapkan pembatasan terkait penambahan perangkat *access point* yang dipasang secara tidak sah di Jaringan Intra DPR RI;

e. menerapkan manajemen kerentanan secara berkala dan berkelanjutan; dan

f. melakukan *patching firmware* secara rutin.

(6) Terpenuhinya kontrol konfigurasi *access point* pada jaringan nirkabel sebagaimana dimaksud dalam Pasal 19 huruf f dilakukan dengan prosedur:

a. menggunakan kata sandi yang kuat;
b. menggunakan protokol model *authentication authorization* dan *accounting* pada perangkat Infrastruktur jaringan untuk *management user* atau otentikasi Administrator *access point*;
c. memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan;
d. mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel; dan
e. menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

Bagian Kelima

Keamanan Pusat Data

Pasal 21

(1) Tim teknis melakukan pengamanan terhadap Pusat Data.

(2) Keamanan Pusat Data sebagaimana dimaksud pada ayat (1) terdiri atas dipenuhinya:

a. persyaratan keamanan fisik dan manajemen Pusat Data; dan
b. persyaratan koneksi ke Pusat Data Nasional.

Pasal22

Terpenuhinya persyaratan keamanan fisik dan manajemen Pusat Data sebagaimana dimaksud dalam Pasal 21 ayat (2) huruf a dilakukan dengan prosedur sesuai dengan Standar

Nasional Indonesia yang terkait dengan Pusat Data.

Pasal23

Terpenuhinya persyaratan koneksi ke Pusat Data Nasional sebagaimana dimaksud dalam Pasal 21 ayat (2) huruf b dilakukan dengan prosedur:

a. memastikan keamanan perangkat yang terkoneksi ke Infrastruktur Pusat Data Nasional;
b. memutus akses fisik atau *logic* dari perangkat yang tidak terotorisasi;
c. memastikan hanya personil yang berwenang yang boleh menggunakan komputer di area Pusat Data Nasional;
d. melakukan *backup* informasi dan Perangkat Lunak yang berada di Pusat Data Nasional secara berkala;
e. memastikan perangkat komputer Pusat Data Nasional terbebas dari virus dan *malware*;
f. melakukan pembatasan akses pemanfaatan *removable media* di area Pusat Data Nasional;
g. memastikan pengaktifan konfigurasi *port universal serial bus* telah mendapatkan izin dari personil yang berwenang; dan
h. memastikan setiap perangkat yang akan terkoneksi ke Infrastruktur Pusat Data Nasional menggunakan *internet protocol address* dan *hostname* yang telah ditentukan.

Bagian Keenam

Keamanan Infrastruktur

Pasal 24

(1) Tim teknis melakukan pengamanan terhadap

Infrastruktur yang terdiri atas:

a. aplikasi;
b. server;
c. *storage*;
d. *firewall*; dan
e. Perangkat Jaringan, seperti *switch*, *router*, dan kabel UTP.

(2) Standar teknis Keamanan Infrastruktur sebagaimana dimaksud pada ayat (1) terdiri atas terpenuhinya fungsi:

a. aspek administrasi keamanan Jaringan Intra;
b. kontrol akses dan autentikasi;
c. persyaratan perangkat dan aplikasi keamanan Jaringan Intra;
d. kontrol keamanan *gateway*; dan
e. kontrol keamanan dan kontrol konfigurasi *access point* pada jaringan nirkabel.

Pasal 25

(1) Terpenuhinya fungsi aspek administrasi keamanan Jaringan Intra sebagaimana dimaksud dalam Pasal 24 ayat (2) huruf a dilakukan dengan prosedur:

a. menyusun dan mengevaluasi dokumen arsitektur Jaringan Intra;
b. mengidentifikasi seluruh aset Infrastruktur jaringan;
c. menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra; dan
d. membuat laporan pengawasan keamanan jaringan secara periodik.

(2) Terpenuhinya fungsi kontrol akses dan autentikasi sebagaimana dimaksud dalam Pasal 24 ayat (2) huruf b dilakukan dengan prosedur:

a. menempatkan perangkat Infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah;
b. menggunakan autentikasi untuk mengakses Jaringan Intra;
c. menerapkan pembatasan akses dalam Jaringan Intra;
d. mematikan atau membatasi protokol, *port*, dan layanan yang tidak digunakan;
e. menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya;
f. menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;
g. memberikan kewenangan hanya kepada Administrator untuk menginstal Perangkat Lunak dan/atau mengubah konfigurasi sistem dalam Jaringan Intra;
h. menerapkan *secure endpoints*;
i. memblokir layanan yang tidak dikenal;
j. menerapkan *secure socket layer* atau *transport layer security* versi terbaru pada jalur akses Jaringan Intra; dan
k. menerapkan server perantara saat *client* mengakses server *database* dalam rangka pemeliharaan.

(3) Terpenuhinya fungsi persyaratan perangkat dan aplikasi keamanan Jaringan Intra sebagaimana

dimaksud dalam Pasal 24 ayat (2) huruf c dilakukan dengan prosedur:

a. menggunakan perangkat *security information and event management* untuk *network logging* dan *monitoring*;
b. menerapkan sistem deteksi dini kerentanan keamanan Perangkat Jaringan;
c. menggunakan perangkat *firewall*;
d. menerapkan *virtual private network* terenkripsi untuk penggunaan akses jarak jauh secara terbatas;
e. menerapkan kontrol *update patching* pada Infrastruktur Jaringan Intra dan sistem komputer;
f. menggunakan perangkat *web application firewall*;
g. menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;
h. memperbarui teknologid keamanan perangkat keras dan Perangkat Lunak untuk meminimalisasi celah peretas;
i. mengunduh Perangkat Lunak melalui *enterprise software distribution system*; dan
j. menerapkan sertifikat elektronik.

(4) Terpenuhinya fungsi kontrol keamanan *gateway* sebagaimana dimaksud dalam Pasal 24 ayat (2) huruf d dilakukan dengan prosedur:

a. menerapkan *content filtering*;
b. menerapkan *inspection packet filtering* untuk memeriksa paket yang masuk pada Jaringan Intra;
c. menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*;

d. memastikan perangkat *gateway* yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik;
e. melaksanakan manajemen *traffic gateway*; dan
f. memastikan *port* tidak dibuka secara *default*.

(5) Terpenuhinya fungsi kontrol keamanan *access point* pada jaringan nirkabel sebagaimana dimaksud dalam Pasal 24 ayat (2) huruf e dilakukan dengan prosedur:
a. menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini;
b. menerapkan media *access control* pada *address filtering*;
c. menerapkan *dedicated service set identifier*;
d. menerapkan pembatasan jangkauan radio transmisi dan Pengguna jaringan;
e. menerapkan pembatasan terkait penambahan perangkat nirkabel yang dipasang secara tidak sah;
f. menerapkan manajemen kerentanan secara berkala dan berkelanjutan; dan
g. melakukan *patching firmware* secara rutin.

(6) Terpenuhinya fungsi kontrol konfigurasi *access point* pada jaringan nirkabel sebagaimana dimaksud dalam Pasal 24 ayat (2) huruf e dilakukan dengan prosedur:
a. menggunakan kata sandi yang kuat;
b. menggunakan protokol model *authentication authorization* pada perangkat Infrastruktur jaringan untuk *user management* atau otentikasi *administrator access point*;
c. memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan;

d. mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel; dan
e. menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

## BAB III
## PENANGGUNG JAWAB SMKI

### Pasal26

(1) Penanggungjawab SMKI adalah Sekretaris Jenderal.
(2) Penanggung jawab menetapkan CISO sebagai pelaksana teknis keamanan informasi.
(3) CISO dijabat oleh pejabat pimpinan tinggi pratama yang membidangi teknologi dan informasi.
(4) Dalam melaksanakan tugasnya, CISO dibantu oleh tim teknis.
(5) Susunan keanggotaan dan tugas tim teknis sebagaimana dimaksud pada ayat (4) ditetapkan dengan keputusan Sekretaris Jenderal.

### Pasal 27

Penanggungjawab sebagaimana dimaksud dalam Pasal 26 ayat (1) memiliki tugas memberikan dukungan pengoperasian keamanan informasi.

### Pasal28

CISO sebagaimana dimaksud dalam Pasal 26 ayat (3) mempunyai tugas:

a. mengkoordinasikan perumusan dan penyempurnaan kebijakan dan standar SMKI Sekretariat Jenderal DPR RI;

b. memastikan penerapan kebijakan dan standar SMKI Sekretariat Jenderal DPR RI;
c. menetapkan target Keamanan Informasi setiap tahun serta menyusun rencana kerja;
d. memastikan tersedianya dukungan pengoperasian Keamanan Informasi;
e. memastikan efektivitas dan konsistensi penerapan kebijakan dan standar SMKI Sekretariat Jenderal DPR RI serta mengukur kinerja keseluruhan;
f. melakukan evaluasi kinerja pelaksanaan Keamanan Informasi;
g. melaporkan kinerja penerapan kebijakan dan standar SMKI Sekretariat Jenderal DPR RI serta pencapaian target kepada Komite Pengarah TIK;
h. menunjuk pihak yang berkompeten untuk melakukan audit terhadap penerapan kebijakan dan standar SMKI Sekretariat Jenderal DPR RI;
i. memastikan seluruh pembangunan atau pengembangan aplikasi dan Infrastruktur SPBE yang dilakukan oleh Pihak Ketiga memenuhi standar teknis dan prosedur keamanan SPBE yang telah ditetapkan; dan
j. berkoordinasi dengan instansi lain terkait penerapan Keamanan Informasi.

## BAB IV
## PERENCANAAN SMKI

### Pasal 29

(1) Perencanaan SMKI dilakukan dengan merumuskan:
a. program kerja Keamanan Informasi yang disusun berdasarkan rencana induk TIK dan/atau *grand*

*design* Keamanan Informasi; dan

b. target realisasi program kerja Keamanan Informasi ditetapkan berdasarkan kebutuhan DPR RI.

(2) Perencanaan SMKI sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan ketentuan dari lembaga yang membidangi siber dan sandi negara.

Pasal 30

Program kerja Keamanan Informasi sebagaimana dimaksud pada Pasal 29 huruf a meliputi:

a. edukasi kesadaran Keamanan Informasi;
b. penilaian kerentanan Keamanan Informasi;
c. peningkatan Keamanan Informasi;
d. penanganan insiden Keamanan Informasi; dan
e. audit Keamanan Informasi.

Pasal 31

Edukasi kesadaran Keamanan Informasi sebagaimana dimaksud dalam Pasal 30 huruf a dilaksanakan kepada kepada Pengguna dan Unit Pemilik Proses Bisnis paling sedikit melalui kegiatan:

a. sosialisasi; dan
b. pelatihan.

Pasal 32

Penilaian kerentanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 30 huruf b dilaksanakan paling sedikit melalui:

a. menginventarisasi seluruh aset yang meliputi data dan informasi, aplikasi, dan Infrastruktur;

b. mengidentifikasi kerentanan dan ancaman terhadap aset; dan
c. mengukur tingkat risiko Keamanan Informasi berdasarkan peraturan perundang-undangan.

Pasal 33

Peningkatan Keamanan Informasi dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 30 huruf c paling sedikit melalui:
a. menerapkan standar teknis dan prosedur Keamanan Informasi; dan
b. menguji fungsi keamanan terhadap aplikasi dan Infrastruktur.

Pasal34

Penanganan insiden Keamanan Informasi sebagaimana dimaksud dalam Pasal 30 huruf d dilaksanakan paling sedikit melalui:
a. mengidentifikasi sumber serangan;
b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
d. mendokumentasi bukti insiden yang terjadi; dan
e. memitigasi atau mengurangi dampak risiko Keamanan Informasi.

Pasal 35

(1) Audit Keamanan Informasi di lingkungan Sekretariat Jenderal DPR RI sebagaimana dimaksud dalam Pasal 30 huruf e dilakukan dengan tujuan untuk

memastikan pengendalian, proses, dan prosedur SMKI dilaksanakan secara efektif dan dipelihara dengan baik.

(2) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan secara internal oleh tim audit yang ditunjuk oleh CISO.

(3) Audit Keamanan Informasi selain dilakukan oleh tim audit sebagaimana dimaksud pada ayat (2) dapat dilakukan oleh pihak eksternal terakreditasi sesuai ketentuan peraturan perundang-undangan.

(4) Pihak yang melakukan audit sebagaimana dimaksud pada ayat (2) dan (3) menyampaikan laporan hasil audit Keamanan Informasi kepada CISO.

(5) CISO menyampaikan laporan hasil audit kepada penanggung jawab SMKI dan instansi terkait sesuai ketentuan peraturan perundang-undangan.

(6) Unit Pengelola TIK berkoordinasi dengan Unit Pemilik Proses Bisnis untuk melakukan tindak lanjut atas laporan hasil audit Keamanan Informasi.

## BAB V
## DUKUNGAN PENGOPERASIAN

### Pasal 36

(1) Dukungan pengoperasian Keamanan Informasi dilakukan dengan meningkatkan kapasitas terhadap:
   a. sumber daya manusia Keamanan Informasi; dan
   b. anggaran Keamanan Informasi.

(2) Dukungan pengoperasian terhadap sumber daya manusia Keamanan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan dengan berkoordinasi dengan unit kerja yang membidangi pendidikan dan

pelatihan.

Pasal 37

(1) Sumber daya manusia Keamanan Informasi sebagaimana dimaksud Pasal 36 huruf a paling sedikit harus memiliki kompetensi:
   a. keamanan Infrastruktur teknologi, informasi, dan komunikasi; dan
   b. keamanan aplikasi.
(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), tim teknis paling sedikit melakukan kegiatan:
   a. pelatihan dan/atau sertifikasi kompetensi keamanan Infrastruktur teknologi, informasi dan komunikasi, dan keamanan aplikasi; dan
   b. bimbingan teknis mengenai standar Keamanan Informasi.

Pasal38

Anggaran Keamanan Informasi sebagaimana dimaksud dalam Pasal 36 huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI

EVALUASI KINERJA

Pasal39

Evaluasi kinerja Keamanan Informasi dilaksanakan dengan:

a. melakukan identifikasi risiko dalam keberhasilan pelaksanaan Keamanan informasi;

b. menganalisis efektifitas pelaksanaan Keamanan informasi; dan
c. mendukung dan merealisasikan program audit Keamanan informasi.

BAB VII
PERBAIKAN BERKELANJUTAN

Pasal40

Perbaikan berkelanjutan Keamanan Informasi merupakan tindak lanjut dari hasil evaluasi kinerja.

Pasal 41

Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 40 dilakukan dengan:
a. mengatasi permasalahan dalam pelaksanaan Keamanan Informasi; dan
b. memperbaiki pelaksanaan Keamanan Informasi secara periodik paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

BAB VIII
KEPATUHAN PENGGUNA

Pasal 42

(1) Pengguna bertanggung jawab terhadap penggunaan Jaringan Intra DPR RI.
(2) Tanggung jawab Pengguna sebagaimana dimaksud pada ayat (1) meliputi:
    a. menggunakan Jaringan Intra DPR RI hanya untuk kepentingan kedinasan sesuai dengan tugas, fungsi, dan wewenang;

b. menggunakan Jaringan Intra DPR RI sesuai dengan norma hukum dan etika yang berlaku; dan
c. menggunakan Jaringan Intra DPR RI secara bijak dan hemat sesuai tugas dan fungsinya.

Pasal 43

Pengguna Jaringan Intra DPR RI dilarang:

a. melewati perangkat pengamanan, pengendalian/ pembatasan akses internet;
b. mengakses, mengunggah, mengunduh, dan/atau mempublikasikan situs-situs yang tidak menunjang kedinasan;
c. mengunggah, mengunduh, dan/atau menjalankan Perangkat Lunak berlisensi milik Sekretariat Jenderal DPR RI untuk keperluan di luar kedinasan;
d. memberikan pendapat pribadi ke pihak lain melalui fasilitas internet dengan mengatasnamakan Sekretariat Jenderal DPR RI;
e. mengungkapkan atau menyebarkan informasi milik Sekretariat Jenderal DPR RI yang termasuk dalam klasifikasi terbatas, rahasia, dan sangat rahasia;
f. menggunakan fasilitas internet untuk menyebarkan ujaran kebencian, pelecehan seksual, suku, agama, ras, dan antargolongan, pornografi, dan kepentingan pribadi;
g. mengakibatkan insiden Keamanan Informasi seperti penerobosan jaringan atau gangguan layanan sistem informasi;
h. mengakses situs yang dikategorikan sebagai *proxy*, *phising*, *malware*, *peer-to-peer*, *hacking*, *games*, *gambling*, *pornography*, dan *command and control*;

i. melakukan segala bentuk monitoring jaringan dan *intercept* (pencegatan) data;
j. melakukan *scanning port* dan aplikasi jaringan; dan
k. menyebarkan program jahat seperti virus, *worm*, *trojan*, *email bomb*, dan lain lain pada Jaringan Intra DPR RI.

Pasal 44

(1) Pengguna yang melanggar larangan sebagaimana dimaksud dalam Pasal 43 dikenakan sanksi berupa penonaktifan Akun sampai dengan adanya permintaan resmi untuk mengaktifkan kembali.
(2) Dalam hal Pengguna yang melanggar adalah aparatur sipil negara, selain sanksi sebagaimana dimaksud pada ayat (1) dikenakan sanksi administratif sesuai dengan Peraturan Sekretaris Jenderal yang mengatur tentang kode etik aparatur sipil negara.

BAB IX
PENUTUP

Pasal 45

Peraturan Sekretaris Jenderal ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta,
pada tanggal 1 Oktober 2021
**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.