DEWAN KETAHANAN NASIONAL RI
SEKRETARIAT JENDERAL

PERATURAN SEKRETARIAT JENDERAL DEWAN KETAHANAN NASIONAL
NOMOR 10 TAHUN 2023
TENTANG
KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN SEKRETARIAT JENDERAL DEWAN KETAHANAN NASIONAL

DENGAN RAHMAT TUHAN YANG MAHA ESA
SEKRETARIS JENDERAL DEWAN KETAHANAN NASIONAL,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 41 ayat Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menetapkan Peraturan Sekretariat Jenderal Dewan Ketahanan Nasional tentang Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional.

Mengingat :

1. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
2. Keputusan Presiden Nomor 101 Tahun 1999 tentang Dewan Ketahanan Nasional dan Sekretariat Jenderal Dewan Ketahanan Nasional;
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
4. Peraturan 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 Tahun 2021 Nomor 541);

5. Peraturan Sekretariat Jenderal Dewan Ketahanan Nasional Nomor 80 Tahun 2020 tentang Struktur Organisasi dan Tata Kerja Sekretariat Jenderal Dewan Ketahanan Nasional;

MEMUTUSKAN:

Menetapkan : PERATURAN SEKRETARIAT JENDERAL DEWAN KETAHANAN NASIONAL TENTANG KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN SEKRETARIAT JENDERAL DEWAN KETAHANAN NASIONAL.

Pasal 1

Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional dimaksudkan sebagai acuan dalam melindungi aset informasi Sekretariat Jenderal Dewan Ketahanan Nasional dari berbagai bentuk ancaman baik dari dalam maupun dari luar, dengan tujuan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.

Pasal 2

Ruang lingkup Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional sebagaimana dimaksud dalam Pasal 1 terdiri atas:

1. Pendahuluan;
2. Organisasi Keamanan Informasi;
3. Perencanaan Keamanan Informasi;
4. Dukungan Pengoperasian;
5. Keamanan Sumber Daya Manusia;
6. Keamanan Aset;
7. Keamanan Akses;
8. Keamanan Fisik dan Lingkungan;
9. Keamanan Kriptografi;
10. Keamanan Operasional;
11. Keamanan Komunikasi;
12. Keamanan Pengembangan dan Pemeliharaan;

13. Keamanan Dengan Institusi Lain;
14. Keamanan Informasi Dalam Pengelolaan Kelangsungan Layanan Informasi;
15. Manajemen Insiden Siber; dan
16. Pengendalian Kepatuhan.

Pasal 3

Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional sebagaimana dimaksud dalam Pasal 2 tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Sekretariat Jenderal Dewan Ketahanan Nasional ini.

Pasal 4

Perturan Sekretariat Jenderal Dewan Ketahanan Nasional ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 22 September 2023

SEKRETARIS JENDERAL
DEWAN KETAHANAN NASIONAL,

DADI HARTANTO

LAMPIRAN
KEPUTUSAN SEKRETARIS JENDERAL DEWAN KETAHANAN NASIONAL
NOMOR 10 TAHUN 2023
TENTANG KEBIJAKAN DAN STANDAR SISTEM KEAMANAN INFORMASI DI LINGKUNGAN SEKRETARIAT JENDERAL DEWAN KETAHANAN NASIONAL

KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN SEKRETARIAT JENDERAL DEWAN KETAHANAN NASIONAL

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 Sekretariat Jenderal Dewan Ketahanan Nasional atau harus dapat dikelola dengan baik. Dalam rangka memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan dalam pengelolaan informasi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional, diperlukan Sistem Manajemen Keamanan Informasi.

Kebijakan Sistem Manajemen Keamanan Informasi disusun sebagai pedoman bagi setiap personel 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 Sekretariat Jenderal Dewan Ketahanan Nasional.

1.2. Tujuan

Kebijakan Sistem Manajemen Keamanan Informasi ini digunakan sebagai pedoman dalam rangka melindungi aset informasi Sekretariat Jenderal Dewan Ketahanan Nasional 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 Sekretariat Jenderal Dewan Ketahanan Nasional yang dilaksanakan oleh personel yang terlibat baik sebagai pengguna atau pengelola, instansi pemerintah terkait, mitra kerja, dan pihak ketiga di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional. Cakupan aset informasi meliputi:

a. Data dan Informasi;
b. Aplikasi;
c. Infrastruktur; dan
d. Sumber Daya Manusia.

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, 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. Data pribadi adalah data yang berkenaan dengan ciri seseorang, nama, umur, jenis kelamin, pendidikan, pekerjaan, alamat, dan kedudukan dalam keluarga.

i. 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.

j. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersedian, dan kenirsangkalan informasi.

k. 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.

l. 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.

m. *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.*

n. 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.

o. Audit Keamanan Informasi adalah Audit TIK cakupan keamanan informasi.

p. Auditor Keamanan Informasi adalah orang yang memiliki kompetensi untuk melakukan Audit Keamanan Informasi.

q. Audit Internal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi internal Sekretariat Jenderal Dewan Ketahanan Nasional.

r. Audit Eksternal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi eksternal Sekretariat Jenderal Dewan Ketahanan Nasional yang memiliki sertifikasi sebagai Auditor Keamanan Informasi.

s. Routing adalah suatu proses pada paket yang meneruskan jaringan dari satu jaringan ke jaringan lainnya melalui internet.

t. *System administrator* adalah orang yang bertanggung jawab untuk mengelola sistem, memelihara dan juga mengoperasikan sistem server.

u. *Database administrator* adalah orang yang mengelola data; dan menjaga keberadaan seluruh data di dalamnya.

v. *Network administrator* adalah orang yang bertugas melakukan konfigurasi, pemeliharaan, dan monitoring jaringan.

w. *Secure areas* adalah daerah yang aman.

x. *clear screen policy* adalah mengunci layar komputer ketika meninggalkan meja kerja dan melakukan *log off* bila pergi untuk jangka waktu lama.

y. *clean desk policy* adalah langkah pengamanan data dan informasi dengan menyimpan seluruh informasi yang bersifat sensitif dan rahasia dengan baik.

z. *conduit* adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.

aa. *Fallback* adalah suatu tindakan pembalikan/ menarik diri dari posisi awal.

bb. *Backup* adalah proses membuat data cadangan dengan cara menyalin atau membuat arsip data komputer sehingga data tersebut dapat digunakan kembali apabila terjadi kerusakan atau kehilangan.

cc. 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.

dd. 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).

ee. Tim Tanggap Insiden Siber adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.

ff. *Denial of Service* adalah suatu kondisi dimana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang tidak terkendali baik dari dalam maupun dari luar sistem.

gg. Kata sandi adalah serangkaian kode yang dibuat Pengguna, bersifat rahasia dan pribadi digunakan bersamaan dengan Akun Pengguna.

hh. *malicious code* adalah semua macam program yang membahayakan termasuk makro atau *script* yang dapat diesekusi dan dibuat dengan tujuan untuk merusak sistem komputer.

1.5. Standar Acuan

Standar yang digunakan sebagai acuan dalam pembuatan SMKI ini adalah:

a. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dan Penyelenggaraan Sistem Elektronik;

b. 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;

c. SNI ISO/IEC 27001 – Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Persyaratan; dan

d. Standar Operasional Prosedur Perangkat Keras dan Petunjuk Pengoperasian Perangkat Lunak.

BAB II
ORGANISASI KEAMANAN INFORMASI

2.1. Umum

Sekretariat Jenderal Dewan Ketahanan Nasional 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. Ruang Lingkup

Kebijakan dan standar organisasi keamanan informasi meliputi:

1. Struktur Tim Keamanan Informasi di Pusat Data dan Informasi;
2. Perjanjian kerahasiaan;
3. Pemisahan tugas;
4. Hubungan dengan pihak berwenang, komunitas keamanan informasi, dan pihak ketiga;
5. Keamanan informasi pada pemeliharaan infrastruktur sistem informasi;
6. Pengendalian terhadap *Mobile Device* dan *Teleworking.*

2.3. Kebijakan

1. Struktur Tim Keamanan Informasi Pusat Data dan Informasi Sekretariat Jenderal Dewan Ketahanan Nasional

   Struktur Tim Keamanan lnformasi Pusat Data dan Informasi Sekretariat Jenderal Dewan Ketahanan Nasional berikut tanggung jawab dan wewenangnya diuraikan dalam standar organisasi keamanan informasi.
2. Tanggung Jawab dan Wewenang

   Tanggung jawab dan wewenang Tim Keamanan Informasi Pusat Data dan Informasi Sekretariat Jenderal Dewan Ketahanan Nasional dapat dipetakan dalam jabatan struktural dan/ atau diperankan oleh Pejabat struktural dan/ atau Pejabat fungsional.
3. Perjanjian Kerahasiaan

   Pusat Data dan Informasi Sekretariat Jenderal Dewan Ketahanan Nasional mengidentifikasi dan mengkaji secara berkala persyaratan untuk menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan.

Perjanjian kerahasiaan harus memuat unsur-unsur sebagai berikut:

a. Definisi dari informasi yang akan dilindungi;
b. Durasi yang diharapkan dari sebuah perjanjian kerahasiaan;
c. Tanggung jawab dan tindakan penanda-tangan utuk menghindari pengungkapan informasi secara tidak sah;
d. Perlindungan kepemilikan informasi, rahasia organisasi, dan kekayaan intelektual;
e. Izin menggunakan informasi rahasia, dan hak-hak penandatangan untuk menggunakan informasi;
f. Hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia;
g. Proses untuk pemberitahuan dan pelaporan dari penyingkapan yang dilakukan secara tidak sah atas pelanggaran terhadap kerahasiaan informasi;
h. Tindakan yang diperlukan pada saat sebuah perjanjian kerahasiaan diakhiri;
i. Syarat-syarat informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian; dan
j. Tindakan yang akan diambil apabila terjadi pelanggaran terhadap perjanjian ini.

4. Pemisahan tugas

   Bagian Sistem Informasi Sekretariat Jenderal Dewan Ketahanan Nasional harus melakukan pemisahan tugas untuk proses yang melibatkan informasi yang memiliki klasifikasi rahasia dan sangat rahasia untuk menghindari adanya pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya.

5. Hubungan dengan Pihak Berwenang

   Bagian Sistem Informasi Sekretariat Jenderal Dewan Ketahanan Nasional mengidentifikasi dan menjalin kerjasama dengan pihak-pihak berwenang di luar Sekretariat Jenderal Dewan Ketahanan Nasional yang terkait dengan keamanan informasi.

6. Hubungan dengan Komunitas Keamanan Informasi

   Bagian Sistem Informasi Sekretariat Jenderal Dewan Ketahanan Nasional menjalin kerjasama dengan komunitas keamanan informasi di luar Bagian Sistem Informasi Sekretariat Jenderal Dewan Ketahanan Nasional melalui pelatihan, seminar, atau forum lain yang relevan dengan keamanan informasi.

7. Keamanan Informasi pada Pemeliharaan Infrastruktur Sistem Informasi

   Pengendalian terhadap keamanan informasi harus diterapkan dalam pemeliharaan infrastruktur sistem informasi dan harus diaplikasikan pada seluruh fase dalam metodologi pengelolaan pemeliharaan.

8. Pengendalian terhadap *Mobile Device* dan *Teleworking*

   a. Pusat Data dan Informasi Sekretariat Jenderal Dewan Ketahanan Nasional membangun kepedulian pengguna perangkat *mobile device* dan *teleworking* akan risiko-risiko keamanan yang terus meningkat terhadap informasi yang tersimpan dalam perangkat *mobile device*; dan

   b. Pengguna perangkat *mobile device* dan *teleworking* harus mengikuti prosedur yang terkait penggunaan perangkat *mobile device* dan *teleworking* untuk menjaga keamanan perangkat dan informasi di dalamnya.

2.4. Peran

1. Kepala Biro PSP berperan sebagai Penanggung Jawab SMKI.
2. Kepala Biro PSP dalam menjalankan tugasnya sebagai Penanggung Jawab SMKI dibantu oleh Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional selaku Pelaksana Teknis keamanan informasi.
3. Kepala Bagian Sistem Informasi berperan sebagai Ketua Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional dan memiliki kewenangan dalam menentukan komposisi, kualifikasi, dan jumlah anggota tim.
4. Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional ditetapkan oleh Sekretaris Jenderal Dewan Ketahanan Nasional.
5. Kepala Biro PSP bersama dengan Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional menjalankan pengelolaan keamanan informasi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional.
6. Pengawasan Internal berperan melaksanakan audit internal keamanan informasi.

2.5. Tanggung Jawab

1. Kepala Biro PSP bertanggung jawab untuk:
   a. Memastikan pelaksanaan Kebijakan SMKI;

b. Menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI;
c. Menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;
d. Memastikan pelaksanaan audit internal SMKI;
e. Menetapkan arsitektur keamanan informasi;
f. Melakukan tinjauan secara berkala atas pelaksanaan kebijakan SMKI; dan
g. Menyampaikan kinerja pelaksanaan kebijakan SMKI kepada Sekretaris Jenderal Dewan Ketahanan Nasional.

2. Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional bertanggung jawab untuk:
   a. Menyusun, mengkomunikasikan, dan memantau pelaksanaan kebijakan SMKI di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional;
   b. Melakukan analisis kebutuhan keamanan informasi, yang mencakup:
      1) mengidentifikasi aplikasi dan infrastruktur untuk keamanan informasi;
      2) mengidentifikasi standar kompetensi personel keamanan informasi;
      3) mengidentifikasi program peningkatan kompetensi keamanan informasi dan penanggulangan insiden siber;
   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. Dalam memfasilitasi pelaksanaan audit internal keamanan informasi, Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional dapat menunjuk pihak yang berkompeten di bidang audit keamanan informasi sebagai konsultan;
i. Memastikan diterapkannya manajemen risiko, manajemen insiden siber, dan manajemen aset dalam pelaksanaan pengamanan aset Informasi;
j. Mendorong perbaikan penerapan keamanan informasi berdasarkan hasil temuan audit internal dan audit eksternal; dan
k. Membuat laporan evaluasi penerapan Kebijakan SMKI dan menyampaikannya kepada Kepala Biro PSP.

BAB III
PERENCANAAN KEAMANAN INFORMASI

3.1. Kategorisasi Sistem Elektronik

Sekretariat Jenderal Dewan Ketahanan Nasional sebagai Penyelenggara SPBE yang merupakan Sistem Elektronik di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional , 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.Manajemen Risiko

Pelaksanaan keamanan informasi dilakukan dengan memperhatikan berbagai risiko yang dapat mengakibatkan terjadinya kegagalan keamanan informasi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional. Oleh karenanya, dalam melakukan perencanaan keamanan informasi, Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional melakukan manajemen risiko keamanan informasi , yang terdiri dari:

1. Penilaian risiko keamanan informasi dengan mengindentifikasi ancaman, kerentanan, peluang, dan dampak apabila risiko terjadi;
2. Bersama dengan unit terkait, menyusun Rencana Tindak Lanjut (RTL); dan
3. Melakukan sosialisasi dan komunikasi RTL pada para personel Sekretariat Jenderal Dewan Ketahanan Nasional.

4. Proses manajemen risiko dilakukan secara berkala paling sedikit setiap 1 (satu) tahun sekali atau jika ada perubahan aset atau proses bisnis yang berdampak signifikan terhadap profil risiko yang ada saat ini.

3.2. Perencanaan Keamanan Informasi

Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional 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.

BAB IV
DUKUNGAN PENGOPERASIAN

4.1. Dukungan Pengoperasian

1. Kepala Biro PSP memberikan dukungan pengoperasian keamanan informasi dengan menyediakan personel keamanan informasi yang berkompeten dan anggaran keamanan informasi;
2. Personel keamanan informasi yang disediakan harus memiliki kompetensi:
   a. Keamanan Infrastruktur TIK; dan
   b. Keamanan Aplikasi.
   3. Dalam hal personel keamanan informasi yang disediakan belum memiliki kompetensi memadai, maka Kepala Biro PSP memfasilitasi peningkatan kompetensi melalui kegiatan pelatihan dan/atau bimbingan teknis;
4. Kepala Biro PSP menyediakan anggaran keamanan informasi berdasarkan arsitektur dan peta rencana keamanan informasi yang telah disusun; dan
5. Anggaran keamanan informasi dibebankan pada Anggaran Pendapatan dan Belanja Negara atau sumber anggaran lainnya yang sah.

BAB V
KEAMANAN SUMBER DAYA MANUSIA

5.1. Keamanan Sumber Daya Manusia

Keamanan Personel dilakukan untuk mengendalikan personel dalam melaksanakan Kebijakan SMKI. Keamanan personel di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional dilaksanakan oleh Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional 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 untuk :
   a. Melaksanakan dan bertindak sesuai dengan Peraturan Sistem Manajemen Keamanan informasi Sekretariat Jenderal Dewan Ketahanan Nasional;
   b. Melindungi aset dari akses yang tidak sah, penyingkapan, modifikasi, kerusakan atau gangguan;
   c. Melaksanakan proses keamanan atau kegiatan keamanan informasi sesuai dengan peran dan tanggung jawabnya; dan
   d. Melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan Kebijakan dan Standar SMKI di Lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional.
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 secara berkala meliputi;
   a. Ketersediaan referensi, dari referensi hubungan kerja dan referensi pribadi;
   b. Melakukan pemeriksaan kelengkapan dan ketetapan dari riwayat hidup pemohon;
   c. Melakukan konfirmasi akademik dan profesional yang diklaim;
   d. Melakukan pemeriksaan independen identitas (KTP atau dokumen yang sama); dan
   e. Melakukan pemeriksaan lebih rinci, seperti pemeriksaan dari catatan kriminal.

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. Memberikan edukasi terkait pentingnya keamanan informasi dalam penggunaan data pribadi, penyebarluasan, dan sanksi atas pelanggaran diberikan tindakan disiplin sesuai dengan ketentuan yang berlaku;
6. Menghentikan hak penggunaan aset informasi bagi pegawai yang sedang dalam pemeriksaan terkait dengan dugaan pelanggaran keamanan informasi;
7. 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 lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional;
8. 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; dan
9. Memberikan edukasi kesadaran keamanan informasi melalui kegiatan sosialisasi, bimbingan teknis, dan/atau pelatihan mengenai keamanan informasi yang dilaksanakan secara berkala.

BAB VI
KEAMANAN ASET

6.1. Keamanan Aset

Keamanan Aset dilakukan untuk mengamankan aset informasi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional berdasarkan tingkat kritikalitasnya. Secara garis besar, tingkat kritikalitas pada keamanan informasi Sekretariat Jenderal Dewan Ketahanan Nasional dapat dibagi menjadi enam lapisan, yaitu:

1. Data dan Informasi

   Sekretariat Jenderal Dewan Ketahanan Nasional selaku Lembaga Pemerintah Non Kementerian sesuai dengan Peraturan Sekretariat Jenderal Dewan Ketahanan Nasional Nomor 80 Tahun 2020 mempunyai tugas merumuskan rancangan kebijakan dan strategi nasional dalam rangka

pembinaan ketahanan nasional untuk menjamin pencapaian tujuan dan kepentingan nasional Indonesia. Rumusan dan rancangan kebijakan yang sudah dikaji kemudian dikirim kepada Presiden sebagai Ketua Dewan Ketahanan Nasional sebagai bahan referensi dalam menetapkan kebijakan strategi nasional khususnya di bidang ideologi, politik, ekonomi, sosial, budaya, pertahanan dan keamanan. Sehingga produk-produk kajian yang dihasilkan oleh Sekretariat Jenderal Dewan Ketahanan Nasional lebih bersifat *confidential*, rahasia dan terbatas. Selain itu konfigurasi jaringan dan sistem informasi Sekretariat Jenderal Dewan Ketahanan Nasional adalah salah satu data yang harus dijaga kerahasiaannya.

2. Perangkat Lunak

   Yang termasuk aset perangkat lunak atau *software* yaitu beberapa modul aplikasi yang berada dan atau dikelola oleh Sekretariat Jenderal Dewan Ketahanan Nasional yakni *Webserver*, Aplikasi Portal Satu Data, Mail Server, *Ruckus ZoneDirector Wireless Controller*, Aplikasi Sistem Dokumentasi Kajian, Aplikasi Perpustakaan, Aplikasi E-Kinerja, *Intelligence* Media Monitoring, Aplikasi Jaringan Dokumen dan Informasi Hukum (JDIH), Aplikasi LPSE, Aplikasi eSign, Aplikasi Sistem Audit Kelembagaan, Aplikasi Sistem Informasi Manajemen Kepegawaian, Sistem Informasi Pertimbangan Jabatan dan Pangkat, Aplikasi Daftar Narasumber, Aplikasi Keuangan, Website Wantannas beserta modul turunannya yaitu Prosedur Layanan Informasi, Website Ortala, Website Perencanaan dan Website Pengawasan Internal.

3. Perangkat Keras

   Yang termasuk dalam aset perangkat keras atau *hardware* yaitu perangkat Server, *Personal Computer* (PC), Laptop, *Harddisk* Eksternal, CD, *Flash Disk*, dsb.

4. Perangkat Jaringan Komunikasi

   Yang termasuk dalam aset jaringan komunikasi antara lain Router, Modem, *Switch*, Kabel, *Firewall*, *Access Point*, dsb.

5. Fasilitas Pendukung

   Yang termasuk fasilitas pendukung antara lain: Ruang Server, Ruang Kerja, UPS, Genset, AC, CCTV, *Fire Extinguisher, Network Panel, Access Door Electronic*, dsb.

6. Sumber Daya Manusia

Yang termasuk dalam sumber daya manusia adalah para pegawai sipil Setjen Wantannas, para pegawai yang ditugaskan di Sekretariat Jenderal Dewan Ketahanan Nasional, para pegawai perbantuan, mitra, vendor, serta pihak ketiga lainnya yang menyediakan layanan dan jasa serta produk yang menunjang kegiatan operasional Sekretariat Jenderal Dewan Ketahanan Nasional.

Keamanan aset informasi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional dilakukan oleh Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut:

a. Mengidentifikasi aset informasi dan mendokumentasikannya dalam daftar inventaris 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 dan bertanggungjawab;
f. Penggunaan aset yang dibawa ke luar dari lingkungan Pusat Data atau tempat layanan informasi harus disetujui oleh Kepala Biro PSP;
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.

6.2. Risiko-risiko terhadap aset

Risiko adalah segala kemungkinan (*likelihood*) yang dapat dimanfaatkan oleh serangan (*threat*). Risiko terkadang juga tidak dapat terhindari, jadi organisasi seyogyanya mampu menerima tingkatan tertentu dari risiko. Risiko dalam berbagai konteks adalah gabungan dari beberapa faktor diantaranya serangan (segala sesuatu yang membahayakan), kelemahan (keterbukaan terhadap serangan), dan nilai aset itu sendiri (seberapa besar dampak apabila tidak adanya aset). Peningkatan terhadap salah satu faktor akan meningkatkan faktor risiko secara umum.

1. Identifikasi Ancaman (*Threat*)

   Ancaman, menurut *National Institute of Standards and Technology* (NIST) Amerika Serikat, adalah segala sesuatu yang berasal dari sumber ancaman dan dapat memanfaatkan kelemahan. Pada dasarnya ancaman dapat di bagi menjadi 3 jenis berdasarkan sumbernya, diantaranya adalah:

   a. Ancaman yang berasal dari bencana alam, contohnya adalah banjir, gempa bumi, badai.
   b. Ancaman yang berasal dari manusia

      Dapat berupa hal yang disengaja ataupun tidak dari manusia dan dapat bersumber dari dalam maupun luar lingkungan organisasi. Contohnya adalah kesalahan dalam melakukan konfigurasi sistem operasi, kesalahan dalam memasukkan data, serangan melalui jaringan, akses pihak yang tidak berwenang terhadap informasi yang sifatnya rahasia, dan lain sebagainya.
   c. Ancaman lingkungan

      Disebabkan oleh kondisi lingkungan, seperti matinya aliran listrik, polusi, bahan kimia berbahaya, dan lain sebagainya.

      Berdasarkan hasil survey yang dilakukan oleh NIST USA, maka dapat diketahui bahwa ancaman yang bersumber dari manusia adalah sumber ancaman yang paling berbahaya terhadap keamanan informasi organisasi.

2. Kelemahan (*vulnerability*) adalah cacatnya atau lemahnya prosedur keamanan, rancangan, atau implementasi sistem informasi di organisasi.

   Tabel dibawah ini mendefinisikan pengaruh dampak terhadap kegiatan pelaporan di Sekretariat Jenderal Dewan Ketahanan Nasional.

Kategori Nilai Dampak	**Penjelasan**
Kecil	Tidak menghambat kegiatan penyampaian informasi
Sedang	Keterlambatan dalam dihasilkannya data dan informasi
Besar	Data tidak bisa dihasilkan dalam jangka waktu tertentu

3. Kebijakan

   a. Seluruh informasi yang disimpan dalam media simpan, ditulis, dicetak, dan dikomunikasikan langsung atau melalui teknologi komunikasi harus dilindungi terhadap kemungkinan kerusakan, kesalahan penggunaan secara sengaja atau tidak, dicegah dari akses oleh *user* yang tidak berwenang dan dari ancaman terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*);

b. Kebijakan keamanan informasi harus dikomunikasikan ke seluruh pegawai dan terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi;
c. Sekretariat Jenderal Dewan Ketahanan Nasional meningkatkan kepedulian (*awareness*), pengetahuan dan ketrampilan tentang keamanan informasi bagi pegawai. Sosialisasi juga perlu diberikan kepada vendor, konsultan, mitra, dan pihak ketiga lainnya sepanjang diperlukan;
d. Seluruh kelemahan keamanan Informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan TI harus segera dilaporkan ke Kepala Biro PSP;
e. Seluruh pimpinan di semua tingkatan bertanggungjawab menjamin kebijakan ini diterapkan di seluruh unit kerja di bawah pengawasannya;
f. Seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan aset informasi serta mematuhi kebijakan dan prosedur keamanan informasi yang telah ditetapkan;
g. Setiap pelanggaran terhadap kebijakan ini yang relevan dapat dikenai sanksi atau tindakan disiplin sesuai peraturan yang berlaku;
h. Kebijakan dan prosedur lainnya yang dianggap perlu akan ditetapkan kemudian; dan
i. Setiap pengecualian terhadap kebijakan ini dan kebijakan turunannya harus mendapat persetujuan dari Kepala Biro PSP.

BAB VII
KEAMANAN AKSES

7.1. 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 lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional dilakukan oleh Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut:

1. Menyusun prosedur, mendokumentasikan, dan mengkaji 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 lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional;
   e. memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya;
   f. memelihara catatan pengguna layanan (*user log*);
   g. memastikan perangkat pengolah informasi yang digunakan mendapatkan perlindungan terutama saat ditinggalkan;
   h. menonaktifkan akses pengguna yang telah berakhir penugasannya; dan
   i. memantau dan mengevaluasi akun dan hak akses secara berkala minimal setiap 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 dan port pada fasilitas jaringan yang tidak dibutuhkan dalam kegiatan atau fungsi layanan wajib dinonaktifkan;
   c. memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi;
   d. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu;
   e. melakukan *routing* jaringan internal Sekretariat Jenderal Dewan Ketahanan Nasional wajib dilakukan sesuai pengendalian akses dan kebutuhan layanan informasi; dan
   f. 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 lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional 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
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 dengan produk, seperti sistem operasi, sistem pengolahan basis data, aplikasi;
   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 yang dialokasikan/diberikan kepada pengguna. Hak akses khusus tidak boleh diberikan sebelum proses otorisasi selesai; dan

d. memberikan hak akses khusus secara terpisah dari akun yang digunakan untuk kegiatan umum seperti akun *system administrator, database administrator,* dan *network administrator.*

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 FISIK DAN LINGKUNGAN

8.1. Keamanan Fisik dan Lingkungan

Keamanan fisik dan lingkungan dilakukan untuk memberikan perlindungan, pemeliharaan, keamanan, dan ketersediaan aset informasi. Keamanan fisik dan lingkungan dilaksanakan oleh Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional bekerja sama dengan unit kerja terkait, keamanan fisik dan lingkungan dapat diklasifikasikan sebagai berikut:

A. Keamanan Area dan Pusat Data

1. Pusat Data dan Informasi Sekretariat Jenderal Dewan Ketahanan Nasional menyimpan perangkat pengolah informasi di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain:
   a. Pintu dengan kontrol akses;
   b. Kamera pengawas (CCTV);
   c. Pendeteksi asap;
   d. Sistem pemadam kebakaran;
   e. Alarm bahaya; dan
   f. 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. Waktu masuk dan keluar serta maksud kedatangan harus dicatat dalam buku catatan kunjungan;
4. Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi rahasia dan sangat rahasia harus dilindungi secara memadai;
5. Makanan dan minuman dilarang untuk dibawa masuk ke atau dikonsumsi di dalam ruang server Pusat Data;
6. Semua area yang digunakan untuk menyimpan aset informasi merupakan area bebas rokok;
7. 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;
8. Pengamanan area Pusat Data dan area kerja layanan informasi dilakukan sesuai Prosedur Keamanan Area;

B. Keamanan Kantor, Ruangan dan Fasilitas

Keamanan kantor, ruangan dan fasilitas mencakup:

1. Pengamanan kantor, ruangan, dan fasilitas kerja sesuai dengan peraturan dan standar keamanan dan keselamatan kerja, termasuk *clear screen policy* dan *clean desk policy*;
2. Fasilitas utama harus ditempatkan khusus untuk menghindari akses publik;
3. Infrastruktur yang digunakan untuk menjalankan aplikasi dipelihara sesuai dengan buku petunjuk/manualnya;
4. Dalam hal pemeliharaan infrastruktur tidak dapat dilakukan di tempat, maka pemindahan infrastruktur dilakukan berdasarkan persetujuan Kepala Biro PSP;

5. 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; dan
6. 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.

C. Keamanan terhadap ancaman eksternal dan lingkungan

Keamanan terhadap ancaman eksternal dan lingkungan harus mempertimbangkan:

1. 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);
2. Bahan berbahaya atau mudah terbakar di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional wajib disimpan pada jarak yang aman dari Pusat Data dan area kerja layanan informasi;
3. Perlengkapan umum seperti alat tulis tidak boleh disimpan didalam *secure areas*;
4. Perangkat *fallback* dan media *backup* harus diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama; dan
5. Perangkat pemadam kebakaran wajib disediakan, dipelihara, dan diletakkan di tempat yang tepat dan mudah dijangkau.

D. Keamanan dan perlindungan perangkat

Penempatan keamanan dan perlindungan perangkat harus mencakup:

1. Perangkat harus diletakkan pada lokasi yang meminimalkan akses yang tidak perlu ke dalam area kerja;
2. Perangkat pengolah informasi wajib dipelihara secara berkala untuk menjamin ketersediaan, keutuhan, dan fungsinya;

3. Perangkat pengolah informasi yang menangani informasi sensitif harus diposisikan dan dibatasi arah sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak yang tidak berwenang selama digunakan, dan perangkat penyimpanan diamankan untuk menghindari akses oleh pihak yang tidak berwenang;
4. Langkah-langkah pengendalian dilakukan untuk meminimalkan risiko potensi ancaman fisik, seperti pencurian, api, gangguan komunikasi, dan perusakan;
5. Kondisi lingkungan, seperti suhu dan kelembaban harus dimonitor untuk mencegah perubahan kondisi yang dapat mempengaruhi pengoperasian perangkat pengolah informasi;
6. Perangkat pengolah informasi sensitif harus dilindungi untuk meminimalkan risiko kebocoran informasi; dan
7. Penggunaan perangkat yang dibawa ke luar dari lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional wajib disetujui oleh pejabat yang berwenang.

E. Keamanan Kabel dan Kelistrikan

1. Pemasangan kabel jaringan, kabel sumber daya listrik dan kabel komunikasi wajib dilindungi dari penyusupan yang tidak sah atau kerusakan, misalnya dengan menggunakan *conduit* atau menghindari rute melalui area publik;
2. Pemisahan antara kabel sumber daya listrik dengan kabel telekomunikasi untuk mencegah interferensi;
3. Penandaan/penamaan kabel dan perangkat harus diterapkan secara jelas untuk memudahkan penanganan kesalahan;
4. Penggunaan dokumentasi daftar *panel patch* diperlukan untuk mengurangi kesalahan;
5. Semua infrastruktur harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang diisyaratkan oleh pabrikan infrastruktur;
6. 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;

7. Perlindungan petir wajib diterapkan untuk semua bangunan dan filter perlindungan petir dipasang untuk semua jalur komunikasi dan listrik;
8. Pengamanan kabel di Pusat Data dan/atau area kerja layanan informasi dilakukan dengan mengikuti standar mekanikal/elektrikal Pusat Data yang berlaku; dan
9. Pengendalian untuk sistem informasi yang sensitif harus mempertimbangkan:
   a) Menggunakan *conduit*;
   b) Penggunaan ruangan terkunci pada tempat inspeksi dan titik pemutusan kabel;
   c) Penggunaan rute alternatif dan atau media transmisi yang menyediakan keamanan yang sesuai;
   d) Penggunaan kabel fiber optik;
   e) Penggunaan lapisan elektromagnet untuk melindungi kabel;
   f) Inisiasi penghapusan teknikal (*technical sweeps*) dan pemeriksaan secara fisik untuk peralatan yang tidak diotorisasi saat akan disambungkan ke kabel; dan
   g) Penerapan akses Kontrol ke panel *patch* dan ruangan kabel.

BAB IX
KEAMANAN KRIPTOGRAFI

9.1. 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; dan
2. menerapkan keamanan kriptografi untuk informasi berklasifikasi rahasia dan/atau sangat rahasia dengan cara sebagai 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.

BAB X
KEAMANAN OPERASIONAL

10.1. Keamanan Operasional

Keamanan operasional dilakukan untuk memastikan operasional yang aman dan benar pada aset informasi, mengimplementasikan dan memelihara keamanan aset informasi, mengelola layanan yang diberikan oleh Pihak Ketiga, meminimalkan risiko kegagalan, dan melindungi keutuhan dan ketersediaan aset informasi. Keamanan operasional di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional dilakukan oleh Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional bekerja sama dengan unit kerja terkait, cara sebagai berikut:

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 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 lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional;
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; dan
13. Melakukan penilaian kerentanan terhadap perangkat informasi (*vulnerability assessment*) secara berkala dan melakukan tindakan perlindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi.

BAB XI
KEAMANAN KOMUNIKASI

11.1. Keamanan Komunikasi

Keamanan komunikasi dilakukan untuk memastikan keamanan pertukaran dan perlindungan terhadap informasi melalui jaringan komunikasi. Keamanan komunikasi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional dilakukan oleh Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut:

1. Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional 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, minimal 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. Melakukan pemantauan kegiatan pengelolaan jaringan untuk menjamin bahwa perangkat jaringan digunakan secara efektif dan efisien;
5. Melakukan pengendalian dan pengaturan tentang penyambungan dan perluasan jaringan internal atau eksternal pusat data dan informasi Sekretariat Jenderal Dewan Ketahanan Nasional;
6. Informasi yang terdapat dalam aplikasi yang melewati jaringan publik harus dilindungi dari upaya pengungkapan, modifikasi, dan perusakan dengan menerapkan mekanisme kriptografi;
7. Pertukaran informasi dan perangkat lunak antara pusat data dan informasi Sekretariat Jenderal Dewan Ketahanan Nasional dengan pihak ketiga hanya akan dilakukan atas kesepakatan tertulis kedua belah pihak;

8. Pengendalian pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
   a. Pencegahan terhadap penyalahgunaan wewenang pegawai dan pihak ketiga yang dapat membahayakan organisasi;
   b. Penggunaan teknik kriptografi;
   c. Penyelenggaraan penyimpanan dan penghapusan/pemusnahan untuk semua korespondensi kegiatan, termasuk pesan, yang sesuai dengan ketentuan yang berlaku;
   d. Larangan meninggalkan informasi sensitif pada perangkat pengolah informasi;
   e. Pembatasan penerusan informasi secara otomatis;
   f. Membangun kepedulian atas ancaman pencurian informasi, misalnya terhadap:
      1) Pengungkapan informasi sensitif untuk menghindari mencuri dengar (penyadapan) saat melakukan panggilan telepon;
      2) Akses pesan diluar kewenangannya;
      3) Pemrograman mesin fax baik sengaja maupun tidak sengaja untuk mengirim pesan ke nomor tertentu;
      4) Pengiriman dokumen dan pesan ke tujuan yang salah;
      5) Pembangunan kepedulian atas pendaftaran data demografis, seperti alamat surat elektronik atau informasi pribadi lainnya untuk menghindari pengumpulan informasi yang tidak sah; dan
      6) Penyediaan informasi internal Sekretariat Jenderal Dewan Ketahanan Nasional bagi masyarakat umum harus disetujui oleh pemilik informasi dan sesuai dengan ketentuan yang berlaku.
9. Melakukan pendeteksian dan perlindungan terhadap kode berbahaya (*malicious code*) yang disisipkan pada file yang dikirim melalui sistem elektronik;
10. Memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan untuk informasi elektronik berklasifikasi rahasia dan/atau sangat rahasia;
11. Menetapkan Prosedur Pertukaran informasi yang mengatur sistem dan keamanan yang digunakan untuk pertukaran informasi;
12. Menerapkan *audit logging* 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.

13. Menerapkan sistem pencatatan aktivitas administrator dan operator sistem;
14. Menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindak pengamanan yang tepat; dan
15. Memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.

BAB XII
KEAMANAN PENGEMBANGAN DAN PEMELIHARAAN

12.1. Keamanan Pengembangan dan Pemeliharaan

Keamanan pengembangan dan pemeliharaan sistem dilakukan untuk memastikan bahwa keamanan informasi merupakan keamanan informasi bagian yang terintegrasi dalam daur hidup aset informasi untuk mencegah terjadinya kesalahan, kehilangan, eksploitasi, modifikasi, dan perusakan aset informasi oleh pihak yang tidak berwenang. Keamanan pengembangan dan pemeliharaan di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional dilakukan oleh Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut:

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. 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;
6. Fitur-fitur keamanan yang dimasukkan sesuai dengan standar keamanan relevan, yang mencakup:

a. Standar keamanan data dan informasi;
b. Standar keamanan aplikasi;

Standar teknis keamanan aplikasi berbasis web terdiri atas terpenuhinya fungsi:

1) authentikasi, yang dapat dilakukan dengan prosedur:
   a) menggunakan manajemen kata sandi untuk proses autentikasi.
   b) menerapkan verifikasi kata sandi pada sisi server;
   c) mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;
   d) mengatur jumlah maksimum kesalahan dalam memasukkan kata sandi;
   e) mengatur mekanisme pemulihan kata sandi;
   f) menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan
   g) menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.
2) Manajemen sesi, yang dapat dilakukan dengan prosedur:
   a) menggunakan pengendali sesi untuk proses manajemen sesi;
   b) menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
   c) mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
   d) mengatur kondisi dan jangka waktu habis sesi;
   e) validasi dan pencantuman *session id*;
   f) perlindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
   g) perlindungan terhadap diplikasi dan mekanisme persetujuan pengguna.
3) Persyaratan Kontrol Akses yang dapat dilakukan dengan prosedur:
   a) menetapkan otorisasi pengguna untuk membatasi kontrol akses;
   b) mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus menerus pada fungsi mengatur antarmuka pada sisi administrator; dan
   c) mengatur verifikasi kebenaran token Ketika mengakses data dan informasi yang dikecualikan.

4) Validasi Input yang dapat dilakukan dengan prosedur:
   a) menerapkan fungsi validasi input pada sisi server;
   b) menerapkan mekanisme penolakan input jika terjadi kesalahan validasi;
   c) memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi input;
   d) melakukan validasi positif pada seluruh input;
   e) melakukan filter terhadap data yang tidak dipercaya;
   f) menggunakan fitur kode dimanis;
   g) melakukan perlindungan terhadap akses yang mengandung konten skrip; dan
   h) melakukan perlindungan dan serangan injeksi berbasis data.
5) Terpenuhinya fungsi kriptografi pada verifikasi statis dapat dilakukan dengan prosedur:
   a) menggunakan algoritma kriptografi, modul kriptografi, protokol kriptograsi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan;
   b) melakukan autentikasi data yang dienkripsi;
   c) menerapkan manajemen kunci kriptografi; dan
   d) membuat angka acak yang menggunakan generator angka acak kriptografi.
6) Penanganan eror dan pencatatan log dapat dilakukan dengan prosedur:
   a) mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;
   b) menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;
   c) tidak mencantumkan informasi yang dikecualikan dalam pencatatan log;
   d) mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
   e) mengatur perlindungan log aplikasi dari akses dan modifikasi yang tidak sah;
   f) melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log; dan

g) melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

7) Proteksi data dapat dilakukan dengan prosedur:
   a) melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
   b) melakukan perlindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;
   c) melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
   d) melakukan penentuan jumlah parameter;
   e) memastikan data disimpan dengan aman;
   f) menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna; dan
   g) membersihkan memori setelah tidak diperlukan.
8) Keamanan komunikasi dilakukan dengan prosedur:
   a) menggunakan komunikasi terenkripsi;
   b) mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna;
   c) mengatur jenis algoritma yang digunakan dan alat pengujiannya; dan
   d) mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikat elektronik.
9) Pengendalian kode berbahaya dapat dilakukan dengan prosedur:
   a) menggunakan analisis kode dalam kontrol kode berbahaya;
   b) memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan;
   c) mengatur izin terkait fitur atau sensor terkait privasi;
   d) mengatur perlindungan integritas; dan
   e) mengatur mekanisme fitur pembaruan.
10) Terpenuhinya fungsi logika bisnis dapat dilakukan dengan prosedur:
   a) memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis;
   b) memastikan logika bisnis memiliki batasan dan validasi;
   c) memonitor aktivitas yang tidak biasa;

d) membantu dalam kontrol antiotomatisasi; dan
e) memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.

11) Terpenuhinya fungsi file dapat dilakukan dengan prosedur:
a) mengatur jumlah file untuk setiap pengguna dan kuota ukuran file yang diunggah;
b) melakukan validasi file sesuai dengan tipe konten yang diharapkan;
c) melakukan perlindungan terhadap metadata input dan metadata file;
d) melakukan pemindaian file yang diperoleh dari sumber yang tidak dipercaya; dan
e) melakukan konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan.

12) Keamanan API dan *web service* dapat dilakukan dengan prosedur:
a) melakukan konfigurasi layanan web;
b) memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
c) membuat keputusan otorisasi;
d) menampilkan metode *RESTful hypertext transfer protocol* apabila input pengguna dinyatakan valid;
e) menggunakan validasi skema dan verifikasi sebelum menerima input;
f) menggunakan metode perlindungan layanan berbasis web; dan
g) menerapkan kontrol antiotomatisasi.

13) Keamanan konfigurasi dapat dilakukan dengan prosedur:
a) mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan;
b) mendokumentasi, menyalin konfigurasi, dan semua dependensi;
c) menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;
d) memvalidasi integritas aset jika aset aplikasi diakses secara eksternal; dan
e) menggunakan respons aplikasi dan konten yang aman.

c. Standar keamanan jaringan intra.

Standar teknis keamanan Jaringan Intra diterapkan pada Jaringan Intra di Sekretariat Jenderal Dewan Ketahanan Nasional, dimana terdiri atas terpenuhinya: aspek administrasi keamanan Jaringan Intra, kontrol akses dan autentikasi, persyaratan perangkat dan aplikasi keamanan Jaringan Intra, kontrol keamanan *gateway*, kontrol keamanan *access point* pada jaringan nirkabel, dan kontrol konfigurasi *access point* pada jaringan nirkabel.

1) Aspek administrasi keamanan Jaringan Intra dapat dilakukan dengan prosedur:
   a) menyusun dan mengevaluasi dokumen arsitektur Jaringan Intra;
   b) mengidentifikasi seluruh aset infrastruktur jaringan;
   c) menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra; dan
   d) membuat laporan pengawasan keamanan jaringan secara periodik.
2) Kontrol akses dan authentikasi dapat dilakukan dengan dengan prosedur:
   a) menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah;
   b) menggunakan autentikasi untuk mengakses Jaringan Intra;
   c) menerapkan pembatasan akses dalam Jaringan Intra;
   d) mematikan atau membatasi *protocol, port,* dan layanan yang tidak digunakan;
   e) menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya;
   f) menerapkan fungsi *honeypot* untuk menganalisis celah keamanan berdasarkan jenis serangan;
   g) menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;
   h) memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan/atau mengubah konfigurasi system dalam jaringan intra;
   i) menerapkan *secure endpoints;*
   j) memblokir layanan yang tidak dikenal;
   k) menerapkan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses jaringan intra; dan

l) menerapkan server perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.

3) Persyaratan perangkat dan aplikasi keamanan Jaringan Intra dapat dilakukan dengan prosedur:
   a) menggunakan perangkat *security information and event management* untuk *network logging* dan monitoring;
   b) menerapkan *system* deteksi dini kerentanan keamanan perangkat jaringan;
   c) menggunakan perangkat *firewall;*
   d) menggunakan perangkat *intrusion detection systems* dan *intrusion prevention systems;*
   e) menerapkan *virtual private network* terenkropsi untuk penggunaan akses jarak jauh secara terbatas;
   f) menerapkan kontrol *update patching* pada infrastruktur jaringan intra dan *system computer*;
   g) menggunakan perangkat *web application firewall;*
   h) menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;
   i) memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisir celah peretas;
   j) mengunduh perangkat lunak melalui *enterprise software distribution system;* dan
   k) menerapkan sertifikat elektronik.

4) Kontrol keamanan *gateway* dapat dilakukan dengan prosedur:
   a) menerapkan *content filering;*
   b) menerapkan *inspection packet filtering* untuk memeriksa *packet* yang masuk pada jaringan intra;
   c) menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*;
   d) memastikan perangkat *gateway* yang menghubungkan antar jaringan intra tidak terkoneksi langsung dengan jaringan publik;
   e) melaksanakan manajemen *traffic gateway;* dan
   f) memastikan *port* tidak terbuka secara *default.*

5) Kontrol keamanan *access point* pada jaringan nirkabel dapat dilakukan dengan prosedur:
   a) menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini;
   b) menerapkan *media access kontrol* pada *address filtering*;

c) menerapkan *dedicated service set identifier*;
d) menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan;
e) menerapkan pembatasan terkait penambahan perangkat nirkabel yang terpasang secara tidak sah;
f) menerapkan manajemen *vulnerability* secara berkala dan berkelanjutan; dan
g) melakukan *patching firmware* secara rutin.

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

7. Standar keamanan sebagaimana dimaksud pada angka 6 minimal memenuhi standar keamanan yang ditetapkan oleh Lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber;
8. Melaksanakan uji kelaikan aplikasi sebelum aplikasi digunakan dan sewaktu-waktu sesuai kebutuhan, yang 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; dan

d. Uji keamanan, yaitu pengujian yang memastikan aplikasi yang dibangun dan/atau dikembangkan dapat menjaga keamanan data dan informasi yang terkait dengannya.

9. 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;
10. Uji kelaikan pada aspek uji keamanan dapat menggunakan pedoman/instrumen pengukuran yang ditetapkan oleh Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber; dan
11. 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 DENGAN INSTITUSI LAIN

13.1. Keamanan Dengan Institusi Lain

Keamanan dengan institusi lain dalam hal ini BIN (Badan Intelijen Negara) dilakukan untuk memastikan perlindungan dari aset informasi yang dapat diakses secara aman. Keamanan dengan BIN di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional dilakukan oleh Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut:

1. Melakukan pemeriksaan latar belakang institusi lain dengan tetap memperhatikan privasi dan perlindungan data pribadi;
2. Membuat dan meninjau ulang secara berkala perjanjian tertulis dengan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan aset informasi yang menyatakan tanggung jawab terhadap keamanan aset informasi. Perjanjian tertulis sebagaimana dimaksud 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 institusi lain, 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 Sekretariat Jenderal Dewan Ketahanan Nasional dengan pihak ketiga; dan
h. Dalam hal ini BIN, tidak lagi menjadi bagian dalam pengelolaan aset informasi, maka aset informasi yang dikuasainya diserahkan kembali kepada Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional.

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 Tim SMKI;
4. Memastikan *Service Level Agreement* (SLA) institusi lain 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 BIN;
7. Mencatat peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan oleh Sekretariat Jenderal Dewan Ketahanan Nasional;
8. Memberikan informasi tentang gangguan keamanan dan mengkaji informasi bersama BIN;
9. Mencabut hak akses terhadap akses informasi yang dimiliki BIN apabila yang bersangkutan tidak lagi bekerja di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional;
10. Membuat berita acara serah terima terkait mengembalikan seluruh aset informasi yang dipergunakan selama bekerjasama dengan BIN yang berakhir masa perjanjiannya; dan
11. Memastikan BIN dan tamu yang memasuki lingkungan area Pusat Data, dan tempat layanan informasi harus mematuhi standar keamanan fisik dan lingkungan.

BAB XIV
KEAMANAN INFORMASI DALAM PENGELOLAAN
KELANGSUNGAN LAYANAN INFORMASI

14.1. Keamanan Informasi Dalam Pengelolaan Kelangsungan Kegiatan

Keamanan informasi dalam pengelolaan kelangsungan layanan informasi yang bertujuan untuk melindungi sistem informasi, memastikan berlangsungnya kegiatan dan layanan pada saat keadaan darurat, serta memastikan pemulihan yang tepat. Keamanan informasi dalam pengelolaan kelangsungan kegiatan dapat berjalan dengan baik wajib melaksanakan :

1. Proses Pengelolaan Kelangsungan Layanan Informasi;
   Pengelolaan Kelangsungan Layanan Informasi pada saat keadaan darurat komponen yang harus diperhatikan dalam mengelola proses kelangsungan kegiatan:
   a. Identifikasi risiko dan analisis dampak yang diakibatkan pada saat terjadi keadaan darurat;
   b. Identifikasi seluruh aset informasi yang menunjang proses kegiatan kritikal;
   c. Identifikasi sumber daya, mencakup biaya, struktur organisasi, teknis pelaksanaan, pegawai dan pihak ketiga;
   d. Memastikan keselamatan pegawai dan perlindungan terhadap perangkat pengolah informasi dan aset organisasi;
   e. Penyusunan dan pendokumentasian Rencana Kelangsungan Layanan Informasi sesuai dengan Rencana Strategi (Renstra) Sekretariat Jenderal Dewan Ketahanan Nasional;
   f. Pelaksanaan uji coba dan pemeliharaan Rencana Kelangsungan Kegiatan secara berkala;
   g. Penetapan peran dan penanggung jawab pegawai yang terlibat dalam pelaksanaan keberlangsungan layanan informasi; dan
   h. Pelaksanaan sosialisasi dan pelatihan keberlangsungan layanan informasi.

2. Jika aplikasi merupakan aplikasi umum/sistem elektronik berkategori strategis, maka harus memiliki redundansi yang cukup untuk memenuhi ketersediaan layanan informasi;

3. Penilaian Risiko dan Analisis Dampak Bisnis (*Business Impact Analysis*/BIA)

   Proses identifikasi risiko mengikuti ketentuan mengenai Penerapan Manajemen Risiko di Lingkungan Pusat Data dan Informasi Sekretariat Jenderal Dewan Ketahanan Nasional;

4. Penyusunan dan Penerapan Rencana Kelangsungan Kegiatan (*Businnes Continuity Plan*/BCP)

   Proses analisis dampak kegiatan harus melibatkan pemilik risiko dan dievaluasi secara berkala. Penyusunan rencana kelangsungan kegiatan mencakup:

   a. Prosedur keberlangsungan layanan informasi saat keadaan darurat, mencakup manajemen risiko, analisis dampak kegiatan, uji coba keberlangsungan kegiatan serta tindakan yang harus dilakukan serta pengaturan hubungan dengan pihak berwenang;
   b. Prosedur *fallback*, mencakup tindakan yang harus diambil untuk memindahkan kegiatan kritikal atau layanan pendukung ke lokasi kerja sementara, dan mengembalikan operasional kegiatan kritikal dalam jangka waktu sesuai dengan standar ketersediaan data yang berlaku di Lingkungan Pusat Data dan Informasi Sekretariat Jenderal Dewan Ketahanan Nasional;
   c. Prosedur saat kondisi telah normal *(resumpfion)*, adalah tindakan mengembalikan kegiatan operasional ke kondisi normal;
   d. Jadwal uji coba, mencakup langkah-langkah dan waktu pelaksanaan uji coba serta proses pemeliharaannya;
   e. Pelaksanaan pelatihan dan sosialisasi dalam rangka meningkatkan kepedulian dan pemahaman proses kelangsungan kegiatan dan memastikan proses kelangsungan kegiatan dilaksanakan secara efektif;
   f. Tanggung jawab dan peran setiap Petugas Pelaksanaan Pengelolaan Proses Kelangsungan; dan
   g. Daftar kebutuhan aset informasi kritikal dan sumber daya untuk dapat menjalankan prosedur saat keadaan darurat, *fallback*: dan saat kondisi telah normal *(resumption).*

5. Pengujian, Pemeliharaan, dan Pengkajian Ulang Rencana Kelangsungan Kegiatan.

   Uji Coba Rencana Kelangsungan Kegiatan harus dilaksanakan untuk memastikan setiap rencana yang disusun dapat dilakukan/ dipenuhi pada saat penerapannya dan dilaksanakan secara berkala. Kegiatan uji coba Rencana Kelangsungan Kegiatan ini mencakup:

a. Simulasi terutama untuk Petugas Pelaksana Pengelolaan Proses Kelangsungan Kegiatan;
b. Uji coba *recovery* sistem informasi untuk memastikan sistem informasi dapat berfungsi kembali;
c. Uji coba proses *recovery* di lokasi kerja sementara untuk menjalankan proses bisnis secara paralel;
d. Uji coba terhadap perangkat dan layanan yang disediakan oleh pihak ketiga; dan
e. Uji coba keseluruhan mulai dari organisasi, petugas, peralatan, perangkat, dan prosesnya.

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

BAB XV
MANAJEMEN INSIDEN SIBER

15.1. Manajemen Insiden Siber

Manajemen insiden siber dilaksanakan untuk mengendalikan insiden siber. Manajemen insiden siber di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional dilakukan oleh Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut:

1. Membentuk Tim Tanggap Insiden siber (TTIS) yang bertugas melakukan pencegahan dan penanganan insiden siber yang terjadi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional;
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 internal 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 lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional termasuk oleh pihak ketiga; dan
9. Melakukan pengukuran tingkat kematangan penanganan insiden siber secara berkala.

BAB XVI
PENGENDALIAN KEPATUHAN

16.1. 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 lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional. Pengendalian kepatuhan keamanan informasi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional, dilakukan oleh Tim SMKI Sekretariat Jenderal Dewan Ketahanan Nasional bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

1. Kepatuhan terhadap Hak Kekayaan Intelektual
   Hal yang perlu diperhatikan dalam melindungi segala materi yang dapat dianggap kekayaan intelektual meliputi:

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. Memelihara daftar aset informasi sesuai persyaratan untuk melindungi hak kekayaan intelektual;
e. Memeriksa kepatuhan penggunaan lisensi aplikasi dan menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;
f. Penggandaan perangkat lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran;
g. Memelihara bukti kepemilikan lisensi, *master disk*, buku manual, dan lain sebagainya;
h. Melakukan pemeriksaan bahwa tidak ada produk bajakan yang terinstal (pelanggaran hak kekayaan intelektual) di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional;
i. Melaksanakan kepatuhan terhadap syarat dan kondisi untuk perangkat lunak dan informasi yang didapat dari jaringan publik;
j. Memastikan pelarangan melakukan duplikasi, konversi ke format lain atau mengambil rekaman komersial (film atau audio), selain yang diperbolehkan oleh Undang-undang Hak Cipta;
k. Memastikan rekaman terlindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah, dan rilis tidak sah sesuai dengan persyaratan peraturan perundang-undangan, kontraktual dan bisnis;
l. Memastikan pengamanan privasi dan data pribadi yang dapat diidentifikasikan sesuai dengan persyaratan peraturan perundang-undangan yang berlaku;
m. Memastikan kesesuaian penerapan kriptografi dengan peraturan perundang-undangan yang berlaku;
n. Kebijakan, standar dan keamanan informasi dan implementasinya harus direviu berkala secara independen atau ketika terjadi perubahan signifikan; dan
o. Mereviu sistem informasi secara berkala agar sesuai dengan kebijakan dan standar keamanan informasi di lingkungan Sekretariat Jenderal Dewan Ketahanan Nasional.

2. Kepatuhan terhadap Kebijakan dan Standar

   Hal yang perlu dilakukan jika terdapat ketidakpatuhan teknis meliputi:

   a. Menentukan dan mengevaluasi penyebab ketidakpatuhan;
   b. Menentukan tindakan yang perlu dilakukan berdasarkan hasil evaluasi agar ketidakpatuhan tidak terulang kembali;
   c. Menentukan dan melaksanakan tindakan perbaikan yang sesuai; dan
   d. Mengkaji tindakan perbaikan yang dilakukan.

3. Kepatuhan Teknis

   Sistem informasi harus diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan perangkat lunak telah diimplementasikan secara benar. Kepatuhan teknis juga mencakup pengujian penetrasi (*penetrating testing*) untuk mendeteksi kerentanan dalam sistem, dan memeriksa pengendalian akses untuk mencegah kerentanan tersebut telah ditetapkan;

4. Kepatuhan terkait Audit Sistem Informasi

   Proses audit sistem informasi harus memperhatikan hal-ha1 berikut:

   a. Persyaratan audit harus disetujui oleh Sekretaris Jenderal Dewan Ketahanan Nasional;
   b. Ruang lingkup pemeriksaan/audit harus disetujui dan dikendalikan oleh pihak berwenang;
   c. Pemeriksaan perangkat lunak dan data harus dibatasi untuk akses baca saja (*read only*);
   d. Selain akses baca saja hanya diizinkan untuk salinan dari ate sistem yang diisolasi, yang harus dihapus bila audit telah selesai, atau diberikan perlindungan yang tepat jika ada kewajiban untuk menyimpan file tersebut di bawah persyaratan dokumentasi audit;
   e. Sumber daya untuk melakukan pemeriksaan harus secara jelas diidentifikasi dan tersedia;
   f. Persyaratan untuk pengolahan khusus atau tambahan harus diidentifikasi dan disepakati;
   g. Semua akses harus dipantau dan dicatat untuk menghasilkan
   h. Jejak audit, dan untuk data dan sistem informasi sensitif harus mempertimbangkan pencatatan waktu pada jejak audit;

i. Semua prosedur, persyaratan, dan tanggung jawab harus didokumentasikan; dan

j. Auditor harus independen dari kegiatan yang diaudit.

SEKRETARIS JENDERAL
DEWAN KETAHANAN NASIONAL,

DADI HARTANTO
LAKSAMANA MADYA TNI