KEPALA BADAN SIBER DAN SANDI NEGARA
REPUBLIK INDONESIA

KEPUTUSAN KEPALA BADAN SIBER DAN SANDI NEGARA

NOMOR 499 TAHUN 2023

TENTANG

TEMPLAT KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

KEPALA BADAN SIBER DAN SANDI NEGARA,

Menimbang :

a. bahwa Sistem Manajemen Keamanan Informasi adalah 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;

b. bahwa templat kebijakan Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik ini merupakan alat bantu bagi Instansi Pemerintah dalam menyusun kebijakan Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan b, perlu menetapkan Keputusan Kepala Badan Siber dan Sandi Negara tentang Templat Kebijakan Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik.

Mengingat :

1. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 185);

3. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

4. Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);

5. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dan Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);

6. Peraturan …

6. 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 (Berita Negara Republik Indonesia 2021 Nomor 541); dan
7. Peraturan Badan Siber dan Sandi Negara Nomor 6 Tahun 2021 tentang Struktur Organisasi dan Tata Kerja Badan Siber dan Sandi Negara (Berita Negara Republik Indonesia Tahun 2021 Nomor 803).

MEMUTUSKAN:

Menetapkan : KEPUTUSAN KEPALA BADAN SIBER DAN SANDI NEGARA TENTANG TEMPLAT KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

KESATU : Menetapkan Templat Kebijakan Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik sebagai alat bantu Instansi Pemerintah dalam menyusun kebijakan Sistem Manajemen Keamanan Informasi.

KEDUA : Instansi Pemerintah dapat mengadopsi templat kebijakan Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik ini sesuai dengan kondisi dan kebutuhan masing-masing Instansi Pemerintah.

KETIGA : Templat Kebijakan Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Keputusan Kepala ini.

KEEMPAT : Keputusan Kepala ini mulai berlaku pada tanggal ditetapkan, dengan catatan bahwa apabila di kemudian hari ternyata terdapat kekeliruan dalam Keputusan Kepala ini maka akan diadakan perubahan sebagaimana mestinya.

Ditetapkan di Jakarta
pada tanggal 8 Agustus 2023

Ditandatangani secara elektronik oleh:
KEPALA BADAN SIBER DAN SANDI NEGARA

**Hinsa Siburian**
Letnan Jenderal TNI (Purn)

LAMPIRAN I
KEPUTUSAN KEPALA BADAN SIBER DAN SANDI NEGARA
NOMOR : 499 TAHUN 2023
TANGGAL : 8 Agustus 2023

PERATURAN **[PIMPINAN INSTANSI]**

NOMOR xxx TAHUN xxxx

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI

SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DI LINGKUNGAN **[NAMA INSTANSI]**

DENGAN RAHMAT TUHAN YANG MAHA ESA

**[PIMPINAN INSTANSI]**,

Menimbang :

a. bahwa untuk menjamin keamanan SPBE di lingkungan **[Nama Instansi]**, perlu melaksanakan manajemen keamanan informasi dalam rangka menjamin kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE;
b. bahwa untuk melaksanakan ketentuan Pasal 48 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu adanya manajemen keamanan informasi;
c. bahwa untuk melaksanakan ketentuan Pasal 9 Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik, Penyelenggaraan Sistem Elektronik lingkup publik yang memiliki sistem elektronik strategis dan/atau tinggi perlu menerapkan SNI ISO/IEC 27001;
d. [dapat ditambahkan sesuai kebutuhan];
e. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, **[huruf d]**, perlu menetapkan Peraturan **[Pimpinan Instansi]** tentang Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan **[Nama Instansi]**.

Mengingat :

1. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia

Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
2. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185)
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
4. 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);
5. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE (Berita Negara Republik Indonesia Tahun 2021 Nomor 541).

MEMUTUSKAN:

Menetapkan : PERATURAN **[PIMPINAN INSTANSI]** TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN **[NAMA INSTANSI]**.

## BAB I
## KETENTUAN UMUM

### Pasal 1

Dalam Peraturan **[Pimpinan Instansi]** ini yang dimaksud dengan:

1. Teknologi Informasi dan Komunikasi selanjutnya disebut TIK adalah terminologi yang mencakup seluruh peralatan teknis untuk memproses dan menyampaikan informasi.
2. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
3. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
4. Data adalah tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic*

*mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi.

5. Informasi adalah satu atau sekumpulan Data, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *eletronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
6. Aplikasi adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan.
7. Infrastruktur adalah semua 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.
8. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko.
9. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersedian, dan kenirsangkalan informasi.
10. Risiko adalah segala kejadian dalam setiap aktivitas yang mungkin timbul karena faktor ketidakpastian, yang mengandung potensi untuk menghambat pencapaian sasaran kinerja dari layanan Sistem Elektronik.
11. Manajemen risiko adalah aktivitas terkoordinasi untuk identifikasi, penilaian, dan penentuan prioritas risiko yang kemudian akan dikelola, dipantau, dan dikontrol untuk mengurangi dampak dan/ atau kemungkinan terjadinya risiko tersebut.
12. *Risk Treatment Plan* (RTP) atau Rencana Tindak Lanjut (RTL) Risiko adalah respon yang direncanakan manajemen untuk menindaklanjuti hasil evaluasi risiko, seperti *mitigate/reduce, avoid, share/ transfer* atau *accept*.
13. Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk

menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.

14. Audit Keamanan Informasi adalah Audit TIK cakupan keamanan informasi.
15. Auditor Keamanan Informasi adalah orang yang memiliki kompetensi untuk melakukan Audit Keamanan Informasi.
16. Audit Internal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi internal **[Nama Instansi]**
17. Audit Eksternal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi eksternal **[Nama Instansi]** yang memiliki sertifikasi sebagai Auditor Keamanan Informasi.
18. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
19. Insiden siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam keamanan informasi antara lain namun tidak terbatas pada *web defacement, malware (virus, worm, trojan backdoor* dan *ransomware*), *unauthorized access, data breach*, dan *Distributed Denial of Service* (DDoS).
20. Tim Tanggap Insiden Siber adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
21. Tim Pengelola Sistem Manajemen Keamanan Informasi yang selanjutnya disebut **[Tim SMKI]** adalah sekelompok orang yang bertanggung jawab untuk menyusun, mengkomunikasikan, memastikan, dan memantau pelaksanaan SMKI di **[Nama Instansi]**
22. [dapat ditambahkan sesuai kebutuhan].

Pasal 2

(1) Peraturan **[Pimpinan Instansi]** ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan **[Nama Instansi]**.

(2) Kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) meliputi:

a. penetapan ruang lingkup;
b. penetapan penanggung jawab SMKI;
c. perencanaan;
d. dukungan pengoperasian;
e. kendali keamanan;
f. audit keamanan informasi; dan
g. evaluasi kinerja dan perbaikan berkelanjutan keamanan informasi.

(3) Kendali keamanan sebagaimana diatur pada ayat (2) huruf e terdiri dari :
a. keamanan sumber daya manusia;
b. keamanan aset informasi;
c. keamanan akses;
d. keamanan kriptografi;
e. keamanan fisik dan lingkungan;
f. keamanan operasional;
g. keamanan komunikasi;
h. keamanan pengembangan dan pemeliharaan;
i. keamanan pihak ketiga;
j. manajemen insiden siber;
k. manajemen keberlangsungan layanan informasi; dan
l. pengendalian kepatuhan;

## BAB II
## KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI SPBE

### Bagian Kesatu
### Penetapan Ruang Lingkup

#### Pasal 3

(1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a meliputi:
a. Data dan Informasi SPBE;
b. Aplikasi SPBE;
c. Infrastruktur SPBE; dan
d. sumber daya manusia SPBE.

(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset **[Nama Instansi]** yang harus diamankan dalam SPBE.

Bagian Kedua

Penetapan Penanggung Jawab

Pasal 4

(1) **[Sekretaris Instansi]** berperan sebagai koordinator SPBE selaku penanggung jawab SMKI.

(2) Penetapan penanggung jawab SMKI sebagaimana dimaksud dalam ayat (1) dilaksanakan oleh **[Pimpinan Instansi]**.

(3) Dalam melaksanakan tugas sebagai penanggung jawab SMKI, **[Sekretaris Instansi]** dibantu oleh **[Tim SMKI]** selaku pelaksana teknis keamanan informasi.

Pasal 5

(1) **[Sekretaris Instansi]** bersama dengan **[Tim SMKI]** menjalankan pengelolaan keamanan informasi di **[Nama Instansi]**.

(2) Ketua **[Tim SMKI]** dijabat oleh pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi pada **[Nama Instansi]**.

(3) Ketua **[Tim SMKI]** memiliki kewenangan dalam menentukan komposisi, kualifikasi, dan jumlah anggota tim.

(4) **[Tim SMKI]** ditetapkan oleh **[Pimpinan Instansi]**.

Pasal 6

Unit yang memiliki fungsi pengawasan internal di **[Nama Instansi]** berperan melaksanakan audit internal keamanan informasi.

Pasal 7

(1) **[Sekretaris Instansi]** bertanggung jawab untuk:

a. memastikan pelaksanaan Kebijakan SMKI;

b. menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI **[Nama Instansi]**;

c. menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;

d. memastikan pelaksanaan audit internal keamanan informasi;

e. menetapkan arsitektur keamanan informasi;

f. menetapkan peta rencana 5 (lima) tahunan dan sasaran keamanan informasi setiap tahunnya;

g. melakukan tinjauan secara berkala atas pelaksanaan kebijakan SMKI; dan

h. menyampaikan kinerja pelaksanaan kebijakan SMKI kepada **[Pimpinan Instansi]**.

(2) **[Tim SMKI]** bertanggung jawab untuk:

a. menyusun, mengkomunikasikan, dan memantau pelaksanaan kebijakan SMKI di **[Nama Instansi]**;

b. melakukan analisis kebutuhan keamanan informasi;

c. merumuskan, mengkoordinasikan, dan melaksanakan program kerja dan anggaran keamanan informasi;

d. memastikan seluruh pembangunan /pengembangan aplikasi dan infrastruktur informasi termasuk yang dilakukan oleh Pihak Ketiga, minimal memenuhi Standar Teknis dan Prosedur Keamanan Informasi yang ditetapkan oleh lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber;

e. memastikan peningkatan kesadaran, kepedulian, dan kepatuhan oleh seluruh pegawai terhadap kebijakan, prosedur, dan standar keamanan informasi;

f. memastikan diterapkannya perjanjian menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan (*Non Disclosure Agreement*);

g. mengendalikan dan menjaga kemutakhiran kebijakan, prosedur, dan standar keamanan informasi;

h. memfasilitasi pelaksanaan audit internal dan audit eksternal keamanan informasi;

i. dalam memfasilitasi pelaksanaan audit internal keamanan informasi sebagaimana dimaksud pada ayat (2) huruf h, **[Tim SMKI]** dapat menunjuk pihak yang berkompeten di bidang audit keamanan informasi sebagai konsultan;

j. memastikan diterapkannya manajemen risiko, manajemen insiden siber, dan manajemen aset dalam pelaksanaan pengamanan aset Informasi;

k. mendorong perbaikan penerapan keamanan informasi berdasarkan hasil temuan audit internal dan audit eksternal; dan

l. menyusun laporan evaluasi penerapan Kebijakan SMKI dan menyampaikannya kepada **[Sekretaris Instansi]**.

(3) Analisis kebutuhan keamanan informasi sebagaimana dimaksud pada ayat (2) huruf b diselenggarakan dengan cara:

a. mengidentifikasi aplikasi dan infrastruktur untuk keamanan informasi;

b. mengidentifikasi standar kompetensi personel keamanan informasi; dan
c. mengidentifikasi program peningkatan kompetensi keamanan informasi dan penanggulangan insiden siber.

(4) Unit pengawasan internal bertanggung jawab untuk:
a. Menyusun pedoman audit internal keamanan informasi;
b. menyusun perencanaan audit internal keamanan informasi;
c. melaksanakan kegiatan audit internal keamanan informasi;
d. memberikan rekomendasi perbaikan atas hasil temuan audit internal keamanan informasi;
e. menyusun laporan audit internal keamanan informasi;
f. menyampaikan laporan audit internal keamanan informasi kepada **[Sekretaris Instansi]**.

Bagian Ketiga
Perencanaan Keamanan Informasi

Pasal 8

(1) **[Nama Instansi]** sebagai Penyelenggara SPBE yang merupakan Sistem Elektronik Lingkup Publik, melakukan kategorisasi setiap sistem elektronik yang dimilikinya sebagai salah satu dasar dalam pelaksanaan keamanan informasi.
(2) Penentuan kategorisasi sistem elektronik dilakukan sesuai dengan peraturan perundangan yang ditetapkan oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

Pasal 9

(1) Pelaksanaan keamanan informasi dilakukan dengan memperhatikan berbagai risiko yang dapat mengakibatkan terjadinya kegagalan keamanan informasi di **[Nama Instansi]**.
(2) Dalam melaksanakan perencanaan keamanan informasi, **[Tim SMKI]** melakukan manajemen risiko keamanan informasi yang meliputi:
a. menyusun penilaian risiko keamanan informasi dengan mengidentifikasi ancaman, kerentanan, peluang, dan dampak apabila risiko terjadi;
b. menyusun RTL bersama dengan unit terkait;dan
c. melakukan sosialisasi dan komunikasi RTL kepada para pemilik risiko.
(3) Proses manajemen risiko dilakukan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan jika ada perubahan aset atau

proses bisnis yang berdampak signifikan terhadap profil risiko yang ditetapkan.

Pasal 10

(1) **[Tim SMKI]** menyusun program kerja keamanan informasi berdasarkan RTL sebagai wujud realisasi atas tindak lanjut risiko keamanan informasi.
(2) Program kerja keamanan informasi sebagaimana dimaksud pada ayat (1) paling sedikit meliputi:
    a. edukasi kesadaran keamanan informasi;
    b. penilaian kerentanan keamanan informasi;
    c. peningkatan keamanan informasi;
    d. penanganan insiden siber; dan
    e. audit keamanan informasi.
(3) Program kerja keamanan informasi dituangkan dalam peta rencana keamanan informasi yang disusun untuk periode 5 (lima) tahunan dengan sasaran keamanan informasi yang ditetapkan untuk setiap tahunnya.
(4) Peta rencana keamanan informasi sebagaimana dimaksud pada ayat (3) menjadi bagian dari peta rencana SPBE.

Bagian Keempat
Dukungan Pengoperasian

Pasal 11

(1) **[Sekretaris Instansi]** memberikan dukungan pengoperasian keamanan informasi dengan menyediakan sumber daya manusia keamanan informasi yang berkompeten dan anggaran keamanan informasi.
(2) sumber daya manusia keamanan informasi yang disediakan harus memiliki kompetensi:
    a. keamanan infrastruktur TIK; dan
    b. keamanan aplikasi.
(3) Dalam hal sumber daya manusia keamanan informasi yang disediakan belum memiliki kompetensi memadai, maka **[Sekretaris Instansi]** memfasilitasi peningkatan kompetensi melalui kegiatan pelatihan dan/atau bimbingan teknis.
(4) **[Sekretaris Instansi]** memfasilitasi penyelenggaraan kegiatan kesadaran keamanan informasi bagi pegawai di lingkungan **[Nama Instansi]**.

(5) **[Sekretaris Instansi]** menyediakan anggaran keamanan informasi berdasarkan arsitektur dan peta rencana keamanan informasi yang telah disusun; dan

(6) Anggaran keamanan informasi dibebankan pada DIPA **[Nama Instansi]** atau sumber lainnya yang sah dan tidak mengikat.

Bagian Kelima

Kendali Keamanan

Paragraf 1

Keamanan Sumber Daya Manusia

Pasal 12

(1) Keamanan sumber daya manusia dilakukan untuk mengendalikan sumber daya manusia dalam melaksanakan Kebijakan SMKI.

(2) Keamanan sumber daya manusia di **[Nama Instansi]** dilaksanakan oleh **[Tim SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. mengkomunikasikan peran dan tanggung jawab pelaksanaan Kebijakan SMKI kepada seluruh pegawai dan pihak ketiga yang terlibat dalam pengelolaan dan pengamanan asset informasi;
b. melakukan pembagian tugas dan wewenang (*segregation of duty*) untuk menghindari kesalahan atau pelanggaran;
c. melakukan pemeriksaan data pribadi pegawai dan pihak ketiga yang terlibat dalam pengelolaan dan pengamanan aset informasi;
d. membuat perjanjian tertulis dengan pegawai dan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan informasi yang menyatakan tanggung jawab terhadap keamanan informasi dan sanksi atas pelanggaran keamanan informasi;
e. menghentikan hak penggunaan aset informasi bagi pegawai yang sedang dalam pemeriksaan terkait dengan dugaan pelanggaran keamanan informasi;
f. mencabut hak akses ke aset informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi memiliki kepentingan terhadap aset informasi, dimutasi, atau tidak lagi bekerja di **[Nama Instansi]**;
g. membuat berita acara serah terima terkait penerimaan seluruh aset informasi yang dipergunakan selama bekerja dan

pengembalian seluruh aset informasi bagi pegawai yang berhenti bekerja atau mutasi;

h. memberikan edukasi kesadaran keamanan informasi melalui kegiatan sosialisasi, bimbingan teknis, dan/atau pelatihan mengenai keamanan informasi yang dilaksanakan secara berkala; dan

i. memelihara catatan pelatihan, kompetensi, pengalaman, dan kualifikasi pegawai yang mengelola keamanan informasi.

Paragraf 2

Keamanan Aset Informasi

Pasal 13

(1) Keamanan aset informasi dilakukan untuk mengamankan aset informasi di **[Nama Instansi]** berdasarkan tingkat kritikalitasnya.

(2) Keamanan aset informasi di **[Nama Instansi]** dilakukan oleh **[Tim SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. mengidentifikasi aset informasi dan mendokumentasikannya dalam daftar inventaris aset informasi yang memuat tingkat kritikalitas dan penanggung jawab setiap aset;

b. memberikan label sesuai tingkat kritikalitas;

c. menetapkan pihak-pihak yang dapat mengakses aset informasi;

d. menetapkan aturan penggunaan aset informasi;

e. menempatkan aset informasi di lokasi yang aman guna mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang;

f. penggunaan aset yang dibawa ke luar dari lingkungan Pusat Data atau tempat layanan informasi harus disetujui oleh pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi;

g. perangkat penyimpanan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dimusnahkan;

h. pemusnahan perangkat penyimpanan data harus dilakukan secara aman sesuai prosedur pemusnahan perangkat penyimpanan; dan

i. Melaksanakan manajemen aset TIK sesuai dengan ketentuan manajemen aset TIK yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang Komunikasi dan Informatika.

Paragraf 3

Keamanan Akses

Pasal 14

(1) Keamanan akses dilakukan untuk mengendalikan akses ke aset informasi yaitu memastikan perangkat pengguna yang terhubung ke aset informasi mendapatkan perlindungan keamanan dan tidak diakses oleh pihak yang tidak berhak.

(2) Keamanan akses terhadap aset informasi di **[Nama Instansi]** dilakukan oleh **[Tim SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:
   a. menyusun prosedur pengelolaan hak akses pengguna yang berisi ketentuan akses ke aset informasi sesuai dengan kebutuhan organisasi, persyaratan keamanan, dan peraturan yang berlaku;
   b. mengelola akses pengguna;
   c. mengendalikan akses ke jaringan dan layanan jaringan informasi;
   d. mengendalikan akses ke aplikasi dan sistem informasi;
   e. mengendalikan perangkat kerja jarak jauh;
   f. dalam hal diperlukan adanya akses ke aset informasi berklasifikasi rahasia, dapat dibuat hak akses khusus untuk mengakses sistem informasi berklasifikasi rahasia pada sistem operasi, perangkat penyimpanan (*storage devices*), *file server*, dan aplikasi sensitif;
   g. melakukan pemantauan terhadap akses ke aset informasi;
   h. menghapus akun setiap pegawai dan pihak ketiga yang tidak lagi memiliki kepentingan terhadap akses aset informasi, dimutasi, berhenti, atau telah berakhir kontraknya.

(3) Pengelolaan akses pengguna sebagaimana dimaksud pada ayat (2) huruf b dilakukan dengan cara:
   a. menggunakan akun yang unik untuk setiap pengguna;
   b. memeriksa tingkat akses yang diberikan sesuai dengan tujuan penggunaan;
   c. membatasi dan mengendalikan penggunaan hak akses khusus (jika ada);
   d. mengatur pengelolaan kata sandi pengguna sesuai dengan ketentuan pengelolaan kata sandi di **[Nama Instansi]**;
   e. memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya;

f. memelihara catatan pengguna layanan (*user log*);
g. menonaktifkan akses pengguna yang telah berakhir penugasannya; dan
h. memantau dan mengevaluasi akun dan hak akses secara berkala paling sedikit 1 (satu) kali dalam 6 (enam) bulan.

(4) Pengendalian akses ke jaringan dan layanan jaringan informasi sebagaimana dimaksud pada ayat (2) huruf c dilakukan dengan cara:
a. menerapkan prosedur otorisasi pemberian akses ke jaringan dan layanan jaringan untuk setiap akses ke dalam jaringan internal;
b. akses ke infrastruktur dan aplikasi yang digunakan untuk melakukan diagnosa harus dikontrol dan hanya digunakan untuk pegawai yang bertugas untuk melakukan pengujian, pemecahan masalah, serta pengembangan sistem;
c. memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi;
d. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu; dan
e. melakukan penghentian layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.

(5) Pengendalian akses ke aplikasi dan sistem informasi sebagaimana dimaksud pada ayat (2) huruf d dilakukan dengan cara:
a. akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai dengan peruntukannya dan dikontrol dengan menggunakan sistem manajemen akses pengguna;
b. setiap pengguna harus memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya dan proses otorisasi pengguna harus menggunakan teknik otentikasi yang sesuai untuk memvalidasi identitas pengguna;
c. menggunakan sistem pengelolaan kata sandi sesuai dengan ketentuan pengelolaan kata sandi di **[Nama Instansi]** untuk memastikan kualitas kata sandi yang dibuat pengguna;
d. fasilitas *session time-out* harus diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu;
e. membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia; dan

f. akses ke kode sumber aplikasi dibatasi secara ketat diperuntukkan hanya bagi pihak-pihak yang sah dan berkepentingan melalui hak akses khusus.

(6) Pengendalian perangkat kerja jarak jauh sebagaimana dimaksud pada ayat (2) huruf e dilakukan dengan cara menentukan parameter-parameter keamanan yang harus dipenuhi oleh perangkat kerja jarak jauh yang digunakan dalam mengakses aset informasi, yang terdiri dari namun tidak terbatas pada:

a. *Virtual Private Network* (VPN);
b. *Secure Socket Layer* (SSL); dan/atau
c. *Two Step Authentication*;

(7) Pemberian hak akses khusus sebagaimana dimaksud pada ayat (2) huruf f dilakukan dengan cara:

a. mengidentifikasi hak akses khusus untuk dialokasikan kepada pengguna terkait;
b. memberikan hak akses khusus hanya kepada pengguna sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu;
c. mengelola proses otorisasi dan catatan dari seluruh hak akses khusus; dan
d. memberikan hak akses khusus secara terpisah dari akun yang digunakan untuk kegiatan lainnya.

(8) Pemantauan terhadap akses ke aset informasi sebagaimana dimaksud pada ayat (2) huruf g meliputi:

a. kegagalan akses;
b. penggunaan hak akses tidak wajar;
c. alokasi dan penggunaan hak akses khusus;
d. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
e. penggunaan sumber daya sensitif.

Paragraf 4

Keamanan Kriptografi

Pasal 15

(1) Keamanan kriptografi dilaksanakan untuk memastikan penggunaan kriptografi yang tepat untuk melindungi kerahasiaan, keutuhan, dan keotentikan data dan informasi rahasia dan/atau sangat rahasia yang dikelola dalam perangkat informasi.

(2) Keamanan kriptografi untuk informasi rahasia dan/atau sangat rahasia dilaksanakan oleh **[Tim SMKI]** bekerja sama dengan unit

kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. melakukan klasifikasi informasi yang disimpan dan dikelola dalam perangkat informasi sesuai dengan peraturan yang berlaku; dan
b. menerapkan keamanan kriptografi untuk informasi berklasifikasi rahasia dan/atau sangat rahasia.

(3) Penerapan keamanan kriptografi sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan dengan cara berikut namun tidak terbatas pada:

a. menerapkan jalur komunikasi aman dengan menerapkan *Secure Socket Layer* (SSL) untuk proses otentikasi antara pengguna dengan aplikasi berbasis *website*;
b. menjaga kerahasiaan kata sandi dan menyimpannya dalam basis data dengan mekanisme *hash function*;
c. melindungi kerahasiaan data dan informasi rahasia dan/atau sangat rahasia yang dipertukarkirimkan dan disimpan dalam basis data dengan melakukan enkripsi;
d. menerapkan otentikasi berbasis tanda tangan digital dengan menggunakan sertifikat elektronik yang dikeluarkan oleh Pihak Ketiga Terpercaya; dan
e. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan peraturan perundangan dan/atau rekomendasi dari lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

Paragraf 5

Keamanan Fisik dan Lingkungan

Pasal 16

(1) Keamanan fisik dan lingkungan dilakukan untuk memberikan pelindungan, pemeliharaan, keamanan, dan ketersediaan aset informasi.

(2) Keamanan fisik dan lingkungan dilaksanakan oleh **[Tim SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. menyimpan infrastruktur di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai;
b. akses ke Pusat Data dan/atau area kerja layanan informasi yang berisi data dan/atau informasi rahasia dan/atau sangat

rahasia harus dibatasi dan hanya diberikan kepada pegawai yang memiliki akses;

c. Pihak Ketiga yang memasuki Pusat Data dan/atau area kerja layanan informasi yang berisikan data dan/atau informasi rahasia dan/ atau sangat rahasia harus didampingi oleh pegawai yang ditugaskan sepanjang waktu kunjungan;
d. makanan dan minuman dilarang untuk dibawa masuk ke atau dikonsumsi di dalam ruang *server* Pusat Data;
e. semua area yang digunakan untuk menyimpan aset informasi merupakan area bebas rokok;
f. batas minimum dan maksimum suhu dan kelembaban di dalam ruang *server* Pusat Data harus memenuhi standar yang disyaratkan pabrikan perangkat dan senantiasa dilakukan pengawasan terhadap kondisi suhu dan kelembaban;
g. pengamanan area Pusat Data dan area kerja layanan informasi dilakukan sesuai prosedur keamanan area;
h. pengamanan kantor, ruangan, dan fasilitas kerja sesuai dengan peraturan dan standar keamanan dan keselamatan kerja, termasuk *clear screen policy* dan *clean desk policy*;
i. infrastruktur yang digunakan untuk menjalankan aplikasi dipelihara sesuai dengan buku petunjuk;
j. dalam hal pemeliharaan infrastruktur tidak dapat dilakukan di tempat, maka pemindahan infrastruktur dilakukan berdasarkan persetujuan pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi pada **[Nama Instansi]**;
k. dalam hal pemindahan infrastruktur terdapat data dan/atau informasi berklasifikasi rahasia dan/atau sangat rahasia yang tersimpan pada perangkat tersebut, maka data dan/atau informasi berklasifikasi rahasia dan/atau sangat rahasia tersebut harus dipindahkan terlebih dahulu ke dalam media penyimpanan lain.
l. dalam hal pemeliharaan dilakukan oleh Pihak Ketiga, maka pelaksanaannya dilakukan dengan membuat perjanjian kerja sama yang paling sedikit memuat perjanjian menjaga kerahasiaan, pemeliharaan yang disediakan, dan tingkat kinerja yang harus dipenuhi Pihak Ketiga.
m. infrastruktur beserta perangkat pemulihan dan media penyimpanan data cadangan harus diletakkan di tempat yang aman dengan struktur yang memadai untuk menghindari kerusakan dari hama dan bencana alam;

n. semua infrastruktur harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang diisyaratkan oleh pabrikan infrastruktur;
o. pasokan listrik yang digunakan untuk mengoperasikan infrastruktur harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan atau jangka waktu pengoperasian yang cukup, yang paling sedikit mencakup generator listrik dan *Uniterruptable Power Supply* (UPS) dengan daya yang cukup dan dengan konfigurasi yang dapat memindahkan pasokan listrik tanpa gangguan terhadap infrastruktur;
p. bahan berbahaya dan/atau mudah terbakar di lingkungan **[Nama Instansi]** harus disimpan pada jarak yang aman dari Pusat Data dan area kerja layanan informasi;
q. perangkat pemadam kebakaran harus disediakan, dipelihara, dan diletakkan di tempat yang mudah dijangkau;
r. infrastruktur diletakkan pada lokasi yang meminimalisasi akses pihak yang tidak berwenang;
s. infrastruktur yang menangani informasi sensitif diposisikan dan dibatasi sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak tidak berwenang;
t. perangkat perlindungan petir harus diterapkan untuk semua bangunan, jalur komunikasi, dan listrik;
u. pengamanan kabel di Pusat Data dan/atau area kerja layanan informasi dilakukan dengan mengikuti standar mekanikal/elektrikal Pusat Data yang berlaku.

(3) Penyimpanan infrastruktur di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai sebagaimana dimaksud pada ayat (2) huruf a antara lain namun tidak terbatas pada:
a. pintu dengan kontrol akses;
b. kamera pengawas;
c. pendeteksi asap;
d. sistem pemadam kebakaran; dan
e. perangkat pemutus aliran listrik.

Paragraf 6
Keamanan Operasional

Pasal 17

(1) Keamanan operasional dilakukan untuk memastikan implementasi, operasional, dan pemeliharaan yang aman dari aset informasi,

pengelolaan layanan oleh Pihak Ketiga, meminimalkan risiko kegagalan, dan melindungi keutuhan dan ketersediaan aset informasi.

(2) Keamanan operasional di **[Nama Instansi]** dilakukan oleh **[Tim SMKI]** bekerja sama dengan unit kerja terkait dengan cara sebagai berikut namun tidak terbatas pada:

a. mendokumentasikan, memelihara, dan menyediakan prosedur penggunaan perangkat informasi sesuai dengan peruntukannya;
b. perubahan pada aset informasi yang dapat mempengaruhi keamanan informasi harus didokumentasikan dan dikendalikan dengan manajemen risiko;
c. menetapkan kriteria penerimaan untuk sistem informasi baru, pemutakhiran dan versi baru, serta melakukan pengujian sebelum penerimaan;
d. memantau penggunaan aset informasi yang dimiliki dan membuat proyeksi kebutuhan ke depan untuk menjamin ketersediaan aset informasi yang dibutuhkan. Untuk aset informasi yang kritikal harus senantiasa dimonitor dan dievaluasi kapasitas dan ketersediaannya;
e. melakukan pemisahan akses terhadap informasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia (seorang pegawai dihindari memiliki akses terhadap seluruh aset informasi dan perangkat pengolahnya); dan
f. memisahkan lingkungan pengembangan, pengujian, dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berhak terhadap sistem operasional;
g. menerapkan sistem pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman *malware*.
h. Perlindungan dilakukan dengan cara pemasangan paling sedikit meliputi perangkat *firewall, Intrusion Prevention System* (IPS), antivirus, perangkat manajemen akses pengguna, dan perangkat monitoring/pendukung lainnya sesuai perkembangan teknologi keamanan informasi.
i. melakukan pembuatan *backup* informasi dan aplikasi yang berada di Pusat Data dan/atau area kerja layanan informasi secara berkala sesuai dengan prosedur *backup* di **[Nama Instansi]**;
j. salinan cadangan data/informasi, aplikasi, dan *image* sistem harus diambil dan diuji secara berkala; dan

k. mencatat (*logging*) setiap aktivitas administrator, aktivitas pengguna, peristiwa kegagalan, dan kejadian keamanan serta disimpan dalam periode tertentu.
l. melindungi sistem pencatatan (*log*) dari pemalsuan dan akses yang tidak berwenang;
m. melakukan penilaian kerentanan terhadap perangkat informasi (*vulnerability assessment*) secara berkala dan melakukan tindakan perlindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi;
n. menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindak pengamanan yang tepat;
o. memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati; dan
p. menerapkan audit terhadap *log* yang mencatat aktivitas pengguna dan kejadian keamanan informasi dalam kurun waktu tertentu untuk membantu investigasi di masa mendatang.

(3) Penerapan audit terhadap *log* sebagaimana dimaksud dalam ayat (2) huruf q untuk melihat ha-hal antara lain:
a. kegagalan akses;
b. penggunaan hak akses tidak wajar;
c. alokasi dan penggunaan hak akses khusus;
d. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
e. penggunaan sumber daya sensitif.

Paragraf 7
Keamanan Komunikasi

Pasal 18

(1) Keamanan komunikasi dilakukan untuk memastikan keamanan pertukaran informasi melalui jaringan komunikasi.
(2) Keamanan komunikasi di **[Nama Instansi]** dilakukan oleh **[Tim SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:
a. mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh Pihak Ketiga;

b. dalam hal Pihak Ketiga diizinkan mengakses ke jaringan, maka dilakukan pemantauan serta pencatatan kegiatan selama menggunakan jaringan;
c. melindungi jaringan dari pihak yang tidak berhak mengakses;
d. menerapkan mekanisme kriptografi untuk melindungi informasi yang terdapat dalam aplikasi yang melewati jaringan publik dari upaya pengungkapan, modifikasi, dan perusakan;
e. melakukan pendeteksian dan perlindungan terhadap kode berbahaya (*malicious code*) yang disisipkan pada file yang dikirim melalui sistem elektronik;
f. memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan untuk informasi elektronik berklasifikasi rahasia dan/atau sangat rahasia; dan
g. menetapkan prosedur pertukaran informasi yang mengatur sistem dan keamanan yang digunakan untuk pertukaran informasi.

(3) Pelindungan jaringan dari pihak yang tidak berhak mengakses sebagaimana dimaksud pada ayat (2) huruf c paling sedikit dilaksanakan dengan cara:
a. mendokumentasikan arsitektur jaringan yang meliputi seluruh komponen infrastruktur dan aplikasi jaringan;
b. menerapkan teknologi keamanan jaringan berbasis enkripsi dan otentikasi (termasuk sertifikat elektronik);
c. menerapkan pemisahan jaringan untuk kelompok pengguna, layanan informasi, dan sistem informasi;
d. menerapkan parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan; dan
e. menerapkan prosedur penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.

Paragraf 8

Keamanan Pengembangan dan Pemeliharaan

Pasal 19

(1) Keamanan pengembangan dan pemeliharaan sistem dilakukan untuk memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dalam daur hidup aset informasi untuk mencegah terjadinya kesalahan, eksploitasi, modifikasi, dan perusakan aset informasi oleh pihak yang tidak berwenang.

(2) Keamanan pengembangan dan pemeliharaan di **[Nama Instansi]** dilakukan oleh **[Tim SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. lingkungan pengembangan, pengujian, dan operasional aplikasi harus dipisahkan baik secara fisik, *logic*, maupun aksesnya;
b. menjaga agar lingkungan pengembangan tidak boleh diakses dari sistem operasional layanan;
c. mengupayakan lingkungan pengujian sama dengan lingkungan operasional layanan;
d. memilih data uji dengan hati-hati, melindungi, dan mengendalikannya;
e. mengawasi dan memantau aktivitas pembangunan dan/atau pengembangan aplikasi dan infrastruktur yang dialihdayakan pada pihak ketiga;
f. memastikan bahwa dalam proses perencanaan dan pembangunan dan/atau pengembangan aplikasi dan infrastruktur termasuk yang dilakukan oleh Pihak Ketiga, telah memasukkan fitur-fitur keamanan dalam spesifikasi aplikasi dan infrastruktur yang dibangun dan/atau dikembangkan;
g. fitur-fitur keamanan yang dimasukkan sesuai dengan standar keamanan relevan; dan
h. melaksanakan uji kelaikan aplikasi sebelum aplikasi digunakan dan sewaktu-waktu sesuai kebutuhan.

(3) Fitur-fitur keamanan yang sesuai dengan standar keamanan relevan sebagaimana dimaksud pada ayat (2) huruf g mencakup:

a. standar keamanan data dan informasi;
b. standar keamanan aplikasi;
c. standar keamanan pusat data;
d. standar keamanan sistem penghubung layanan; dan
e. standar keamanan jaringan intra.

(4) Standar keamanan relevan sebagaimana dimaksud pada ayat (3) minimal memenuhi standar keamanan yang ditetapkan oleh lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

(5) Pelaksanaan uji kelaikan aplikasi sebelum aplikasi digunakan dan sewaktu-waktu sesuai kebutuhan sebagaimana dimaksud pada ayat (2) huruf h mencakup aspek:

a. uji fungsi, yaitu pengujian yang memastikan aplikasi yang dibangun dan/atau dikembangkan telah memenuhi fungsi-fungsi sesuai dengan dokumentasi terkait;

b. uji integrasi, yaitu pengujian yang memastikan aplikasi yang dibangun dan/atau dikembangkan telah memenuhi kebutuhan dan persyaratan integrasi dengan aplikasi, data, serta komponen-komponen lain yang terkait;
c. uji beban, yaitu pengujian yang memastikan aplikasi yang dibangun dan/atau dikembangkan dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya;
d. uji keamanan, yaitu pengujian yang memastikan aplikasi yang dibangun dan/atau dikembangkan dapat menjaga keamanan data dan informasi yang terkait dengannya.

(6) uji kelaikan pada aspek uji fungsi, uji integrasi, dan uji beban dapat menggunakan pedoman dan/atau instrumen pengukuran yang ditetapkan oleh Kementerian yang menyelenggarakan tugas pemerintahan di bidang komunikasi dan informatika.

(7) uji kelaikan pada aspek uji keamanan dapat menggunakan pedoman dan/atau instrumen pengukuran yang ditetapkan oleh lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

(8) pelaksanaan pembangunan dan pengembangan aplikasi dilakukan sesuai dengan Standar Teknis dan Prosedur Pembangunan dan Pengembangan Aplikasi yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang Komunikasi dan Informatika.

Paragraf 9

Keamanan Pihak Ketiga

Pasal 20

(1) Keamanan Pihak Ketiga dilakukan untuk memastikan perlindungan dari aset informasi yang dapat diakses oleh Pihak Ketiga.

(2) Keamanan Pihak Ketiga di **[Nama Instansi]** dilakukan oleh **[Tim SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:
a. melakukan pemeriksaan latar belakang Pihak Ketiga dengan tetap memperhatikan privasi dan perlindungan data pribadi;
b. membuat dan meninjau ulang secara berkala perjanjian keamanan dengan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan aset informasi yang menyatakan tanggung jawab terhadap keamanan aset informasi.

c. memastikan secara berkala bahwa pengendalian keamanan informasi, definisi layanan, dan tingkat layanan yang termuat dalam kesepakatan penyediaan layanan, telah diterapkan, dioperasikan, dan dipelihara oleh Pihak Ketiga;
d. memastikan *Service Level Agreement* (SLA) pihak ketiga telah mengatur ketersediaan layanan dan penyelesaian insiden keamanan;
e. melakukan pemantauan terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh Pihak Ketiga secara berkala;
f. memperhatikan kritikalitas, proses yang terkait dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan oleh Pihak Ketiga;
g. mencatat peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan oleh pihak ketiga;
h. memberikan informasi tentang gangguan keamanan dan mengkaji informasi bersama Pihak Ketiga;
i. mencabut hak akses terhadap akses informasi yang dimiliki Pihak Ketiga apabila yang bersangkutan tidak lagi bekerja di **[Nama Instansi]**;
j. membuat berita acara serah terima terkait mengembalikan seluruh aset informasi yang dipergunakan selama bekerja bagi Pihak Ketiga yang berakhir masa kontraknya; dan
k. memastikan Pihak Ketiga dan tamu yang memasuki lingkungan Pusat Data dan tempat layanan informasi harus mematuhi standar keamanan fisik dan lingkungan.

(3) Perjanjian keamanan sebagaimana dimaksud pada ayat (2) huruf b disusun secara tertulis dengan paling sedikit memuat:
a. pelindungan atas informasi rahasia dan/atau sangat rahasia dan hak kekayaan intelektual setiap pihak;
b. dalam hal aset informasi disediakan oleh Pihak Ketiga, maka adanya jaminan bahwa tidak terdapat *malicious code* dan *backdoor*;
c. hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia dan/atau sangat rahasia;
d. pengawasan atas akses terhadap aset informasi yang diberikan pada pihak ketiga;
e. pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan;

f. syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian;
g. penggunaan jalur komunikasi yang aman untuk perpindahan informasi antara **[Nama Instansi]** dengan pihak ketiga; dan
h. dalam hal Pihak Ketiga tidak lagi menjadi bagian dalam pengelolaan aset informasi, maka aset informasi yang dikuasainya diserahkan kembali kepada **[Tim SMKI]**.

Paragraf 10
Manajemen Insiden Siber

Pasal 21

(1) Manajemen insiden siber dilaksanakan untuk mengendalikan insiden siber.
(2) Manajemen insiden siber di **[Nama Instansi]** dilaksanakan oleh **[Tim SMKI]** bekerja sama dengan unit kerja terkait dengan cara sebagai berikut namun tidak terbatas pada:
   a. membentuk Tim Tanggap Insiden Siber (TTIS) yang bertugas melakukan pencegahan dan penanganan insiden siber yang terjadi di **[Nama Instansi]**;
   b. TTIS melakukan tindakan pencegahan insiden siber;
   c. Dalam hal terjadi insiden siber, Tim Tanggap Insiden Siber melaksanakan prosedur penanganan insiden siber;
   d. menyusun skenario penanganan insiden siber;
   e. melakukan simulasi berkala skenario penanganan insiden siber yang telah disusun;
   f. memberikan pelatihan terhadap sumber daya manusia yang terlibat dalam simulasi penanganan insiden siber sesuai skenario yang disusun;
   g. menjalankan program kesadaran ancaman dan penanganan insiden siber, serta ajakan peran aktif pada seluruh pegawai;
   h. memastikan tersedianya kontak pelaporan insiden siber yang dapat diakses oleh seluruh pegawai di lingkungan **[Nama Instansi]** termasuk oleh Pihak Ketiga; dan
   i. melaksanakan pengukuran tingkat kematangan penanganan insiden siber secara berkala.
(3) Tindakan pencegahan insiden siber sebagaimana dimaksud pada ayat (2) huruf b paling sedikit meliputi:
   a. melakukan penilaian kerentanan dan/atau *penetration testing* untuk menemukan celah keamanan pada aset informasi;

b. mengimplementasikan alat monitoring keamanan berupa *Security information and event management* (SIEM); dan
c. melakukan monitoring dan pendeteksian serangan terhadap aset informasi.

(4) Prosedur penanganan insiden siber sebagaimana dimaksud pada ayat (2) huruf c paling sedikit meliputi:
a. menerima laporan dan mencatat insiden siber;
b. melakukan triase insiden siber;
c. mengidentifikasi sumber serangan;
d. menganalisis informasi yang berkaitan dengan insiden siber;
e. memprioritaskan penanganan insiden berdasarkan tingkat dampak;
f. memelihara artefak digital untuk keperluan investigasi;
g. menyusun laporan penanganan insiden siber; dan
h. mengevaluasi dan memperbaiki standar, prosedur, dan kontrol-kontrol keamanan informasi agar insiden siber serupa tidak terulang kembali di masa mendatang.

Paragraf 11
Manajemen Keberlangsungan Layanan Informasi

Pasal 22

(1) Manajemen keberlangsungan layanan informasi dilakukan untuk menjamin ketersediaan layanan informasi pada saat terjadi keadaan darurat.

(2) Manajemen keberlangsungan layanan informasi dilakukan oleh **[Tim SMKI]** bekerja sama dengan unit terkait dengan cara sebagai berikut namun tidak terbatas pada:
a. melakukan identifikasi risiko terhadap keberlangsungan layanan informasi;
b. menyusun dan menerapkan rencana keberlangsungan layanan informasi (*Business Continuity Planning)* untuk menjaga dan mengembalikan operasional aset informasi dalam jangka waktu yang disepakati dan tingkat keberlangsungan yang dibutuhkan;
c. dalam hal aplikasi merupakan aplikasi umum dan/atau sistem elektronik berkategori strategis, maka harus memiliki redundansi yang cukup untuk memenuhi ketersediaan layanan informasi;
d. melakukan uji coba rencana keberlangsungan layanan informasi secara berkala; dan

e. pelaksanaan pengelolaan layanan dilakukan sesuai dengan pedoman manajemen layanan SPBE yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang Komunikasi dan Informatika.

(3) Rencana keberlangsungan layanan informasi sebagaimana dimaksud pada ayat (2) huruf b paling sedikit meliputi:

a. prosedur keberlangsungan layanan informasi pada saat keadaan darurat, manajemen risiko, analisis dampak kegiatan, pengembalian kondisi sebelum terjadi gangguan peralihan kondisi normal, dan uji coba keberlangsungan kegiatan;
b. penetapan peran dan penanggung jawab pegawai yang terlibat dalam pelaksanaan keberlangsungan layanan informasi; dan
c. pelaksanaan sosialisasi dan pelatihan keberlangsungan layanan informasi.

Paragraf 12

Pengendalian Kepatuhan

Pasal 23

(1) Pengendalian kepatuhan dilaksanakan untuk memastikan kepatuhan pegawai dan pihak ketiga dalam melaksanakan keamanan informasi sesuai dengan ketentuan peraturan perundang-undangan, kontrak dan keselarasan dengan kebijakan keamanan informasi yang berlaku di **[Nama Instansi]**.

(2) Pengendalian kepatuhan keamanan informasi di **[Nama Instansi]**, dilakukan oleh **[Tim SMKI]** bekerja sama dengan unit kerja terkait dengan cara sebagai berikut namun tidak terbatas pada:

a. mengidentifikasi, mendokumentasikan, mereviu, dan memelihara regulasi, standar, dan prosedur keamanan informasi;
b. memeriksa kepatuhan seluruh pegawai dan Pihak Ketiga terhadap regulasi, standar, dan prosedur keamanan informasi;
c. mendapatkan aplikasi hanya melalui sumber yang dikenal dan memiliki reputasi baik untuk memastikan tidak ada pelanggaran hak cipta;
d. memeriksa kepatuhan penggunaan lisensi aplikasi dan menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;
e. memelihara bukti kepemilikan lisensi, *master disk*, buku manual, dan lain sebagainya;

f. melakukan pemeriksaan bahwa tidak ada produk bajakan yang terinstal di **[Nama Instansi]**;
g. memastikan rekaman terlindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah, dan rilis tidak sah sesuai dengan persyaratan peraturan perundang-undangan, kontraktual, dan bisnis;
h. memastikan pengamanan privasi dan data pribadi yang dapat diidentifikasikan sesuai dengan persyaratan peraturan perundang-undangan yang berlaku;
i. memastikan kesesuaian penerapan kriptografi dengan peraturan perundang-undangan yang berlaku; dan
j. mereviu sistem informasi secara berkala agar sesuai dengan kebijakan dan standar keamanan informasi di **[Nama Instansi]**.

Bagian Keenam
Audit Keamanan Informasi

Pasal 24

(1) Audit Keamanan Informasi dilaksanakan secara berkala untuk memastikan diterapkannya kebijakan, standar, dan prosedur keamanan informasi.
(2) Audit Keamanan Informasi dilaksanakan melalui kegiatan Audit Internal Keamanan Informasi dan Audit Eksternal Keamanan Informasi.
(3) Audit Internal Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan dengan cara sebagai berikut:
    a. Audit Internal Keamanan Informasi di **[Nama Instansi]** dilaksanakan oleh unit kerja yang melaksanakan tugas dibidang pengawasan internal;
    b. unit kerja yang melaksanakan tugas dibidang pengawasan internal merencanakan, menetapkan, dan menjalankan program audit sesuai dengan pedoman Audit Internal Keamanan Informasi;
    c. program audit minimal mencakup frekuensi, metode, kriteria, lingkup, tanggung jawab, dan pelaporan audit, serta mempertimbangkan pentingnya proses yang sedang berjalan dan hasil audit sebelumnya;
    d. Audit Internal Keamanan Informasi dilaksanakan paling sedikit 1 (satu) kali dalam 2 (dua) tahun dan dimasukkan dalam Peta Rencana SPBE **[Nama Instansi]**;

e. Audit Internal Keamanan Informasi dilaksanakan oleh Auditor yang memiliki kompetensi memadai dan memiliki objektivitas serta imparsialitas (ketidakberpihakan) dalam melaksanakan Audit Internal Keamanan Informasi;
f. setiap temuan audit harus dicatat secara formal oleh Auditor dan diberikan kepada auditan;
g. auditan harus melakukan perbaikan terhadap setiap temuan yang diberikan oleh Auditor dalam jangka waktu yang disepakati;
h. laporan hasil audit keamanan dilaporkan kepada **[Tim SMKI]** dan **[Sekretaris Instansi]** sebagai bahan evaluasi penerapan Kebijakan SMKI;
i. menyimpan dan mendokumentasikan proses dan hasil audit internal sebagai alat bukti dari program audit; dan
j. pelaksanaan audit internal keamanan informasi dapat menggunakan instrumen penilaian Audit Keamanan SPBE yang ditetapkan oleh Kepala Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

(4) Audit Eksternal Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan oleh pihak ketiga sesuai dengan peraturan perundang-undangan yang berlaku.

Bagian Ketujuh

Evaluasi Kinerja dan Perbaikan Berkelanjutan Keamanan Informasi

Pasal 25

(1) Evaluasi kinerja keamanan informasi dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun dalam bentuk tinjauan manajemen untuk memastikan pencapaian target keamanan informasi yang telah direncanakan.
(2) **[Sekretaris Instansi]** dengan dibantu **[Tim SMKI]** melakukan evaluasi kinerja keamanan informasi berdasarkan peta rencana, sasaran keamanan informasi, dan hasil Audit Keamanan Informasi dengan cara sebagai berikut namun tidak terbatas pada:
a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan keamanan informasi;
b. menetapkan indikator kinerja pada setiap area proses;
c. memformulasi pelaksanaan keamanan informasi dengan mengukur secara kuantitatif kinerja yang diharapkan;
d. melakukan evaluasi terhadap pelaksanaan SMKI;
e. menganalisis efektifitas pelaksanaan keamanan informasi; dan

f. mendukung dan merealisasikan program Audit Keamanan Informasi.

(3) Hasil evaluasi kinerja keamanan informasi didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja keamanan informasi berikutnya.

Pasal 26

(1) Perbaikan berkelanjutan merupakan tindak lanjut dari hasil evaluasi kinerja keamanan informasi.

(2) **[Tim SMKI]** melakukan perbaikan berkelanjutan dengan cara sekurang-kurangnya sebagai berikut:

a. mengatasi permasalahan dalam pelaksanaan keamanan informasi; dan

b. memperbaiki pelaksanaan keamanan informasi secara berkala.

(3) Tindakan perbaikan yang telah dilakukan didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja keamanan informasi.

BAB III

KETENTUAN PENUTUP

Pasal 27

Peraturan **[Pimpinan Instansi]** ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan **[Pimpinan Instansi]** ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal
**[PIMPINAN INSTANSI]**,

**[NAMA]**

Diundangkan di **[Lokasi]**
pada tanggal
KEPALA BADAN
PEMBINAAN HUKUM NASIONAL
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

**[NAMA]**

BERITA NEGARA REPUBLIK INDONESIA TAHUN NOMOR

LAMPIRAN II
KEPUTUSAN KEPALA BADAN SIBER DAN SANDI NEGARA
NOMOR : 499 TAHUN 2023
TANGGAL : 8 Agustus 2023

TEMPLAT KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAH BERBASIS ELEKTRONIK BERBENTUK NARASI

**SISTEM MANAJEMEN KEAMANAN INFORMASI**
**[Nama Instansi]**

## BAB I
## PENDAHULUAN

### 1.1 Latar belakang

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) telah mendorong transformasi layanan pemerintahan dari semula dilakukan secara manual menjadi berbasis digital. Transformasi layanan berbasis digital menawarkan berbagai keuntungan antara lain efisiensi, efektifitas, dan akuntabilitas yang tinggi. Namun demikian, transformasi layanan berbasis digital juga menimbulkan risiko baru yaitu munculnya kerentanan dan potensi ancaman terhadap kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan informasi yang dikelola yang diakibatkan oleh berbagai gangguan terhadap sistem yang dimiliki termasuk serangan dan insiden siber.

Keamanan informasi merupakan hal penting yang harus diperhatikan dalam membangun dan menjalankan layanan berbasis digital. Dengan semakin meningkatnya risiko dan insiden siber dalam penyelenggaraan SPBE, maka upaya pengamanan terhadap SPBE harus dilakukan. Data pribadi, infrastruktur, dan aset lainnya yang dimiliki oleh **[Nama Instansi]** harus dapat dikelola dengan baik. Dalam rangka memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan dalam pengelolaan informasi di **[Nama Instansi]**, diperlukan Sistem Manajemen Keamanan Informasi.

Kebijakan Sistem Manajemen Keamanan Informasi disusun sebagai pedoman bagi setiap SDM yang terlibat dalam pengelolaan informasi untuk memastikan terjaganya keamanan informasi. Pedoman ini mengatur proses pengelolaan pengamanan informasi maupun kendali yang diperlukan dalam melakukan pengamanan informasi. Pedoman ini menjadi acuan dalam penyusunan prosedur, petunjuk teknis maupun aturan yang lainnya dalam rangka pengamanan informasi di **[Nama Instansi].**

### 1.2 Tujuan

Kebijakan Sistem Manajemen Keamanan Informasi ini digunakan sebagai pedoman dalam rangka melindungi aset informasi **[Nama Instansi]** dari berbagai bentuk ancaman baik internal maupun eksternal, yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian (*authenticcation*), dan kenirsangkalan (*non-repudiation*) aset informasi selalu terjaga dan terpelihara dengan baik.

### 1.3 Ruang Lingkup

Kebijakan dan standar ini berlaku untuk pengelolaan pengamanan seluruh aset informasi **[Nama Instansi]** yang dilaksanakan oleh SDM yang terlibat baik sebagai

pengguna atau pengelola, instansi pemerintah terkait, mitra kerja, dan pihak ketiga di **[Nama Instansi]**. Cakupan aset informasi meliputi:

a. Data dan Informasi SPBE;
b. Aplikasi SPBE;
c. Infrastruktur SPBE; dan
d. Sumber daya manusia (SDM) SPBE.

**1.4 Pengertian**

a. Teknologi Informasi dan Komunikasi selanjutnya disebut TIK adalah terminologi yang mencakup seluruh peralatan teknis untuk memproses dan menyampaikan informasi.
b. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik
c. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
d. Data adalah tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, teleacopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi.
e. Informasi adalah satu atau sekumpulan Data, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *eletronic data interchange* (EDI), surat elektronik (electronic mail), telegram, teleks, telecopy atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
f. Aplikasi adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan.
g. Infrastruktur adalah semua 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.
h. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko.
i. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersedian, dan kenirsangkalan informasi.
j. Risiko adalah segala kejadian dalam setiap aktivitas yang mungkin timbul karena faktor ketidakpastian, yang mengandung potensi untuk menghambat pencapaian sasaran kinerja dari layanan Sistem Elektronik.
k. Manajemen risiko adalah aktivitas terkoordinasi untuk identifikasi, penilaian, dan penentuan prioritas risiko yang kemudian akan dikelola, dipantau, dan dikontrol untuk mengurangi dampak dan/ atau kemungkinan terjadinya risiko tersebut.
l. *Risk Treatment Plan* (RTP) atau Rencana Tindak Lanjut (RTL) Risiko adalah respon yang direncanakan manajemen untuk menindaklanjuti hasil evaluasi risiko, seperti *mitigate/reduce*, *avoid*, *share/ transfer* atau *accept*.
m. Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
n. Audit Keamanan Informasi adalah Audit TIK cakupan keamanan informasi.

o. Auditor Keamanan Informasi adalah orang yang memiliki kompetensi untuk melakukan Audit Keamanan Informasi.
p. Audit Internal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi internal **[Nama Instansi]**
q. Audit Eksternal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi eksternal **[Nama Instansi]** yang memiliki sertifikasi sebagai Auditor Keamanan Informasi.
r. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh Penyelenggara Sertifikasi Elektronik.
s. Insiden siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam keamanan informasi antara lain namun tidak terbatas pada *web defacement, malware* (*virus, worm, trojan backdoor dan ransomware*), *unauthorized access*, *data breach*, dan *Distributed Denial of Service* (DDoS).
t. Tim Tanggap Insiden Siber adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
u. Tim Pengelola Sistem Manajemen Keamanan Informasi yang selanjutnya disebut **[Tim SMKI]** adalah sekelompok orang yang bertanggung jawab untuk menyusun, mengkomunikasikan, memastikan, dan memantau pelaksanaan SMKI di **[Nama Instansi]**
v. **[dapat ditambahkan sesuai kebutuhan]**

### 1.5 Standar Acuan

Standar yang digunakan sebagai acuan dalam pembuatan SMKI ini adalah:

a. 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;
b. SNI ISO/IEC 27001 – Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi - Persyaratan
c. **[Standar lainnya jika ada]**

# BAB II
# ORGANISASI KEAMANAN INFORMASI

## 2.1 Umum

**[Nama Instansi]** menetapkan, menerapkan, memelihara, dan memperbaiki secara berkelanjutan SMKI. SMKI dijalankan melalui organisasi keamanan informasi yang peran dan tanggung jawabnya ditetapkan melalui pedoman ini.

## 2.2 Peran

1. **[SEKRETARIS]** berperan sebagai Koordinator SPBE selaku penanggung jawab SMKI.
2. **[SEKRETARIS]** dalam menjalankan tugasnya sebagai penanggung jawab SMKI dibantu oleh **[TIM SMKI]** selaku pelaksana teknis keamanan informasi.
3. **[KAPUSDAT]** berperan sebagai Ketua **[TIM SMKI]** dan memiliki kewenangan dalam menentukan komposisi, kualifikasi, dan jumlah anggota tim.
4. **[TIM SMKI]** ditetapkan oleh **[KEPALA/MENTERI]**.
5. **[SEKRETARIS]** bersama dengan **[TIM SMKI]** menjalankan pengelolaan keamanan informasi di **[Nama Instansi]**.
6. **[INSPEKTORAT]** berperan melaksanakan Audit Internal Keamanan Informasi.

## 2.3 Tanggung Jawab

**[SEKRETARIS]** bertanggung jawab untuk:

1. memastikan pelaksanaan Kebijakan SMKI;
2. menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI **[Nama Instansi]**;
3. menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;
4. memastikan pelaksanaan Audit Internal Keamanan Informasi;
5. menetapkan arsitektur keamanan informasi;
6. menetapkan peta rencana 5 (lima) tahunan dan sasaran keamanan informasi setiap tahunnya;
7. melakukan tinjauan secara berkala atas pelaksanaan kebijakan SMKI; dan
8. menyampaikan kinerja pelaksanaan kebijakan SMKI kepada **[KEPALA/MENTERI]**;

**[TIM SMKI]** bertanggung jawab untuk:

1. menyusun, mengkomunikasikan, dan memantau pelaksanaan kebijakan SMKI di **[Nama Instansi]**;
2. melakukan analisis kebutuhan keamanan informasi, yang mencakup:
   a. mengidentifikasi aplikasi dan infrastruktur untuk keamanan informasi;
   b. mengidentifikasi standar kompetensi SDM keamanan informasi;
   c. mengidentifikasi program peningkatan kompetensi keamanan informasi dan penanggulangan insiden siber;
3. merumuskan, mengkoordinasikan, dan melaksanakan program kerja dan anggaran keamanan informasi;
4. memastikan seluruh pembangunan/pengembangan aplikasi dan infrastruktur informasi termasuk yang dilakukan oleh Pihak Ketiga, minimal memenuhi Standar Teknis dan Prosedur Keamanan Informasi yang ditetapkan oleh Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber;
5. memastikan peningkatan kesadaran, kepedulian, dan kepatuhan oleh seluruh pegawai terhadap kebijakan, prosedur, dan standar keamanan informasi;
6. memastikan diterapkannya perjanjian menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan (*Non Disclosure Agreement*);

7. mengendalikan dan menjaga kemutakhiran kebijakan, prosedur, dan standar keamanan informasi;
8. memfasilitasi pelaksanaan audit internal dan audit eksternal keamanan informasi. Dalam memfasilitasi pelaksanaan Audit Internal Keamanan Informasi, **[TIM SMKI]** dapat menunjuk pihak yang berkompeten di bidang audit keamanan informasi sebagai konsultan;
9. memastikan diterapkannya manajemen risiko, manajemen insiden siber, dan manajemen aset dalam pelaksanaan pengamanan aset Informasi;
10. mendorong perbaikan penerapan keamanan informasi berdasarkan hasil temuan audit internal dan audit eksternal; dan
11. menyusun laporan evaluasi penerapan Kebijakan SMKI dan menyampaikannya kepada **[SEKRETARIS].**

**[INSPEKTORAT]** bertanggung jawab untuk:

1. menyusun pedoman Audit Internal Keamanan Informasi;
2. menyusun perencanaan Audit Internal Keamanan Informasi;
3. melaksanakan kegiatan Audit Internal Keamanan Informasi;
4. memberikan rekomendasi perbaikan atas hasil temuan Audit Internal Keamanan Informasi;
5. menyusun laporan Audit Internal Keamanan Informasi;
6. menyampaikan laporan Audit Internal Keamanan Informasi kepada **[SEKRETARIS]**.

# BAB III
# PERENCANAAN KEAMANAN INFORMASI

## 3.1 Kategorisasi Sistem Elektronik

**[Nama Instansi]** sebagai Penyelenggara SPBE yang merupakan Sistem Elektronik Lingkup Publik, melakukan kategorisasi setiap sistem elektronik yang dimilikinya sebagai salah satu dasar dalam pelaksanaan keamanan informasi. Penentuan kategorisasi sistem elektronik dilakukan sesuai dengan peraturan perundangan yang ditetapkan oleh Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

## 3.2 Manajemen Risiko

Pelaksanaan keamanan informasi dilakukan dengan memperhatikan berbagai risiko yang dapat mengakibatkan terjadinya kegagalan keamanan informasi di **[Nama Instansi].** Oleh karenanya, dalam melakukan perencanaan keamanan informasi, **[TIM SMKI]** melakukan manajemen risiko keamanan informasi, yang terdiri dari:

1. menyusun **penilaian risiko keamanan informasi** dengan mengindentifikasi ancaman, kerentanan, peluang, dan dampak apabila risiko terjadi;
2. bersama dengan unit terkait, menyusun **Rencana Tindak Lanjut (RTL)**;
3. melakukan sosialisasi dan komunikasi RTL pada para pemilik risiko.

   Proses manajemen risiko dilakukan secara berkala paling sedikit 1 (satu) kali dalam 1 (satu) tahun dan jika ada perubahan aset atau proses bisnis yang berdampak signifikan terhadap profil risiko yang ditetapkan.

## 3.2 Perencanaan Keamanan Informasi

**[Tim SMKI]** menyusun program kerja keamanan informasi berdasarkan RTL sebagai wujud realisasi atas tindak lanjut risiko keamanan informasi. Program kerja keamanan informasi paling sedikit meliputi:

1. edukasi kesadaran keamanan informasi;
2. penilaian kerentanan keamanan informasi;
3. peningkatan keamanan informasi;
4. penanganan insiden siber; dan
5. audit keamanan informasi.

   Program kerja keamanan informasi dituangkan dalam peta rencana keamanan informasi yang disusun untuk periode 5 (lima) tahunan dengan sasaran keamanan informasi yang ditetapkan untuk setiap tahunnya. Peta rencana keamanan informasi sebagaimana dimaksud menjadi bagian dari peta rencana SPBE.

## BAB IV
## DUKUNGAN PENGOPERASIAN

1. **[SEKRETARIS]** memberikan dukungan pengoperasian keamanan informasi dengan menyediakan SDM keamanan informasi yang berkompeten dan anggaran keamanan informasi.
2. SDM keamanan informasi yang disediakan harus memiliki kompetensi:
   a. Keamanan Infrastruktur TIK; dan
   b. Keamanan Aplikasi
3. Dalam hal SDM keamanan informasi yang disediakan belum memiliki kompetensi memadai, maka **[SEKRETARIS]** memfasilitasi peningkatan kompetensi melalui kegiatan pelatihan dan/atau bimbingan teknis.
4. Memfasilitasi penyelenggaraan kegiatan kesadaran keamanan informasi bagi pegawai di lingkungan **[Nama Instansi]**
5. **[SEKRETARIS]** menyediakan anggaran keamanan informasi berdasarkan arsitektur dan peta rencana keamanan informasi yang telah disusun; dan
6. Anggaran keamanan informasi dibebankan pada DIPA **[Nama Instansi]** atau sumber lainnya yang sah dan tidak mengikat.

## BAB V
## KEAMANAN SDM

Keamanan SDM dilakukan untuk mengendalikan SDM dalam melaksanakan Kebijakan SMKI. Keamanan SDM di **[Nama Instansi]** dilaksanakan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. mengkomunikasikan peran dan tanggung jawab pelaksanaan Kebijakan SMKI kepada seluruh pegawai dan pihak ketiga yang terlibat dalam pengelolaan dan pengamanan aset informasi;
2. melakukan pembagian tugas dan wewenang (*segregation of duty*) untuk menghindari kesalahan atau pelanggaran;
3. melakukan pemeriksaan data pribadi pegawai dan pihak ketiga yang terlibat dalam pengelolaan dan pengamanan aset informasi;
4. membuat perjanjian tertulis dengan pegawai dan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan informasi yang menyatakan tanggung jawab terhadap keamanan informasi dan sanksi atas pelanggaran keamanan informasi;
5. menghentikan hak penggunaan aset informasi bagi pegawai yang sedang dalam pemeriksaan terkait dengan dugaan pelanggaran keamanan informasi;
6. mencabut hak akses ke aset informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi memiliki kepentingan terhadap aset informasi, dimutasi, atau tidak lagi bekerja di **[Nama Instansi];**
7. membuat berita acara serah terima terkait penerimaan seluruh aset informasi yang dipergunakan selama bekerja dan pengembalian seluruh aset informasi bagi pegawai yang berhenti bekerja atau mutasi;
8. memberikan edukasi kesadaran keamanan informasi melalui kegiatan sosialisasi, bimbingan teknis, dan/atau pelatihan mengenai keamanan informasi yang dilaksanakan secara berkala; dan
9. memelihara **catatan pelatihan, kompetensi, pengalaman, dan kualifikasi pegawai** yang mengelola keamanan informasi.

## BAB VI
## KEAMANAN ASET INFORMASI

Keamanan aset informasi dilakukan untuk mengamankan aset informasi di **[Nama Instansi]** berdasarkan tingkat kritikalitasnya. Keamanan aset informasi di **[Nama Instansi]** dilakukan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. mengidentifikasi aset informasi dan mendokumentasikannya dalam **daftar inventaris aset informasi** yang memuat tingkat kritikalitas dan penanggung jawab setiap aset;
2. memberikan label sesuai tingkat kritikalitas;
3. menetapkan pihak-pihak yang dapat mengakses aset informasi;
4. menetapkan **aturan penggunaan aset informasi**;
5. menempatkan aset informasi di lokasi yang aman guna mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang;
6. penggunaan aset yang dibawa ke luar dari lingkungan Pusat Data atau tempat layanan informasi harus disetujui oleh **[KAPUSDAT]**;
7. perangkat penyimpanan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dimusnahkan;
8. pemusnahan perangkat penyimpanan data harus dilakukan secara aman sesuai **Prosedur Pemusnahan Perangkat Penyimpanan**; dan
9. Melaksanakan manajemen aset TIK sesuai dengan ketentuan manajemen aset TIK yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang Komunikasi dan Informatika.

## BAB VII
## KEAMANAN AKSES

Keamanan akses dilakukan untuk mengendalikan akses ke aset informasi yaitu memastikan perangkat pengguna yang terhubung ke aset informasi mendapatkan perlindungan keamanan dan tidak diakses oleh pihak yang tidak berhak. Keamanan akses terhadap aset informasi di **[Nama Instansi]** dilakukan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. menyusun **Prosedur Pengelolaan Hak Akses Pengguna** yang berisi ketentuan akses ke aset informasi sesuai dengan kebutuhan organisasi, persyaratan keamanan, dan peraturan yang berlaku;
2. mengelola akses pengguna dengan cara:
    a. menggunakan akun yang unik untuk setiap pengguna;
    b. memeriksa tingkat akses yang diberikan sesuai dengan tujuan penggunaan;
    c. membatasi dan mengendalikan penggunaan hak akses khusus (jika ada);
    d. mengatur pengelolaan kata sandi pengguna sesuai dengan **Ketentuan Pengelolaan Kata Sandi** di **[Nama Instansi]**;
    e. memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya;
    f. memelihara catatan pengguna layanan (*user log*);
    g. menonaktifkan akses pengguna yang telah berakhir penugasannya; dan
    h. memantau dan mengevaluasi akun dan hak akses secara berkala paling sedikit 1 (satu) kali dalam 6 (enam) bulan.
3. mengendalikan akses ke jaringan dan layanan jaringan informasi dengan cara;
    a. menerapkan **Prosedur Otorisasi Pemberian Akses ke Jaringan dan Layanan Jaringan** untuk setiap akses ke dalam jaringan internal;
    b. akses ke infrastruktur dan aplikasi yang digunakan untuk melakukan diagnosa harus dikontrol dan hanya digunakan untuk pegawai yang bertugas untuk melakukan pengujian, pemecahan masalah, serta pengembangan sistem;
    c. memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi;
    d. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu; dan
    e. melakukan penghentian layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.
4. mengendalikan akses ke aplikasi dan sistem informasi dengan cara;
    a. akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai dengan peruntukannya dan dikontrol dengan menggunakan sistem manajemen akses pengguna;
    b. setiap pengguna wajib memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya dan proses otorisasi pengguna wajib menggunakan teknik otentikasi yang sesuai untuk memvalidasi identitas pengguna;
    c. menggunakan sistem pengelolaan kata sandi sesuai dengan **Ketentuan Pengelolaan Kata Sandi** di **[Nama Instansi]** untuk memastikan kualitas kata sandi yang dibuat pengguna;
    d. fasilitas *session time-out* wajib diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu;
    e. membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia; dan
    f. akses ke kode sumber aplikasi dibatasi secara ketat diperuntukkan hanya bagi pihak-pihak yang sah dan berkepentingan melalui hak akses khusus.

5. mengendalikan perangkat kerja jarak jauh dengan cara menentukan parameter-parameter keamanan yang harus dipenuhi oleh perangkat kerja jarak jauh yang digunakan dalam mengakses aset informasi, yang terdiri dari namun tidak terbatas pada:
   a. *Virtual Private Network* (VPN);
   b. *Secure Socket Layer* (SSL); dan/atau
   c. *Two Step Authentication*;
   6. hak akses khusus dapat dibuat untuk mengakses sistem informasi berklasifikasi rahasia pada sistem operasi, perangkat penyimpanan (*storage devices*), file server, dan aplikasi sensitif, dengan cara:
   a. mengidentifikasi hak akses khusus untuk dialokasikan kepada pengguna terkait;
   b. memberikan hak akses khusus hanya kepada pengguna sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu;
   c. mengelola proses otorisasi dan catatan dari seluruh hak akses khusus; dan
   d. memberikan hak akses khusus secara terpisah dari akun yang digunakan untuk kegiatan lainnya.
7. melakukan pemantauan terhadap akses ke aset informasi meliputi:
   a. kegagalan akses;
   b. penggunaan hak akses tidak wajar;
   c. alokasi dan penggunaan hak akses khusus;
   d. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
   e. penggunaan sumber daya sensitif.
8. menghapus akun setiap pegawai dan pihak ketiga yang tidak lagi memiliki kepentingan terhadap akses aset informasi, dimutasi, berhenti, atau telah berakhir kontraknya.

## BAB VIII
## KEAMANAN KRIPTOGRAFI

Keamanan kriptografi untuk memastikan penggunaan kriptografi yang tepat untuk melindungi kerahasiaan, keutuhan, dan keotentikan data dan informasi rahasia dan/atau sangat rahasia yang dikelola dalam perangkat informasi. Keamanan kriptografi untuk informasi rahasia dan/atau sangat rahasia dilaksanakan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. melakukan klasifikasi informasi yang disimpan dan dikelola dalam perangkat informasi sesuai dengan peraturan yang berlaku.
2. menerapkan keamanan kriptografi untuk informasi berklasifikasi rahasia dan/atau sangat rahasia dengan cara sebagai berikut namun tidak terbatas pada:
    f. menerapkan jalur komunikasi aman dengan menerapkan *Secure Socket Layer* (SSL) untuk proses otentikasi antara pengguna dengan aplikasi berbasis website;
    g. menjaga kerahasiaan kata sandi dan menyimpannya dalam basis data dengan mekanisme *hash function*;
    h. melindungi kerahasiaan data dan informasi rahasia dan/atau sangat rahasia yang dipertukarkirimkan dan disimpan dalam basis data dengan melakukan enkripsi;
    i. menerapkan otentikasi berbasis tanda tangan digital dengan menggunakan sertifikat elektronik yang dikeluarkan oleh Pihak Ketiga Terpercaya; dan
    j. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan peraturan perundangan dan/atau rekomendasi dari Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

## BAB IX
## KEAMANAN FISIK DAN LINGKUNGAN

Keamanan fisik dan lingkungan dilakukan untuk memberikan pelindungan, pemeliharaan, keamanan, dan ketersediaan aset informasi. Keamanan fisik dan lingkungan dilaksanakan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. menyimpan infrastruktur di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain namun tidak terbatas pada:
    a. Pintu dengan kontrol akses;
    b. Kamera pengawas (CCTV);
    c. Pendeteksi asap;
    d. Sistem pemadam kebakaran; dan
    e. Perangkat pemutus aliran listrik.
2. akses ke Pusat Data dan/atau area kerja layanan informasi yang berisi data dan/atau informasi rahasia dan/atau sangat rahasia harus dibatasi dan hanya diberikan kepada pegawai yang memiliki akses;
3. Pihak Ketiga yang memasuki Pusat Data dan/atau area kerja layanan informasi yang berisikan data dan/atau informasi rahasia dan/ atau sangat rahasia harus didampingi oleh pegawai yang ditugaskan sepanjang waktu kunjungan;
4. makanan dan minuman dilarang untuk dibawa masuk ke atau dikonsumsi di dalam ruang *server* Pusat Data;
5. semua area yang digunakan untuk menyimpan aset informasi merupakan area bebas rokok;
6. batas minimum dan maksimum suhu dan kelembaban di dalam ruang *server* Pusat Data harus memenuhi standar yang disyaratkan pabrikan perangkat dan senantiasa dilakukan pengawasan terhadap kondisi suhu dan kelembaban;
7. pengamanan area Pusat Data dan area kerja layanan informasi dilakukan sesuai **Prosedur Keamanan Area**;
8. pengamanan kantor, ruangan, dan fasilitas kerja sesuai dengan peraturan dan standar keamanan dan keselamatan kerja, termasuk *clear screen policy* dan *clean desk policy*;
9. infrastruktur yang digunakan untuk menjalankan aplikasi dipelihara sesuai dengan buku petunjuk;
10. Dalam hal pemeliharaan infrastruktur tidak dapat dilakukan di tempat, maka pemindahan infrastruktur dilakukan berdasarkan persetujuan **[KAPUSDAT]**.
11. Dalam hal pemindahan infrastruktur terdapat data dan/atau informasi berklasifikasi rahasia dan/atau sangat rahasia yang tersimpan pada perangkat tersebut, maka data dan/atau informasi berklasifikasi rahasia dan/atau sangat rahasia tersebut harus dipindahkan terlebih dahulu ke dalam media penyimpanan lain.
12. Dalam hal pemeliharaan dilakukan oleh Pihak Ketiga, maka pelaksanaannya dilakukan dengan membuat perjanjian kerja sama yang paling sedikit memuat perjanjian menjaga kerahasiaan, pemeliharaan yang disediakan, dan tingkat kinerja yang harus dipenuhi Pihak Ketiga.
13. infrastruktur beserta perangkat pemulihan dan media penyimpanan data cadangan wajib diletakkan di tempat yang aman dengan struktur yang memadai untuk menghindari kerusakan dari hama (misal: tikus, semut dan rayap) dan bencana (misal: banjir dan gempa);
14. semua infrastruktur harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang diisyaratkan oleh pabrikan infrastruktur;
15. pasokan listrik yang digunakan untuk mengoperasikan infrastruktur harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan atau jangka waktu pengoperasian yang cukup, yang paling sedikit mencakup generator listrik dan

*Uniterruptable Power Supply* (UPS) dengan daya yang cukup dan dengan konfigurasi yang dapat memindahkan pasokan listrik tanpa gangguan terhadap infrastruktur;

16. bahan berbahaya atau mudah terbakar di lingkunngan **[Nama Instansi]** wajib disimpan pada jarak yang aman dari Pusat Data dan area kerja layanan informasi;
17. perangkat pemadam kebakaran wajib disediakan, dipelihara, dan diletakkan di tempat yang mudah dijangkau;
18. infrastruktur diletakkan pada lokasi yang meminimalisasi akses pihak yang tidak berwenang;
19. infrastruktur yang menangani informasi sensitif diposisikan dan dibatasi sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak tidak berwenang;
20. perlindungan petir harus diterapkan untuk semua bangunan, jalur komunikasi dan listrik.
21. pengamanan kabel di Pusat Data dan/atau area kerja layanan informasi dilakukan dengan mengikuti standar mekanikal/elektrikal Pusat Data yang berlaku.

## BAB X
## KEAMANAN OPERASIONAL

Keamanan operasional dilakukan untuk memastikan implementasi, operasional, dan pemeliharaan yang aman dari aset informasi, pengelolaan layanan oleh Pihak Ketiga, meminimalkan risiko kegagalan, dan melindungi keutuhan dan ketersediaan aset informasi. Keamanan operasional di **[Nama Instansi]** dilakukan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, cara sebagai berikut namun tidak terbatas pada:

1. mendokumentasikan, memelihara, dan menyediakan **Prosedur Penggunaan Perangkat Informasi** sesuai dengan peruntukannya;
2. perubahan pada aset informasi yang dapat mempengaruhi keamanan informasi harus didokumentasikan dan dikendalikan dengan memperhatikan manajemen risiko dan persetujuan dari pemilik aset informasi;
3. menetapkan kriteria penerimaan untuk sistem informasi baru, pemutakhiran dan versi baru serta melakukan pengujian sebelum penerimaan;
4. memantau penggunaan aset informasi yang dimiliki dan membuat proyeksi kebutuhan ke depan untuk menjamin ketersediaan aset informasi yang dibutuhkan. Untuk aset informasi yang kritikal harus senantiasa dimonitor dan dievaluasi kapasitas dan ketersediaannya;
5. melakukan pemisahan akses terhadap informasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia (seorang pegawai dihindari memiliki akses terhadap seluruh aset informasi dan perangkat pengolahnya);
6. memisahkan lingkungan pengembangan, pengujian, dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berhak terhadap sistem operasional;
7. menerapkan sistem pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman *malware*;
8. Perlindungan dilakukan dengan cara pemasangan paling sedikit meliputi:
    a. perangkat *firewall*;
    b. perangkat *Intrusion Prevention System* (IPS);
    c. perangkat antivirus;
    d. perangkat manajemen akses pengguna; dan
    e. perangkat monitoring / pendukung lainnya sesuai perkembangan teknologi keamanan informasi.
9. melakukan pembuatan *backup* informasi dan aplikasi yang berada di Pusat Data dan/atau area kerja layanan informasi secara berkala sesuai dengan **Prosedur *Backup*** di **[Nama Instansi]**;
10. salinan cadangan data/informasi, aplikasi, dan *image* sistem harus diambil dan diuji secara berkala;
11. mencatat (*logging*) setiap aktivitas administrator, aktivitas pengguna, peristiwa kegagalan, dan kejadian keamanan serta disimpan dalam periode tertentu;
12. melindungi sistem pencatatan (*log*) dari pemalsuan dan akses yang tidak berwenang;
13. melakukan penilaian kerentanan terhadap perangkat informasi (*vulnerability assessment*) secara berkala dan melakukan tindakan perlindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi;
14. menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindak pengamanan yang tepat;
15. memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati; dan
16. menerapkan audit terhadap *log* yang mencatat aktivitas pengguna dan kejadian keamanan informasi dalam kurun waktu tertentu untuk membantu investigasi di masa mendatang, antara lain:
    a. kegagalan akses;
    b. penggunaan hak akses tidak wajar;

c. alokasi dan penggunaan hak akses khusus;
d. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
e. penggunaan sumber daya sensitif.

## BAB XI
## KEAMANAN KOMUNIKASI

Keamanan komunikasi dilakukan untuk memastikan keamanan pertukaran informasi melalui jaringan komunikasi. Keamanan komunikasi di **[Nama Instansi]** dilakukan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. **[TIM SMKI]** mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh Pihak Ketiga;
2. dalam hal Pihak Ketiga diizinkan mengakses ke jaringan, maka dilakukan pemantauan serta pencatatan kegiatan selama menggunakan jaringan; dan
3. melindungi jaringan dari pihak yang tidak berhak mengakses, paling sedikit dengan cara:
    a. mendokumentasikan arsitektur jaringan yang meliputi seluruh komponen infrastruktur dan aplikasi jaringan;
    b. menerapkan teknologi keamanan jaringan berbasis enkripsi dan otentikasi (termasuk sertifikat elektronik);
    c. menerapkan pemisahan jaringan untuk kelompok pengguna, layanan informasi, dan sistem informasi;
    d. menerapkan parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan; dan
    e. menerapkan **Prosedur Penggunaan Layanan Jaringan** yang membatasi akses ke layanan jaringan atau aplikasi.
4. menerapkan mekanisme kriptografi untuk melindungi informasi yang terdapat dalam aplikasi yang melewati jaringan publik dari upaya pengungkapan, modifikasi, dan perusakan;
5. melakukan pendeteksian dan perlindungan terhadap kode berbahaya (*malicious code*) yang disisipkan pada file yang dikirim melalui sistem elektronik;
6. memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan untuk informasi elektronik berklasifikasi rahasia dan/atau sangat rahasia; dan
7. menetapkan **Prosedur Pertukaran informasi** yang mengatur sistem dan keamanan yang digunakan untuk pertukaran informasi.

## BAB XII
## KEAMANAN PENGEMBANGAN DAN PEMELIHARAAN

Keamanan pengembangan dan pemeliharaan sistem dilakukan untuk memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dalam daur hidup aset informasi untuk mencegah terjadinya kesalahan, eksploitasi, modifikasi, dan perusakan aset informasi oleh pihak yang tidak berwenang. Keamanan pengembangan dan pemeliharaan di **[Nama Instansi]** dilakukan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. lingkungan pengembangan, pengujian, dan operasional aplikasi harus dipisahkan baik secara fisik, *logic*, maupun aksesnya;
2. menjaga agar lingkungan pengembangan tidak boleh diakses dari sistem operasional layanan;
3. mengupayakan lingkungan pengujian sama dengan lingkungan operasional layanan;
4. memilih data uji dengan hati-hati, melindungi, dan mengendalikannya;
5. mengawasi dan memantau aktivitas pembangunan/pengembangan aplikasi dan infrastruktur yang dialihdayakan pada pihak ketiga;
6. memastikan bahwa dalam proses perencanaan dan pembangunan/pengembangan aplikasi dan infrastruktur termasuk yang dilakukan oleh Pihak Ketiga, telah memasukkan fitur-fitur keamanan dalam spesifikasi aplikasi dan infrastruktur yang dibangun/dikembangkan;
7. fitur-fitur keamanan yang dimasukkan sesuai dengan standar keamanan relevan, yang mencakup:
    a. Standar keamanan data dan informasi;
    b. Standar keamanan aplikasi;
    c. Standar keamanan pusat data;
    d. Standar keamanan sistem penghubung layanan; dan
    e. Standar keamanan jaringan intra.
8. standar keamanan sebagaimana dimaksud pada angka 7 (tujuh) minimal memenuhi standar keamanan yang ditetapkan oleh Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.
9. melaksanakan uji kelaikan aplikasi sebelum aplikasi digunakan dan sewaktu-waktu sesuai kebutuhan, yang mencakup aspek:
    a. uji fungsi, dilakukan untuk memastikan aplikasi yang dibangun dan/atau dikembangkan telah memenuhi fungsi-fungsi sesuai dengan dokumentasi terkait;
    b. uji integrasi, dilakukan untuk yang memastikan aplikasi yang dibangun dan/atau dikembangkan telah memenuhi kebutuhan dan persyaratan integrasi dengan aplikasi, data, serta komponen-komponen lain yang terkait;
    c. uji beban, dilakukan untuk yang memastikan aplikasi yang dibangun dan/atau dikembangkan dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya;
    d. uji keamanan, dilakukan untuk memastikan aplikasi yang dibangun dan/atau dikembangkan dapat menjaga keamanan data dan informasi yang terkait dengannya.
10. uji kelaikan pada aspek uji fungsi, uji integrasi, dan uji beban dapat menggunakan pedoman/instrumen pengukuran yang ditetapkan oleh Kementerian yang menyelenggarakan tugas pemerintahan di bidang komunikasi dan informatika;
11. uji kelaikan pada aspek uji keamanan dapat menggunakan pedoman/instrumen pengukuran yang ditetapkan oleh Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber; dan
12. pelaksanaan pembangunan dan pengembangan aplikasi dilakukan sesuai dengan Standar Teknis dan Prosedur Pembangunan dan Pengembangan Aplikasi yang

ditetapkan oleh Kementerian yang melaksanakan tugas di bidang Komunikasi dan Informatika.

## BAB XIII
## KEAMANAN PIHAK KETIGA

Keamanan Pihak Ketiga dilakukan untuk memastikan perlindungan dari aset informasi yang dapat diakses oleh Pihak Ketiga. Keamanan Pihak Ketiga di **[Nama Instansi]** dilakukan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. melakukan pemeriksaan latar belakang Pihak Ketiga dengan tetap memperhatikan privasi dan perlindungan data pribadi;
2. membuat dan meninjau ulang secara berkala **perjanjian keamanan dengan pihak ketiga** yang terlibat dalam penggunaan dan/atau pengelolaan aset informasi yang menyatakan tanggung jawab terhadap keamanan aset informasi. Perjanjian keamanan sebagaimana dimaksud dibuat secara tertulis paling sedikit memuat:
    a. perlindungan atas informasi rahasia dan/atau sangat rahasia dan hak kekayaan intelektual setiap pihak;
    b. dalam hal aset informasi disediakan oleh Pihak Ketiga, maka adanya jaminan bahwa tidak terdapat *malicious code* dan *backdoor*;
    c. hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia dan/atau sangat rahasia;
    d. pengawasan atas akses terhadap aset informasi yang diberikan pada pihak ketiga;
    e. pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan;
    f. syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian;
    g. penggunaan jalur komunikasi yang aman untuk perpindahan informasi antara **[Nama Instansi]** dengan pihak ketiga; dan
    h. dalam hal Pihak Ketiga tidak lagi menjadi bagian dalam pengelolaan aset informasi, maka aset informasi yang dikuasainya diserahkan kembali kepada **[Tim SMKI]**.
3. memastikan secara berkala bahwa pengendalian keamanan informasi, definisi layanan, dan tingkat layanan yang termuat dalam kesepakatan penyediaan layanan, telah diterapkan, dioperasikan, dan dipelihara oleh Pihak Ketiga;
4. memastikan *Service Level Agreement* (SLA) pihak ketiga telah mengatur ketersediaan layanan dan penyelesaian insiden keamanan;
5. melakukan pemantauan terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh Pihak Ketiga secara berkala;
6. memperhatikan kritikalitas, proses yang terkait dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan oleh Pihak Ketiga;
7. mencatat peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan oleh pihak ketiga;
8. memberikan informasi tentang gangguan keamanan dan mengkaji informasi bersama Pihak Ketiga;
9. mencabut hak akses terhadap akses informasi yang dimiliki Pihak Ketiga apabila yang bersangkutan tidak lagi bekerja di **[Nama Instansi]**;
10. membuat berita acara serah terima terkait mengembalikan seluruh aset informasi yang dipergunakan selama bekerja bagi Pihak Ketiga yang berakhir masa kontraknya; dan
11. memastikan Pihak Ketiga dan tamu yang memasuki lingkungan Pusat Data, dan tempat layanan informasi harus mematuhi standar keamanan fisik dan lingkungan.

## BAB XIV
## MANAJEMEN INSIDEN SIBER

Manajemen insiden siber dilaksanakan untuk mengendalikan insiden siber. Manajemen insiden siber di **[Nama Instansi]** dilakukan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. membentuk Tim Tanggap Insiden siber (TTIS) yang bertugas melakukan pencegahan dan penanganan insiden siber yang terjadi di **[Nama Instansi]**;
2. Tim Tanggap Insiden siber melakukan tindakan pencegahan insiden siber paling sedikit meliputi:
    a. melakukan penilaian kerentanan dan/atau *penetration testing* untuk menemukan celah keamanan pada aset informasi;
    b. mengimplementasikan alat monitoring keamanan berupa *Security information and event management* (SIEM); dan
    c. melakukan monitoring dan pendeteksian serangan terhadap aset informasi.
3. Dalam hal terjadi insiden siber, Tim Tanggap Insiden siber melaksanakan **Prosedur Penanganan Insiden siber** paling sedikit meliputi:
    a. menerima laporan dan mencatat insiden siber;
    b. melakukan triase insiden siber;
    c. mengidentifikasi sumber serangan;
    d. menganalisis informasi yang berkaitan dengan insiden siber;
    e. memprioritaskan penanganan insiden berdasarkan tingkat dampak;
    f. memelihara artefak digital untuk keperluan investigasi;
    g. menyusun laporan penanganan insiden siber; dan
    h. mengevaluasi dan memperbaiki standar, prosedur, dan kontrol-kontrol keamanan informasi agar insiden siber serupa tidak terulang kembali di masa mendatang.
4. menyusun berbagai macam skenario penanganan insiden siber;
5. melakukan simulasi secara berkala skenario penanganan insiden siber yang telah disusun;
6. memberikan pelatihan terhadap SDM yang terlibat pada penanganan insiden siber sesuai skenario yang disusun;
7. menjalankan program kesadaran ancaman dan penanganan insiden siber, serta ajakan peran aktif pada seluruh pegawai;
8. memastikan tersedianya kontak pelaporan insiden siber yang dapat diakses oleh seluruh pegawai di **[Nama Instansi]** termasuk oleh pihak ketiga; dan
9. melakukan pengukuran tingkat kematangan penanganan insiden siber secara berkala.

## BAB XV
## MANAJEMEN KEBERLANGSUNGAN LAYANAN INFORMASI

Manajemen keberlangsungan layanan informasi dilakukan untuk menjamin ketersediaan layanan informasi pada saat terjadi keadaan darurat. Manajemen keberlangsungan layanan informasi dilakukan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. melakukan identifikasi risiko terhadap keberlangsungan layanan informasi;
2. menyusun dan menerapkan rencana keberlangsungan layanan informasi (*Business Continuity Planning)* untuk menjaga dan mengembalikan operasional aset informasi dalam jangka waktu yang disepakati dan tingkat keberlangsungan yang dibutuhkan;
3. rencana keberlangsungan layanan informasi paling sedikit meliputi:

a. **Prosedur Keberlangsungan Layanan informasi** pada saat keadaan darurat, manajemen risiko, analisis dampak kegiatan, pengembalian kondisi sebelum terjadi gangguan peralihan kondisi normal, dan uji coba keberlangsungan kegiatan;
b. penetapan peran dan penanggung jawab pegawai yang terlibat dalam pelaksanaan keberlangsungan layanan informasi;
c. pelaksanaan sosialisasi dan pelatihan keberlangsungan layanan informasi;

4. jika aplikasi merupakan aplikasi umum/sistem elektronik berkategori strategis, maka harus memiliki redundansi yang cukup untuk memenuhi ketersediaan layanan informasi;
5. melakukan uji coba rencana keberlangsungan layanan informasi secara berkala; dan
6. pelaksanaan pengelolaan layanan dilakukan sesuai dengan pedoman manajemen layanan SPBE yang ditetapkan oleh Kementerian yang melaksanakan tugas di bidang Komunikasi dan Informatika.

## BAB XVI
## PENGENDALIAN KEPATUHAN

Pengendalian kepatuhan dilaksanakan untuk memastikan kepatuhan pegawai dan Pihak Ketiga dalam melaksanakan keamanan informasi sesuai dengan ketentuan peraturan perundang-undangan, kontrak dan keselarasan dengan kebijakan keamanan informasi yang berlaku di **[Nama Instansi]**. Pengendalian kepatuhan keamanan informasi di **[Nama Instansi]**, dilakukan oleh **[TIM SMKI]** bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. mengidentifikasi, mendokumentasikan, mereviu, dan memelihara regulasi, standar, dan prosedur keamanan informasi;
2. memeriksa kepatuhan seluruh pegawai dan Pihak Ketiga terhadap regulasi, standar, dan prosedur keamanan informasi;
3. mendapatkan aplikasi hanya melalui sumber yang dikenal dan memiliki reputasi baik untuk memastikan tidak ada pelanggaran hak cipta;
4. memeriksa kepatuhan penggunaan lisensi aplikasi dan menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;
5. memelihara bukti kepemilikan lisensi, *master disk*, buku manual, dan lain sebagainya;
6. melakukan pemeriksaan bahwa tidak ada produk bajakan yang terinstal (pelanggaran hak kekayaan intelektual) di **[Nama Instansi]**;
7. memastikan rekaman terlindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah, dan rilis tidak sah sesuai dengan persyaratan peraturan perundang-undangan, kontraktual, dan bisnis;
8. memastikan pengamanan privasi dan data pribadi yang dapat diidentifikasikan sesuai dengan persyaratan peraturan perundang-undangan yang berlaku;
9. memastikan kesesuaian penerapan kriptografi dengan peraturan perundang-undangan yang berlaku;
10. mereviu sistem informasi secara berkala agar sesuai dengan kebijakan dan standar keamanan informasi di **[Nama Instansi]**.

## BAB XVII
## AUDIT KEAMANAN INFORMASI

Audit keamanan informasi dilaksanakan secara berkala untuk memastikan diterapkannya kebijakan, standar, dan prosedur keamanan informasi. Audit keamanan informasi dilaksanakan melalui kegiatan Audit Internal Keamanan Informasi dan Audit Eksternal keamanan informasi yang dilaksanakan dengan cara sebagai berikut namun tidak terbatas pada:

1. Audit Internal Keamanan Informasi
    a. Audit Internal Keamanan Informasi di **[Nama Instansi]** dilaksanakan oleh **[INSPEKTORAT]**;
    b. **[INSPEKTORAT]** merencanakan, menetapkan, dan menjalankan program audit sesuai dengan pedoman Audit Internal Keamanan Informasi;
    c. Program audit minimal mencakup frekuensi, metode, kriteria, lingkup, tanggung jawab, dan pelaporan audit, serta mempertimbangkan pentingnya proses yang sedang berjalan dan hasil audit sebelumnya;
    d. Audit Internal Keamanan Informasi dilaksanakan paling sedikit 1 (satu) kali dalam 2 (dua) tahun dan dimasukkan dalam Peta Rencana SPBE **[Nama Instansi]**;
    e. Audit Internal Keamanan Informasi dilaksanakan oleh Auditor yang memiliki kompetensi memadai dan memiliki objektivitas serta imparsialitas (ketidakberpihakan) dalam melaksanakan Audit Internal Keamanan Informasi;
    f. Setiap temuan audit harus dicatat secara formal oleh Auditor dan diberikan kepada auditan;
    g. Auditan harus melakukan perbaikan terhadap setiap temuan yang diberikan oleh Auditor dalam jangka waktu yang disepakati;
    h. **Laporan Hasil Audit Keamanan Informasi** dilaporkan kepada **[TIM SMKI]** dan **[SEKRETARIS]** sebagai bahan evaluasi penerapan Kebijakan SMKI;
    i. Menyimpan dan mendokumentasikan proses dan hasil audit internal sebagai alat bukti dari program audit; dan
    j. Pelaksanaan Audit Internal Keamanan Informasi dapat menggunakan instrumen penilaian Audit Keamanan SPBE yang ditetapkan oleh Kepala Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

2. Audit Eksternal Keamanan Informasi
    Audit Eksternal Keamanan Informasi di **[Nama Instansi]** dilaksanakan oleh Pihak Ketiga sesuai dengan peraturan perundang-undangan yang berlaku.

## BAB XVIII
## EVALUASI KINERJA DAN PERBAIKAN BERKELANJUTAN KEAMANAN INFORMASI

### 18.1 Evaluasi Kinerja

Evaluasi kinerja keamanan informasi dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun dalam bentuk tinjauan manajemen untuk memastikan pencapaian target keamanan informasi yang telah direncanakan. **[SEKRETARIS]** dengan dibantu **[TIM SMKI]** melakukan evaluasi kinerja keamanan informasi berdasarkan peta rencana, sasaran keamanan informasi, dan hasil audit keamanan informasi dengan cara sebagai berikut namun tidak terbatas pada:

1. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan keamanan informasi;
2. menetapkan indikator kinerja pada setiap area proses;
3. memformulasi pelaksanaan keamanan informasi dengan mengukur secara kuantitatif kinerja yang diharapkan;
4. melakukan evaluasi terhadap penyelenggaraan atau pelaksanaan SMKI;
5. menganalisis efektifitas pelaksanaan keamanan informasi; dan
6. mendukung dan merealisasikan program Audit Keamanan Informasi.

**Hasil evaluasi kinerja keamanan informasi** didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja keamanan informasi berikutnya.

### 18.2 Perbaikan Berkelanjutan Keamanan Informasi

Perbaikan berkelanjutan merupakan tindak lanjut dari hasil evaluasi kinerja keamanan informasi. **[TIM SMKI]** melakukan perbaikan berkelanjutan dengan cara sekurang-kurangnya sebagai berikut:

1. mengatasi permasalahan dalam pelaksanaan keamanan informasi;
2. memperbaiki pelaksanaan keamanan informasi secara berkala.

**Tindakan perbaikan yang telah dilakukan** didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja keamanan informasi.

Legenda:

| | | |
|---|---|---|
| [KEPALA/MENTERI] | : | Nama jabatan pimpinan Instansi Pemerintah |
| [SEKRETARIS] | : | Nama jabatan Sekretaris Instansi Pemerintah |
| [KAPUSDAT] | : | Nama jabatan setingkat Eselon II yang melaksanakan tugas di bidang keamanan TIK |
| [TIM SMKI] | : | Nama Tim / Satuan Tugas Manajemen keamanan informasi |
| **[INSPEKTORAT]** | : | Nama Unit Kerja / Satuan Kerja yang melaksanakan tugas di bidang audit |