KEMENTERIAN PERTAHANAN RI
PUSAT DATA DAN INFORMASI

PEDOMAN KERJA
SISTEM MANAJEMEN KEAMANAN INFORMASI
PUSDATIN KEMHAN

Nomor : PK/01/VIII/2022/PUSDATIN

TAHUN 2022

BAB I
PEDOMAN SISTEM MANAJEMEN KEAMANAN INFORMASI

1. Pedoman Sistem Manajemen Keamanan Informasi (SMKI)

   Pedoman ini merupakan suatu pendekatan proses untuk membuat, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi (SMKI) di Pusat Data dan Informasi Kementerian Pertahanan Republik Indonesia (Pusdatin Kemhan RI).

   Pedoman ini dibuat dengan tujuan:

   a. Untuk meminimalisir kerusakan terhadap bisnis jika terjadi gangguan keamanan informasi.

   b. Memaksimalkan nilai atas investasi teknologi informasi.

   c. Menjaga kerahasiaan data dan informasi.

   d. Menjamin integritas data dan informasi.

   e. Menjamin ketersediaan data dan informasi.

   f. Memastikan kepatuhan atas aspek hukum, peraturan pemerintah, perundang-undangan, dan kewajiban atas kontrak yang berlaku.

   g. Memastikan implementasi SMKI di Pusdatin Kemhan RI selalu diperbaiki dan ditingkatkan secara berkesinambungan, dan

   h. Memenuhi persyaratan standar internasional ISO 27001:2013 di Pusdatin Kemhan RI.

BAB II
PERNYATAAN KEBIJAKAN SMKI PUSDATIN KEMHAN RI

2. Pernyataan Kebijakan SMKI Pusdatin Kemhan RI

   Kepala dan jajaran manajemen Pusdatin Kemhan RI berkomitmen untuk:

   a. Melindungi data dan informasi yang bersifat kritis yang dikelola oleh Pusdatin Kemhan RI serta digunakan oleh pemangku kepentingan terkait, dengan cara menjamin kerahasiaannya, integritasnya, dan ketersediaannya.

b. Memastikan cukupnya kesadaraan keamanan informasi oleh seluruh personel, personel kontrak, partner, mitra, dan pihak pengguna layanan Pusdatin Kemhan RI dengan 95% tingkat kepatuhan melalui jadwal pelatihan kesadaran dengan waktu yang telah ditetapkan.

c. Memastikan akses terhadap berbagai macam data dan informasi serta fasilitas pemrosesan data dan informasi kepada seluruh personel, personel kontrak, partner, vendor dan juga pihak pengguna layanan Pusdatin Kemhan RI, hanya dapat diperoleh setelah mendapatkan persetujuan pihak berwenang, dan setiap penyimpangan yang terjadi harus dicatat sebagai insiden keamanan.

d. Memastikan akses terhadap area kerja aman seperti *Data Center* Pusdatin, ruangan *server*, dan ruangan peralatan jaringan, hanya dapat diberikan setelah mendapatkan persetujuan pihak yang berwenang dengan 100% tingkat kepatuhan dan dilakukan peninjauan akses secara berkala (bulanan atau kwartalan).

e. Memastikan semua perubahan yang terjadi atas infrastruktur teknologi informasi dan aplikasi dilakukan melalui mekanisme perubahan terintregrasi yang dicatat, disetujui, dan diimplementasikan.

f. Memastikan semua insiden teknologi informasi dicatat dan diselesaikan sesuai dengan target waktu yang telah ditentukan dengan 95% tingkat kepatuhan.

g. Memastikan audit internal dan audit eksternal dilakukan minimum setiap tahunnya, dan hasil temuan audit internal dan audit eksternal ditindaklanjuti dengan pembuatan rencana langkah tindakan dan diselesaikan berdasarkan target waktu yang ditetapkan.

h. Menyediakan sumber daya yang dibutuhkan untuk menjamin terciptanya SMKI di lingkungan Pusdatin Kemhan RI.

i. Mengembangkan, memelihara, menguji coba dan memperbarui secara berkala dokumen rencana keberlangsungan bisnis (*Business Continuity Plan*) untuk menjamin terciptanya SMKI Instansi yang efektif dan efisien.

j. Mengembangkan, memelihara dan memperbarui proses manajemen risiko secara berkala terkait dengan keamanan informasi di lingkungan Pusdatin Kemhan RI, dan

k. Memastikan bahwa kebijakan ini dimengerti dan dijalankan di seluruh lingkungan Pusdatin Kemhan RI serta ditinjau oleh Ketua SMKI dan tim untuk diperbaiki secara berkelanjutan.

BAB III
KONTEKS ORGANISASI

3. Konteks Organisasi

a. Kedudukan, Tugas dan Fungsi Pusdatin Kemhan RI.

Berdasarkan Peraturan Menhan Nomor 14 Tahun 2019 yang diundangkan di Jakarta pada Tanggal 21 Maret 2019 tentang Organisasi dan Tata Kerja Kementerian Pertahanan Pasal 1255, bahwa:

1) Pusat Data dan Informasi selanjutnya disebut Pusdatin berada di bawah dan bertanggung jawab kepada Menteri melalui Sekjen, dan

2) Pusat Data dan Informasi dipimpin oleh Kepala Pusat Data dan Informasi disebut Kapusdatin.

Pusdatin Kemhan RI mempunyai tugas menyelenggarakan dukungan yang bersifat substantif kepada seluruh Satuan Kerja dan instansi di lingkungan Kemhan RI di bidang pengembangan dan pengelolaan sistem informasi pertahanan, infrastruktur teknologi informasi dan komunikasi, pengamanan sistem informasi dan persandian, dan pembinaan jabatan fungsional pranata komputer dan fungsional persandian di lingkungan Kemhan RI.

Dalam melaksanakan tugas sebagaimana dimaksud, Pusdatin menyelenggarakan fungsi:

1) Penyusunan kebijakan teknis, program dan anggaran di bidang pengembangan dan pengelolaan sistem informasi pertahanan, infrastruktur teknologi informasi dan komunikasi, pengamanan sistem informasi dan persandian, pembinaan jabatan fungsional pranata komputer dan fungsional persandian di lingkungan Kemhan RI.

2) Penyusunan peraturan dan petunjuk di bidang pengembangan dan pengelolaan sistem informasi pertahanan, infrastruktur teknologi informasi dan komunikasi, pengamanan sistem informasi dan persandian, pembinaan jabatan fungsional

pranata komputer dan fungsional persandian di lingkungan Kemhan RI.

3) Pelaksanaan pengembangan dan pengelolaan sistem informasi pertahanan dan manajemen bandwidth, infrastruktur teknologi informasi dan komunikasi, pengamanan sistem informasi dan persandian, pembinaan jabatan fungsional pranata komputer dan fungsional persandian di lingkungan Kemhan RI.

4) Pemantauan, supervisi, evaluasi dan pelaporan pelaksanaan pengembangan dan pengelolaan sistem informasi pertahanan dan manajemen bandwidth, infrastruktur teknologi informasi dan komunikasi, pengamanan sistem informasi dan persandian, pembinaan jabatan fungsional pranata komputer dan fungsional persandian di lingkungan Kemhan RI, dan

5) Pengelolaan ketatausahaan dan kerumahtanggaan Pusat.

Pusat Data dan Informasi terdiri dari :

1) Bagian Tata Usaha (Bag TU)

Bagian Tata Usaha selanjutnya disebut Bag TU dipimpin oleh Kepala Bagian Tata Usaha disebut Kabag TU mempunyai tugas melaksanakan penyiapan, penyusunan, perencanaan program dan anggaran, evaluasi dan laporan, kepersonelan, ketatausahaan, kerumahtanggaan, pengadminstrasian dan pembinaan jabatan fungsional, dokumentasi dan kepustakaan, penataan kelembagaan dan ketatalaksanaan serta pelaporan keuangan Pusat.

Dalam melaksanakan tugas sebagaimana dimaksud, Bag TU mempunyai fungsi:

a) Penyiapan penyusunan perencanaan, pelaksanaan dan pengendalian program kerja dan anggaran Pusat.

b) Penyiapan evaluasi dan laporan pelaksanaan program kerja serta laporan kinerja Pusat.

c) Penyiapan penataan kelembagaan dan ketatalaksanaan Pusat.

d) Penyiapan pembinaan kepersonelan, pengelolaan keuangan, sarana dan prasarana Pusat.

e) Pengadminstrasian dan pembinaan jabatan fungsional serta perpustakaan Pusat.

f) Penyiapan administrasi pengadaan barang dan jasa serta pengelolaan barang milik negara. dan

g) Pengelolaan ketatausahaan dan kerumahtanggaan Pusat.

2) Bidang Pengembangan dan Pengelolaan Sistem Informasi Pertahanan (Banglola Sisfohan)

Bidang Pengembangan dan Pengelolaan Sistem lnformasi Pertahanan selanjutnya disebut Bid Banglola Sisfohan dipimpin oleh Kepala Bidang Pengembangan dan Pengelolaan Sistem lnformasi Pertahanan disebut Kabid Banglola Sisfohan mempunyai tugas melaksanakan pengembangan dan pengelolaan aplikasi, pengolahan database, manajemen bandwidth dan manajemen sistem informasi di lingkungan Kemhan RI.

a) Penyiapan penyusunan kebijakan teknis di bidang pengembangan dan pengelolaan aplikasi, pengolahan database, manajemen bandwidth dan manajemen sistem informasi di lingkungan Kemhan RI.

b) Pelaksanaan pengembangan dan pengelolaan sistem aplikasi, pengumpulan data, pengelolaan data, dan manajemen data dan informasi di lingkungan Kemhan RI.

c) Pelaksanaan pengembangan, analisis, pengolahan, pengelolaan dan penataan sistem informasi di lingkungan Kemhan RI.

d) Pemantauan, supervisi, evaluasi dan pelaporan di bidang Aplikasi, Database, dan manajemen Sistem Informasi di lingkungan Kemhan RI. dan

e) Pelaksanaan fasilitas kebijakan teknis di bidang Layanan Pengadaan Barang dan Jasa Secara Elektronik.

3) Bidang Infrastruktur Teknologi Informasi dan Komunikasi (Infra TIK).

Bidang lnfrastruktur Teknologi lnformasi dan Komunikasi selanjutnya disebut Bid lnfra TIK dipimpin oleh Kepala Bidang lnfrastruktur Teknologi lnformasi dan Komunikasi disebut Kabid lnfra TIK mempunyai tugas melaksanakan perencanaan dan pengembangan infrastruktur, operasional dan layanan

infrastruktur serta pemeliharaan infrastruktur teknologi informasi dan komunikasi di lingkungan Kemhan RI.

a) Penyiapan penyusunan kebijakan teknis di bidang perencanaan dan pengembangan infrastruktur, operasional dan layanan infrastruktur serta pemeliharaan infrastruktur teknologi informasi dan komunikasi di lingkungan Kemhan RI.

b) Pelaksanaan perencanaan dan pengembangan infrastruktur, operasional dan layanan infrastruktur serta pemeliharaan infrastruktur teknologi informasi dan komunikasi di lingkungan Kemhan RI.

c) Pelaksanaan fasilitasi kebijakan teknis di bidang perencanaan dan pengembangan infrastruktur, operasional dan layanan infrastruktur serta pemeliharaan infrastruktur teknologi informasi dan komunikasi di lingkungan Kemhan RI. dan

d) Pemantauan, supervisi, evaluasi dan pelaporan di bidang perencanaan dan pengembangan infrastruktur, operasional dan layanan infrastruktur serta pemeliharaan infrastruktur teknologi informasi dan komunikasi di lingkungan Kemhan RI.

4) Bidang Pengamanan Sistem Informasi dan Persandian (Pamsisinfosan).

Bidang Pengamanan Sistem lnformasi dan Persandian selanjutnya disebut Bid Pamsisinfosan dipimpin oleh Kepala Bidang Pengamanan Sistem lnformasi dan Persandian disebut Kabid Pamsisinfosan mempunyai tugas melaksanakan pengelolaan pengamanan sistem informasi dan persandian.

a) Penyiapan penyusunan kebijakan teknis di bidang pengelolaan pengamanan sistem informasi, pengembangan sistem persandian serta operasional dan pengamanan persandian di lingkungan Kemhan RI.

b) Pelaksanaan pengelolaan pengamanan sistem informasi, pengembangan sistem persandian serta operasional dan pengamanan persandian di lingkungan Kemhan RI.

c) Pelaksanaan pengembangan, pemeliharaan dan pengendalian pengamanan sistem informasi, pengembangan sistem persandian serta operasional dan pengamanan persandian di lingkungan Kemhan RI.

d) Pelaksanaan fasilitas kebijakan teknis di bidang pengelolaan pengamanan sistem informasi, pengembangan sistem persandian serta operasional dan pengamanan persandian di lingkungan Kemhan RI. dan

e) Pemantauan, supervisi, evaluasi dan pelaporan di bidang pengelolaan pengamanan sistem informasi, pengembangan sistem persandian serta operasional dan pengamanan persandian di lingkungan Kemhan RI.

5) Kelompok Jabatan Fungsional

a) Kelompok Jabatan Fungsional terdiri dari jabatan fungsional umum dan jabatan fungsional tertentu.

b) Jabatan Fungsional Tertentu sebagaimana dimaksud pada ayat (1) terbagi dalam berbagai kelompok jabatan fungsional sedangkan masing-masing kelompok terdiri dari Jabatan Fungsional Ahli dan Terampil.

c) Jabatan Fungsional Umum sebagaimana dimaksud pada ayat (1) adalah jabatan pelaksana.

d) Jabatan Fungsional sebagaimana dimaksud pada ayat (1) diatur tersendiri dengan peraturan Menteri Pertahanan Republik Indonesia, dan

e) Jenjang Jabatan Fungsional sebagaimana dimaksud pada ayat (1) diatur berdasarkan peraturan perundang-undangan yang berlaku.

6) Memahami Kebutuhan dan Ekspektasi Pihak Yang Berkepentingan.

a) Semua pihak yang berkepentingan terhadap SMKI, yaitu semua Personel (tetap ataupun kontrak), partner, vendor dan juga pihak pengguna layanan, yang mendukung infrastruktur teknologi informasi dan operasional bisnis, dan semua Personel yang menyediakan dan mendapatkan layanan dari infrastruktur teknologi informasi dan operasional bisnis Pusdatin Kemhan RI.

b) Kebutuhan atau persyaratan dari pihak yang berkepentingan terhadap SMKI baik dari pihak internal ataupun eksternal akan dipertimbangkan, ditinjau, dan diperbarui sepanjang waktu sebagai bagian dari perbaikan yang berkelanjutan.

Tabel 1 : Kebutuhan Persyaratan Dari Pemangku Kepentingan Internal

Pemangku kepentingan internal	Layanan yang di berikan
Manajemen	Tata Kelola, ketersediaan sumber daya, struktur organisasi, peran, tugas dan tanggung jawab, pedoman, kebijakan, objektif, strategi serta hubungan dengan pihak pengguna layanan
Personel	Pemenuhan komitmen, ketaatan ter - hadap peraturan, proses dan pedoman dan memastikan tidak ada gangguan operasional
Persyaratan Organisasi	Standar, pedoman, dan model yang harus diadopsi oleh organisasi
Bagian Tata Usaha	Persetujuan terhadap komitmen finansial seperti anggaran dalam penerapan SMKI
Bidang Pengembangan dan Pengelolaan Sistem Informasi Pertahanan	Pengembangan dan pengelolaan aplikasi, pengolahan *database*, dan manajemen sistem informasi (termasuk hak akses terhadap data dan sistem informasi)
Bidang Infrastruktur Teknologi Informasi dan Komunikasi	Perencanaan, pengembangan, operasi - onal, layanan, pengelolaan hak akses, serta pemeliharaan infrastruktur teknologi informasi dan komunikasi
Bidang Pengamanan Sistem Informasi dan Persandian	Pengelolaan sistem informasi dan persandian terkait keamanan dan hak akses. Memproteksi organisasi dari ancaman dan gangguan keamanan informasi

Tabel 2 : Kebutuhan Persyaratan Dari Pemangku Kepentingan Eksternal

Pemangku Kepentingan Eksternal	Layanan yang di berikan
Mitra	Memberikan pasokan barang dan jasa untuk memenuhi kebutuhan atau persyaratan Pihak pengguna layanan dan Pusdatin Kemhan sesuai dengan hukum,

	undang-undang, dan kontrak yang berlaku
Pihak pengguna layanan	Memberikan akses data dan informasi terkait layanan teknologi informasi dan sistem informasi seperti hak akses dan ketersediaan infrastruktur teknologi informasi dan sistem informasi

7) Sistem Manajemen Keamanan Informasi (SMKI).

Sesuai dengan persyaratan ISO/IEC 27001:2013, Pusdatin Kemhan RI telah menetapkan dan menerapkan Sistem Manajemen Keamanan Informasi (SMKI) dan menetapkan prosedur untuk memelihara dan meningkatkan sistem secara berkelanjutan. Dokumen induk SMKI mengikuti format yang sama dengan standar ISO/IEC 27001:2013 yang dikeluarkan oleh Badan Standardisasi Nasional dalam format dwi bahasa.

BAB IV
RUANG LINGKUP PEDOMAN SMKI

4. Ruang Lingkup Pedoman SMKI

a. Ruang Lingkup, Aset, Bidang, Aplikasi, dan Layanan

b. Ruang lingkup pedoman SMKI di Pusdatin Kemhan RI ini meliputi:

1) Ruang Server (*Data Center*), operasional dan manajemennya.

2) Layanan Teknologi Informasi yang diberikan kepada pihak internal atau eksternal

c. Kategori Aset yang termasuk dalam lingkup SMKI:

1) Aset perangkat keras dan infrastruktur Teknologi Informasi dan Sistem Informasi.

2) Aset digital

3) Aset orang

4) Aset layanan

5) Aset nyata (*tangible)*

d. Bagian atau bidang yang termasuk dalam lingkup SMKI

1) Bagian Tata Usaha (Bag TU).

2) Bidang Pengembangan dan Pengelolaan Sistem Informasi Pertahanan (Banglola Sisfohan).

3) Bidang Infrastruktur Teknologi Informasi dan Komunikasi (Infra TIK).

4) Bidang Pengamanan Sistem Informasi dan Persandian (Pamsisinfosan).

e. Aplikasi dan sistem informasi yang termasuk dalam lingkup SMKI.

No	Nama Aplikasi / Sistem Informasi	Fungsi
1	Aplikasi SIMPEG	Sistem informasi yang bisa memberikan beberapa informasi mengenai beberapa data personel dan ASN dalam satu instansi. Juga dijadikan sebagai alat untuk pengelolaan data personel atau organik /ASN meliputi pendataan, proses perencanaan pengadaan personel sampai dengan formasi kepegawaian. Aplikasi simpeg di dalam sebuah instansi dipergunakan untuk melakukan input, pengawasan dan monitoring beberapa data yang berhubungan dengan personel/ASN
2	SISFOHANNEG	Alat bantu utama proses pengambilan keputusan dalam pengelolaan pertahanan negara yang akuntabel
3	LPSE	unit kerja yang dibentuk untuk melayani Unit Layanan Pengadaan (ULP) atau Panitia/Pokja ULP Pengadaan yang akan melaksanakan pengadaan secara elektronik
4	Aplikasi SIMAK BMN	menghasilkan informasi yang diperlukan sebagai alat pertanggungjawaban atas pelaksanaan APBN serta pengelolaan/pengendalian BMN yang

		dikuasai oleh suatu unit akuntansi barang.
5	SIRUP	Entity Relationship Diagram sebagai sarana atau alat untuk mengumumkan RUP
6	Aplikasi SAIBA	Normalisasi Database aplikasi yang biasa dipakai untuk mencatat transaksi keuangan di beberapa Kementerian Negara/ Lembaga
7	Aplikasi SAS	Unified Modeling Language Pengelolaan proses Keuangan
8	Aplikasi SIMAN	Membantu proses perencanaan, penetapan status, penatausahaan, pemanfaatan, pemindahtanganan, dan penghapusan aset negara yang berbasis teknologi informasi dan komunikasi
9	Web Terintegrasi	Activity Diagram yang berjalan di website yang di miliki
10	WebMail	Sequence keamanan email yang khusus dari email yang masuk
11	SMDP KEMHAN	Wadah pelatihan yang diadakan
12	Aplikasi Wasgar	Pengawasan dalam rangka Audit internal
13	Aplikasi DPP/GPP	Sistem pembayaran Gaji atau pembelajaan, pegawai dan prajurit TNI
14	Aplikasi E-REKON-KEMKU	Berbasis web yang dikembangkan dalam rangka proses rekonsiliasi data transaksi keuangan dan penyusunan Laporan Keuangan Kementerian Negara/ Lembaga
15	Aplikasi Lapkin	Laporan kinerja tahunan yang dilakukan oleh masing-masing instansi serta dapat melihat profil instansi, prestasi kerja, grafik perbandingan penilaian pertahun,dan status pegawai

16	Aplikasi Krisna	Untuk meningkatkan sinergi perencanaan pusat dan daerah untuk mendukung pencapaian prioritas nasional dalam Rencana Kerja Lembaga/pemerintah
17	SIMRS Suyoto	Pengelolaan management rumah sakit yang terintegrasi
18	Fact Miner	Pemanfaatan data mining guna kelengkapan data yang sudah di kumpulkan
19	Aplikasi PPID	Pengelola dan penyampai dokumen yang dimiliki oleh badan publik
20	Aplikasi Input Data	perintah kepada komputer untuk digunakan pada proses lebih lanjut
21	Aplikasi Monev	menghimpun data dan informasi hasil pemantauan (data realisasi) pelaksanaan rencana pembangunan
22	GEOBIGDATA	Penentuan dan menganalisa penyebab dari suatu permasalahan yang terjadi di dalam sebuah system
23	Monitoring	Pengumpulan dan menganalisis suatu informasi bersadarkan indikator yang telah ditentukan seebelumnya
24	Sisfo Berita & Medsos	Analisis aplikasi berita dan informasi melalui medsos
25	Analisis Ancaman Negara	Setiap usaha dan kegiatan, baik dari dalam negeri maupun luar negeri yang dinilai membahayakan kedaulatan negara, keutuhan wilayah negara, dan keselamatan segenap bangsa
26	Pengelolaan Data Statistik IPH	Pengolahan data statistik merupakan bagian dari proses mengolah data menggunakan metode tertentu dengan tujuan untuk memperoleh informasi
27	E-takah Pusdatin	tata naskah elektronik yang menjadi rangkaian administrasi umum untuk memproses, mengolah, mengendalikan /

		mengawasi suatu persoalan atau kegiatan yang memerlukan proses tindak lanjut secara kronologis dalam sebuah tata naskah persuratan
28	Program Kerja Pusdatin	Rangkaian kegiatan yang dibut setiap satker guna pelaksanaan kegaiatan pada tahun yang awal
29	SI Agenda Infromasi Pusdatin	Kegaiatan pengolahan data dan statistik Pusdatin
30	Sinkronisasi DPP/GPP	Penggabungan dan menyemaan dalam pengajuan dan pembayaran gaji Prajurit maupun ASN
31	Interaktif Geo Dashboard	dashboard sumber daya pertahanan, dashboard situational awareness
32	SI Registrasi LPSE & SIRUP	Pendaftaran dan management pengelolaan user dan vendor dalam pengadaan
33	Pusdatin Clouds	Sebagai media penyimpanan sementara sebelum penggabungan di server internal
34	Bigdata Management	Pembagian slot data keseluruhan yang akan menjadi gabungan data-data secara menyeluruh
35	SIEHAN (SI Executif Pertahanan)	Penggunaan user yang memiliki ijin secara menyeluruh.
36	Singkronisasi Anggaran	Meningkatkan Keterpaduan perencanan dan penganggaran
37	SI Balitbang	Pemanfaatan system dalam melakukan penelitian yang lebih efektif
38	E-Library	User penggunaan secara umum baik di tingkat internal, siswa Unhan, Badiklat bahkan masyarakat umum
39	SMART CAMPUS UNHAN	Digitalisasi dalam management universitas yang dapat meningkatkan minat belajar siswa dan integrasi dengan Dikti

40	Interoperability Data Puskod	dalam memberikan/menyampaikan infor masi dan memberikan gambaran tentang Pusat Kodifikasi
41	Pengembangan IGD	Geo Bigdata
42	Sinkronisasi BMN Kemhan	Monitoring BMN yang dilaksanakan kemhan
43	Peta Digital Pertahanan	Potensi pertahanan yang digunakan untuk kepentingan pertahanan Nasional
44	Pembangunan SI Pranata Komputer	Tugas pokok Pranata Komputer adalah merencanakan, menganalisis, merancang, mengimplementasikan, mengembangkan dan atau mengoperasikan sistem informasi berbasis computer
45	Pembangunan Smart Office dan Sarana Pendukungnya Berbasis Private Cloud	Data center atau ruangan khusus dalam melakukan pengawasan baik data pada Cloud maupun yang terdapat di Server
46	Pembangunan Digitalisasi Tata Naskah dan Sarana Pendukungnya Berbasis Cloud	Administrasi internal sebagai monitoring surat menyurat secara digital
47	Pembangunan Layanan Data Terbuka	mendukung penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (SPBE) di lingkungan Kemhan dan pemadanan data Satker Kemhan pada Aplikasi Layanan Data Terbuka (LDT)

f. Layanan yang termasuk dalam lingkup SMKI sesuai Permenhan Nomor 14 Tahun 2019 tentang :

1) Penyusunan kebijakan teknis, program dan anggaran di bidang pengembangan dan pengelolaan sistem informasi pertahanan, infrastruktur teknologi informasi dan komunikasi, pengamanan sistem informasi dan persandian, pembinaan jabatan fungsional pranata komputer dan fungsional persandian di lingkungan Kemhan RI.

2) Penyusunan peraturan dan petunjuk di bidang pengembangan dan pengelolaan sistem informasi pertahanan, infrastruktur teknologi informasi dan komunikasi, pengamanan sistem informasi dan persandian, pembinaan jabatan fungsional pranata komputer dan fungsional persandian di lingkungan Kemhan RI.

3) Pelaksanaan pengembangan dan pengelolaan sistem informasi pertahanan dan manajemen *bandwidth*, infrastruktur teknologi informasi dan komunikasi, pengamanan sistem informasi dan persandian, pembinaan jabatan fungsional pranata komputer dan fungsional persandian di lingkungan Kemhan RI.

4) Pemantauan, supervisi, evaluasi dan pelaporan pelaksanaan pengembangan dan pengelolaan sistem informasi pertahanan dan manajemen *bandwidth*, infrastruktur teknologi informasi dan komunikasi, pengamanan sistem informasi dan persandian, pembinaan jabatan fungsional pranata komputer dan fungsional persandian di lingkungan Kemhan RI.

5) Pengelolaan, pemantauan dan evaluasi sistem keamanan informasi di lingkungan Kemhan RI dan pelaporan postur keamanan informasi dan potensi masalah berisiko tinggi serta memastikan setiap kepatuhan dan tindakan perbaikan dilaksanakan sebaik mungkin untuk setiap insiden keamanan informasi yang dilaporkan. dan

6) Pengelolaan ketatausahaan dan kerumahtanggaan pusat.

g. Pernyataan Penerapan (*Statement of Applicability*)

Bagian ini memberikan daftar kontrol yang Pusdatin Kemhan RI pilih dari ISO/IEC 27001:2013 Lampiran 'A' dan pertimbangan untuk pemilihan, untuk mengurangi risiko Keamanan Informasi yang teridentifikasi selama penilaian risiko. Ini adalah dokumen wajib sesuai persyaratan ISO/IEC 27001:2013. Dokumen terkait: Dokumen *Statement Of Applicability* Nomor: PK/05/VIII/2022/PUSDATIN untuk sasaran kendali.

BAB V
KEPEMIMPINAN SMKI

5. Kepemimpinan SMKI

a. Kepemimpinan dan Komitmen

Kepala Pusat Data dan Informasi Kementerian Pertahanan Republik Indonesia (Kapusdatin Kemhan RI) harus menunjukkan kepemimpinan dan komitmen sehubungan dengan Sistem Manajemen Keamanan Informasi dengan:

1) Memastikan kebijakan keamanan informasi dan tujuan keamanan informasi ditetapkan dan kompatibel dengan arah strategis organisasi.

2) Memastikan integrasi persyaratan sistem manajemen keamanan informasi ke dalam proses organisasi.

3) Memastikan bahwa sumber daya yang dibutuhkan untuk sistem manajemen keamanan informasi tersedia.

4) Mengkomunikasikan pentingnya manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan sistem manajemen keamanan informasi.

5) Memastikan bahwa sistem manajemen keamanan informasi mencapai hasil yang diinginkan.

6) Mengarahkan dan mendukung Personeldan pihak terkait untuk berkontribusi pada efektivitas sistem manajemen keamanan informasi.

7) Mempromosikan perbaikan secara terus-menerus. dan

8) Mendukung peran manajemen lain yang relevan untuk menunjukkan kepemimpinan mereka di bidang yang menjadi tanggung jawabnya.

b. Kebijakan

Kepala Pusat Data dan Informasi Kementerian Pertahanan Republik Indonesia (Kapusdatin Kemhan RI) telah membuat suatu kebijakan keamanan informasi yang:

1) sesuai dengan kebutuhan dan tujuan Pusdatin Kemhan RI.

2) mencakup tujuan keamanan informasi tingkat tinggi.

3) mencakup komitmen untuk memenuhi persyaratan yang berlaku terkait dengan keamanan informasi. dan

4) mencakup komitmen untuk perbaikan berkelanjutan SMKI.

Kebijakan keamanan informasi ini:

1) tersedia sebagai informasi yang terdokumentasi dalam sistem kontrol dokumen terintegrasi.

2) dikomunikasikan dalam organisasi. dan

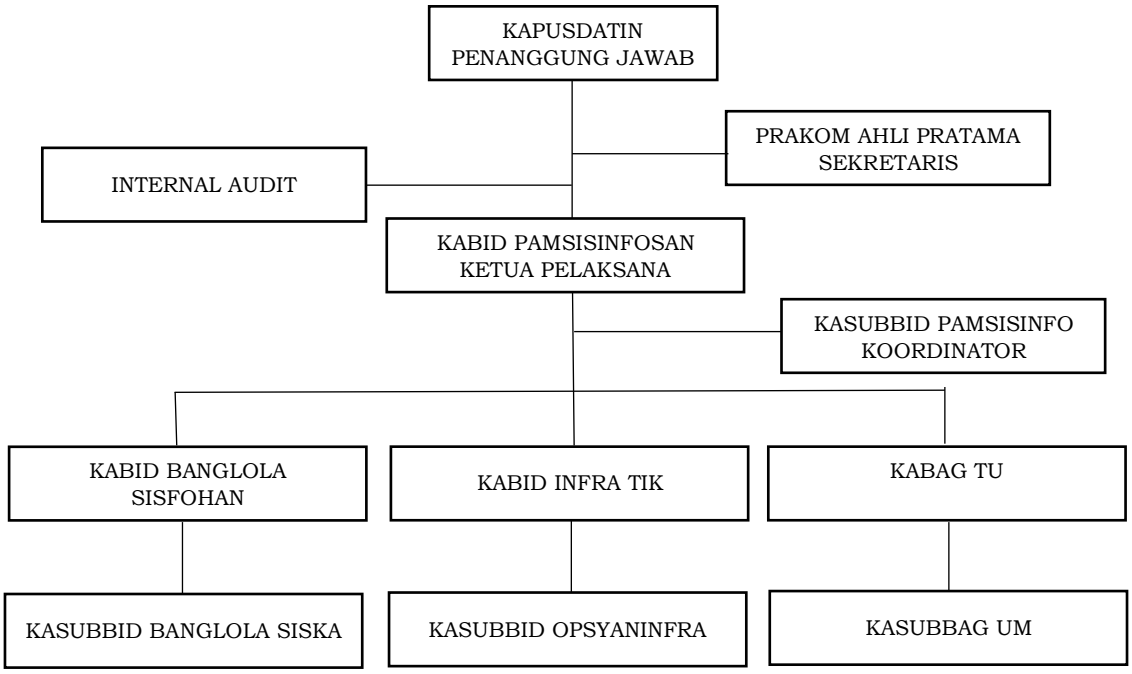
3) tersedia untuk pihak yang berkepentingan, ditentukan oleh Ketua Satgas SMKI Pusdatin Kemhan RI.

Kebijakan Keamanan Informasi ini sesuai dengan yang telah dijabarkan pada bagian 2 dokumen ini.

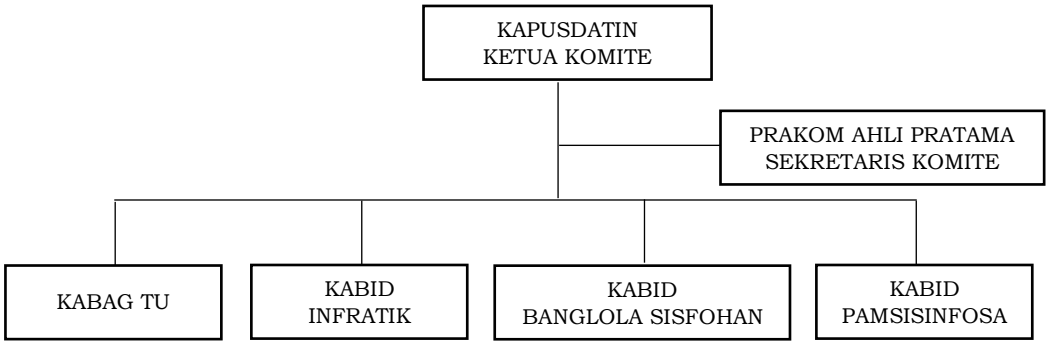
c. Struktur organisasi, peran, tanggung jawab dan otoritas dalam SMKI

Tujuan dari bagian ini adalah untuk menyediakan struktur pelaporan yang jelas bagi personel Sistem Manajemen Keamanan Informasi dan tanggung jawab yang harus ditetapkan untuk dilaksanakan oleh setiap individu sesuai perannya.

1) Struktur Organisasi Keamanan Informasi



2) Tugas dan Tanggung Jawab Komite Manajemen Keamanan Informasi (KMKI)



Struktur Komite Manajemen Keamanan Informasi

KMKI bertanggung jawab untuk memberikan pengawasan kepada Program Keamanan Informasi di tingkat organisasi. Tanggung jawab tersebut meliputi:

a) Memastikan bahwa tujuan dan rencana keamanan informasi Pusdatin Kemhan RI secara keseluruhan terpenuhi.

b) Meninjau dan menyetujui kebijakan dan prosedur keamanan informasi setidaknya sekali setahun atau ketika terjadi perubahan besar.

c) Meninjau dan menyetujui metodologi Penilaian Risiko keamanan informasi.

d) Meninjau dan menyetujui kriteria Penerimaan Risiko keamanan informasi.

e) Meninjau dan menyetujui Penilaian Risiko keamanan informasi, Risiko Residual dan Rencana Aksi Mitigasi Risiko.

f) Meninjau dan memantau tindakan perbaikan untuk setiap insiden keamanan informasi.

g) Menyediakan sumber daya yang cukup untuk mengembangkan, menerapkan, mengoperasikan dan memelihara SMKI.

h) Memastikan bahwa pelatihan dan kesadaran keamanan informasi yang relevan diberikan kepada semua personel kunci dalam ruang lingkup dan batasan SMKI.

i) Memberikan pengawasan terhadap inisiatif utama yang dilakukan untuk meningkatkan keamanan informasi di Pusdatin Kemhan RI.

j) Mengevaluasi efektivitas matrik KPI yang ditetapkan untuk fungsi organisasi/bisnis setiap tahun.

k) Memastikan bahwa audit internal SMKI yang independen dilakukan setiap tahun.

l) Memastikan bahwa audit SMKI pihak ketiga dilakukan setidaknya setahun sekali. dan

m) KMKI setidaknya melakukan rapat formal 2 kali dalam 1 tahun untuk memberikan pengawasan dan evaluasi terhadap program keamanan informasi.

3) Tugas dan Tanggung Jawab Ketua Tim Satgas Sistem Manajemen Keamanan Informasi.

Tugas dan tanggung jawab dari Ketua Tim Satgas Sistem Manajemen Keamanan Informasi meliputi:

a) Menginformasikan Komite Manajemen/Pengarah tentang masalah apapun seperti belanja modal, perubahan tak terjadwal dalam Kerangka SMKI di seluruh organisasi.

b) Memastikan bahwa semua pemangku kepentingan (khususnya anggota Tim Satgas SMKI) menyadari tanggung jawabnya.

c) Mengembangkan metodologi Penilaian Risiko dan kriteria penerimaan risiko.

d) Memulai dan meninjau Penilaian Risiko sesuai dengan rencana Penilaian Risiko.

e) Menyetujui Rencana Penanganan Risiko (sebagaimana berlaku) untuk menghindari kerusakan informasi dan aset pemrosesan informasi dalam situasi munculnya ancaman yang teridentifikasi.

f) Melaporkan postur keamanan informasi dan potensi masalah berisiko tinggi kepada Komite Manajemen Keamanan Informasi setiap dua kali dalam satu tahun.

g) Meninjau semua inisiatif utama yang dilakukan untuk meningkatkan keamanan informasi dalam ruang lingkup dan batasan SMKI.

h) Meninjau dan menganalisis insiden keamanan informasi yang dilaporkan di Pusdatin Kemhan RI setidaknya sekali setiap tahun dan memastikan bahwa rencana Ketidakpatuhan *(Non-Conformity)* dan Tindakan perbaikan *(Corrective Action)* yang dihasilkan selalu diterapkan.

i) Mengidentifikasi pelatihan kesadaran keamanan informasi yang relevan untuk diberikan kepada semua personel inti dalam ruang lingkup dan batasan SMKI.

j) Menyiapkan anggaran keamanan informasi tahunan, selaras dengan bisnis dan strategi TI.

k) Memimpin dan memelihara kesadaran keamanan informasi di dalam Pusdatin Kemhan RI dengan merencanakan dan melakukan sesi pelatihan berkoordinasi dengan dengan bagian Tata Usaha.

l) Mengkoordinasikan audit internal independen SMKI setiap tahun dan memfasilitasi penyelesaian masalah terkait keamanan yang dilaporkan oleh sistem dalam audit.

m) Melaporkan kepatuhan atau ketidakpatuhan terhadap SMKI yang diterbitkan secara berkala.

n) Bertindak sebagai titik kontak tunggal *(Site Point of Contact)* ketika berhadapan dengan lembaga penegak hukum saat mengejar sumber pelanggaran Keamanan Informasi oleh Personel atau entitas eksternal lainnya.

o) Bertindak sebagai titik kontak tunggal *(Site Point of Contact)* untuk melaporkan, mencatat, menyelidiki, dan mengeskalasi insiden dan kejadian Keamanan Informasi. dan

p) Meninjau dan memelihara kebijakan, prosedur dan tempat Keamanan Informasi yang memberikan perlindungan yang memadai tanpa mengorbankan persyaratan bisnis utama.

4) Tugas dan Tanggung Jawab Koordinator Keamanan Informasi

Koordinator Keamanan Informasi akan ditunjuk oleh Komite Manajemen Keamanan Informasi. Tanggung jawabnya meliputi:

a) Bertindak sebagai Koordinator Keamanan Informasi untuk setiap fungsi atau bagian yang ada di Pusdatin Kemhan RI.

b) Memantau kepatuhan dan melakukan kegiatan serupa dengan Kabag/Kabid di bagian/bidang masing-masing.

c) Melaporkan setiap insiden keamanan informasi, yang mencakup, namun tidak terbatas pada, kelemahan, kerentanan dan/atau pelanggaran keamanan informasi, kepada Kabid Pamsisinfosan. dan

d) Memastikan bahwa langkah-langkah keamanan informasi yang diperlukan diidentifikasi dan diterapkan dalam fungsi dan bidang masing-masing, dan semua pengguna mengetahui kebijakan, standar, prosedur, dan tempat keamanan informasi milik Pusdatin Kemhan RI.

5) Tugas dan Tanggung Jawab Anggota Tim Satgas Keamanan Informasi

Anggota Tim Satgas Sistem Manajemen Keamanan Informasi bertanggung jawab atas penetapan, penerapan, pengoperasian, pemantauan, peninjauan, pemeliharaan dan peningkatan SMKI untuk ruang lingkup dan batasan yang telah ditentukan. Tanggung jawabnya meliputi:

a) Berpartisipasi secara proaktif dalam inisiatif SMKI.

b) Mengkomunikasikan tujuan dan persyaratan SMKI ke bidang masing-masing.

c) Memantau kepatuhan dan melakukan kegiatan serupa dengan manajemen keamanan informasi di unit operasional masing-masing.

d) Melaporkan setiap insiden keamanan informasi, yang mencakup, namun tidak terbatas pada, kelemahan, kerentanan dan/atau pelanggaran terhadap keamanan informasi.

e) Memastikan bahwa langkah-langkah keamanan informasi yang diperlukan diidentifikasi dan diterapkan dalam bidang dan fungsinya masing-masing, dan semua pengguna mengetahui kebijakan, standar, prosedur, dan template keamanan informasi organisasi.

f) Meninjau dan mengukur efektivitas indikator kinerja utama terkait SMKI, yang ditetapkan untuk fungsi organisasi dan bisnis, setiap tahunnya.

g) Meninjau kebijakan dan prosedur keamanan informasi setiap tahunnya atau sesuai kebutuhan.

h) Meninjau metodologi penilaian risiko dan kriteria penerimaan risiko.

i) Meninjau penilaian risiko, risiko residual dan rencana aksi mitigasi risiko.

j) Mengembangkan rencana aksi untuk mencapai inisiatif utama yang dilakukan untuk meningkatkan keamanan informasi dalam ruang lingkup dan batasan SMKI.

k) Memastikan bahwa postur keamanan informasi dilaporkan ke Komite Manajemen Keamanan Informasi secara 2 (dua) kali dalam 1 (satu) tahun. dan

l) Anggota Tim Satgas Keamanan Informasi setidaknya melakukan rapat formal setiap kwartal sekali atau 3 bulan 1 kali, untuk memberikan tinjauan dan pemantauan secara berkala atas program keamanan informasi.

6) Tugas dan Tanggung Jawab Auditor Internal Keamanan Informasi

Auditor Internal SMKI harus tetap independen dan tidak akan terlibat dalam pelaksanaan pengendalian Keamanan Informasi. Rincian tanggung jawab Auditor SMKI meliputi:

a) Berpartisipasi dalam pertemuan rutin Tim Satgas SMKI dan memberikan umpan balik yang relevan tentang SMKI.

b) Mendapatkan pengetahuan materi pelajaran yang diperlukan dalam kaitannya dengan kontrol teknis dan prosedural yang diterapkan dalam ruang lingkup dan batasan SMKI.

c) Melakukan audit internal SMKI secara independen setiap tahun. dan

d) Berkoordinasi dengan pihak ketiga untuk audit eksternal SMKI.

BAB VI
PERENCANAAN

6. Perencanaan

a. Tindakan untuk mengatasi Risiko dan Peluang

1) Umum

Saat merencanakan Sistem Manajemen Keamanan Informasi, organisasi harus mempertimbangkan masalah dan persyaratan serta menentukan risiko dan peluang yang perlu ditangani untuk:

a) Memberikan jaminan bahwa Sistem Manajemen Keamanan Informasi dapat mencapai tujuan penggunaannya.

b) Meningkatkan efek yang diinginkan.

c) Mencegah atau mengurangi efek yang tidak diinginkan.

d) Mencapai perbaikan yang berkelanjutan.

e) Merencankan tindakan untuk mengatasi risiko dan peluang yang ada.

f) Merencanakan integrasi dan implementasi Sistem Manajemen Keamanan Informasi. dan

g) Mengevaluasi efektivitas tindakan.

2) Penilaian Risiko Keamanan Informasi

Pusdatin Kemhan RI telah menetapkan dan menerapkan prosedur penilaian risiko keamanan informasi dengan referensi dokumen Registrasi Aset Penilaian Risiko Tindak Lanjut Nomor: SOP/18/VIII/2022/PUSDATIN tentang Registrasi Aset Penilaian Risiko Tindak Lanjut, Prosedur tersebut menjelaskan hal-hal berikut:

a) Kriteria penerimaan risiko.

b) Kriteria untuk melakukan penilaian risiko keamanan informasi. dan

c) Kriteria untuk kategorisasi risiko dan peluang.

Prosedur Penilaian Risiko Keamanan Informasi mendefinisikan proses penilaian risiko keamanan informasi untuk mengidentifikasi risiko yang terkait dengan hilangnya kerahasiaan, integritas, dan ketersediaan informasi dalam ruang lingkup SMKI dan mengidentifikasi pemilik risiko. Prosedur tersebut memiliki rincian analisis risiko keamanan informasi dan evaluasi risiko keamanan informasi.

Organisasi harus merencanakan untuk mengatasi risiko dan peluang ini. Detail dari penilaian risiko dilakukan sesuai Prosedur Manajemen Risiko dengan referensi dokumen registrasi asset penilaian Risiko tindak lanjut Nomor: SOP/18/VIII/2022/PUSDATIN tentang Registrasi Asset Penilaian Risiko Tindak Lanjut, beserta catatannya di berbagai area.

3) Penanganan Risiko Keamanan Informasi

Dokumen prosedur Nomor: SOP/18/VIII/2022/ PUSDATIN tentang Registrasi Aset Penilaian Risiko Tindak Lanjut, serta Analisis dan Rencana Penanganan Risiko memberikan rincian mengenai kontrol yang diterapkan untuk mengelola risiko Sistem Informasi. Kedua dokumen tersebut ditinjau setidaknya setiap tahun oleh pemilik risiko, untuk:

a) Memastikan bahwa risiko yang diidentifikasi masih berlaku untuk organisasi.

b) Memastikan bahwa pengendalian yang diterapkan tetap memadai dan efektif. dan

c) Merekomendasikan tindakan untuk meningkatkan pengendalian yang diterapkan saat ini.

b. Tujuan Keamanan Informasi dan Rencana Untuk Mencapainya

Pusdatin Kemhan RI telah menetapkan tujuan keamanan informasi pada fungsi dan tingkat yang relevan. Tujuan keamanan informasi harus:

1) Konsisten dengan kebijakan keamanan informasi.

2) Dapat diukur (jika dapat dilakukan).

3) Mempertimbangkan persyaratan keamanan informasi yang berlaku, hasil dari penilaian risiko dan penanganan risiko.

4) Dikomunikasikan

5) Diperbarui sebagaimana mestinya.

BAB VII
DUKUNGAN

7. Dukungan

a. Sumber Daya

Pimpinan Pusdatin Kemhan RI berkomitmen penuh terhadap pembentukan, implementasi, pengoperasian, pemantauan, peninjauan, pemeliharaan dan peningkatan SMKI. Selain menciptakan dan melembagakan sistem keamanan informasi yang komprehensif, Komite Manajemen Keamanan Informasi Pusdatin telah menetapkan proses tinjauan manajemen untuk memastikan bahwa operasi SMKI berjalan sesuai rencana, dan bahwa sumber daya yang memadai didedikasikan untuk memungkinkan program keamanan informasi yang efisien dan proaktif. Komite Manajemen Keamanan Informasi Pusdatin memastikan bahwa semua pemangku kepentingan tetap mendapatkan informasi terkait SMKI. Selain itu, Komite Manajemen Keamanan Informasi juga memastikan dan memantau koordinasi kegiatan secara proaktif dan terintegrasi di seluruh area atau bidang yang ada di lingkungan Pusdatin Kemhan RI.

b. Kompetensi.

Pusdatin Kemhan RI memastikan bahwa semua personel yang ditugaskan dalam struktur organisasi SMKI memiliki kompetensi yang sesuai dengan tugas dan kewajibannya. Personel ditunjuk, direkrut atau dikontrak berdasarkan keterampilan, kompetensi, dan sertifikasi yang sesuai dengan posisi tersebut, serta diberikan pelatihan formal tambahan di tempat kerja atau di luar tempat kerja jika diperlukan. Catatan pelatihan untuk Personel disimpan oleh Bagian Tata Usaha di Pusdatin pada dokumen deskripsi pekerjaan, analisis kebutuhan pelatihan, catatan pelatihan, dan evaluasi personel.

c. Kesadaran.

Pusdatin Kemhan RI memastikan bahwa semua personel di lingkungan Pusdatin Kemhan RI menyadari pentingnya kegiatan keamanan informasi bagi mereka dan bagaimana mereka dapat berkontribusi untuk mencapai tujuan SMKI. Personel diperkenalkan dengan SMKI dan tanggung jawabnya dalam keamanan informasi sejak pertama kali mereka mulai bekerja

sampai meninggalkan atau mengundurkan diri dari pekerjaannya. Rencana SMKI ini tersedia untuk seluruh Personel sebagai panduan, kebijakan, rencana, prosedur dan instruksi kerja terkait SMKI.

Para Personel dan pemangku kepentingan di lingkungan Pusdatin Kemhan RI harus mengetahui:

1) Kebijakan keamanan informasi.

2) Kontribusi mereka terhadap efektivitas sistem manajemen keamanan informasi, termasuk manfaat dari peningkatan kinerja keamanan informasi.

3) Implikasi dari ketidaksesuaian dengan ketentuan & pedoman sistem manajemen keamanan informasi. dan

4) Semua pembaruan dalam kebijakan & prosedur organisasi, yang relevan dengan fungsi pekerjaannya.

d. Komunikasi.

Pusdatin Kemhan RI telah menentukan kebutuhan komunikasi internal dan eksternal yang relevan dengan sistem manajemen keamanan informasi termasuk:

1) Tentang apa yang harus dikomunikasikan.

2) Kapan harus berkomunikasi.

3) Dengan siapa berkomunikasi.

4) Siapa yang harus berkomunikasi.

5) Proses dimana komunikasi akan efektif

6) Untuk rincian prosedur komunikasi dapat merujuk pada dokumen prosedur komunikasi internal dan eksternal Nomor: SOP/02/VIII/2022/PUSDATIN tentang Prosedur Pertukaran Informasi.

e. Informasi Terdokumentasi

1) Umum

Sistem Manajemen Keamanan Informasi Pusdatin Kemhan RI mencakup:

a) Informasi terdokumentasi yang disyaratkan oleh Standar Internasional ISO 27001:2013

b) Informasi terdokumentasi yang ditentukan oleh organisasi dan peraturan pemerintah yang berlaku sebagai hal yang diperlukan untuk efektivitas sistem manajemen keamanan informasi.

2) Membuat dan Memperbarui

Saat membuat dan memperbarui informasi terdokumentasi, organisasi harus mencakup bahwa:

a) Identifikasi dan deskripsi (misalnya judul, tanggal, penulis, atau nomor referensi).

b) Format (misalnya bahasa, versi perangkat lunak, grafik) dan media (misalnya kertas, elektronik).

c) Reviu dan persetujuan untuk kesesuaian dan kecukupan. dan

d) Proses ini diatur dalam prosedur pengendalian dokumen Nomor: SOP/22/VIII/2022/ PUSDATIN tentang Prosedur Pengendalian Rekaman.

3) Pengendalian Informasi Terdokumentasi

Informasi terdokumentasi yang diperlukan oleh Sistem Manajemen Keamanan Informasi dan Standar Internasional dikendalikan melalui Prosedur Pengendalian Dokumen Nomor: SOP/22/VIII/2022/PUSDATIN tentang Prosedur Pengendalian Rekaman, untuk memastikan:

a) Dokumen tersedia dan sesuai untuk digunakan, di mana dan kapan diperlukan. dan

b) Dokumen dilindungi secara memadai (misalnya dari kebocoran informasi, penggunaan yang tidak semestinya, atau hilangnya integritas).

Prosedur Pengendalian Dokumen memberikan arahan dan panduan untuk:

a) Distribusi, akses, pengambilan dan penggunaan.

b) Penyimpanan dan pemeliharaan, termasuk keterbacaan dokumen.

c) Kontrol perubahan (misalnya kontrol versi). dan

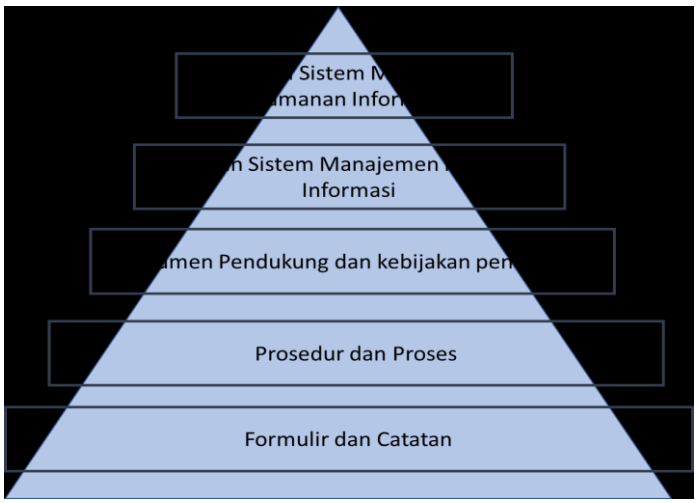
d) Retensi dan disposisi.

Informasi terdokumentasi yang berasal dari eksternal, ditentukan oleh organisasi diperlukan untuk perencanaan dan pengoperasian sistem manajemen keamanan informasi, diidentifikasi sebagai kebutuhan dan standardisasi, juga dikendalikan melalui Prosedur Pengendalian Dokumen.

Pengendalian rekaman dikelola melalui Prosedur Pengendalian Rekaman dan mencakup standar yang disyaratkan oleh ISO 27001:2013 serta rekaman internal yang diperlukan untuk operasional bisnis.

Untuk memenuhi persyaratan klausa 7.5, struktur dokumen Sistem Manajemen Keamanan Informasi sebagaimana gambar:

Gambar 1. Struktur Dokumen Sistem Manajemen Keamanan Informasi



BAB VIII
OPERASIONAL

8. Operasional

a. Perencanaan dan Pengendalian Operasional

1) Pusdatin Kemhan RI merencanakan, menerapkan dan mengendalikan proses yang di perlukan untuk memenuhi

persyaratan keamanan informasi dan untuk menerapkan tindakan yang ditentukan dalam klausa 6.1.

2) Pusdatin Kemhan RI menerapkan rencana mencapai sasaran keamananan informasi yang ditentukan dalam klausa 6.2.

3) Pusdatin Kemhan RI menyimpan informasi terdokumentasi sesuai rentang waktu yang ditentukan untuk memastikan proses telah dilakukan seperti yang telah direncanakan dan tertuang dalam. Laporan Evaluasi Manajemen Risiko.

4) Pusdatin Kemhan RI mengendalikan perubahan yang direncanakan dan melakukan tinjauan atas konsekuensi dari perubahan yang tidak terencana serta melakukan tindakan yang diperlukan untuk melakukan mitigasi setiap dampak yang muncul dan tertuang dalam Dokumen laporan Manajemen Perubahan.

5) Pusdatin Kemhan RI memastikan proses yang dilakukan oleh pihak ketiga ditentukan dan dikendalikan dengan baik. Dokumen yang butuhkan adalah dokumen Kontrak dan laporan pelaksanaan pekerjaan.

6) Prosedur operasional didokumentasikan dan tersedia untuk semua pengguna yang membutuhkannya.

7) Perubahan terhadap Instansi, proses bisnis, fasilitas pengolahan informasi dan sistem yang mempengaruhi keamanan informasi perlu dikendalikan.

8) Penggunaan sumber daya dimonitor, dievaluasi dan diproyeksikan dari kebutuhan kapasitas di masa depan untuk memastikan kinerja sistem yang diperlukan.

9) Pengembangan, pengujian, dan operasional lingkungan perlu dipisahkan untuk mengurangi risiko akses yang tidak sah atau perubahan lingkungan operasional.

10) Pendeteksian, pencegahan dan pemulihan kontrol untuk perlindungan terhadap *malware* perlu diterapkan.

11) Salinan back-up informasi, perangkat lunak dan hasil image dari sistem harus disimpan dan diuji secara teratur sesuai dengan aturan back-up yang telah disepakati.

12) Log kejadian untuk merekam kegiatan pengguna dan kejadian keamanan informasi pada perangkat TI perlu diterapkan, disimpan dan di kaji secara berkala.

13) Fasilitas *Logging* dan informasi log perlu dilindungi terhadap gangguan dan akses yang tidak sah.

14) Kegiatan operator dan administrator sistem harus tercatat *(logged)* dan catatan (log) tersebut harus dilindungi dan dikaji secara berkala.

15) Waktu dari semua sistem pengolahan informasi yang relevan perlu disinkronisasikan sesuai referensi sumber waktu tunggal.

16) Peraturan untuk mengendalikan instalasi perangkat lunak pada sistem operasional dan instalasi yang dilakukan oleh pengguna perlu ditetapkan.

17) Informasi tentang kerentanan teknis terhadap sistem informasi yang digunakan harus diperoleh secara tepat waktu. Dampak kerentanan tersebut perlu dievaluasi dan langkah yang tepat diambil untuk mengatasi risiko terkait.

18) Audit yang dilakukan terhadap system informasi perlu direncanakan dengan komperhensif dan disetujui pimpinan untuk meminimalisir gangguan terhadap proses bisnis.

19) Sebuah aturan perlu ditetapkan untuk mengelola risiko yang diakibatkan penggunaan *mobile device.* dan

20) Sebuah aturan perlu ditetapkan untuk melindungi informasi yang diakses, diproses atau disimpan pada perangkat *teleworking.*

b. Meja Bersih, Layar Bersih *(Clean Desk, Clean Screen)*

1) Semua perangkat komputasi maupun pengolahan data harus dalam keadaan *log off* atau dilindungi dengan *screensaver* yang aktif pada batas waktu tertentu (contohnya 5 menit) atau mekanisme penguncian akses jika tidak sedang digunakan. Pengamanan perangkat dapat menggunakan salah satu atau lebih mekanisme yaitu menggunakan password, PIN, *fingerprint*, *pattern* atau *face lock*. Hal ini termasuk pada perangkat komputer, laptop, tablet dan *smartphone* yang digunakan untuk menunjang pekerjaan.

2) Saat menampilkan informasi rahasia pada layar, perlu memastikan tidak ada pihak tidak berkepentingan yang dapat melihat informasi yang ditampilkan.

3) Setiap informasi rahasia atau kritikal terkait keberlangsungan bisnis, seperti informasi pada kertas maupun perangkat

penyimpanan harus diamankan, terutama saat personel tidak berada di tempat kerja.

4) Kertas yang menyantumkan informasi rahasia atau kritikal harus segeradiambil dari perangkat cetak. dan

5) Setiap informasi rahasia maupun kritikal yang terdapat di media kertas maupun media penyimpanan elektronik harus segera dihancurkan jika sudah tidak terpakai, atau disimpan di tempat yang aman sampai dengan informasi tersebut bisa dihancurkan atau dihapus.

c. Penilaian Risiko Keamanan Informasi

1) Pusdatin Kemhan RI melakukan penilaian Risiko keamanan informasi pada selang waktu terencana atau ketika perubahan dengan mempertimbangkan kriteria yang telah ditetapkan dalam klausa 6.1.2 a).

2) Pusdatin Kemhan RI menyimpan informasi terdokumentasi dari hasil penilaian Risiko keamanan informasi. dan

3) Pusdatin kemhan RI perlu menentukan kriteria penerimaan Risiko.

d. Penanganan Risiko Keamanan Informasi

1) Pusdatin Kemhan RI menerapkan rencana penanganan Risiko keamanan informasi.

2) Pusdatin Kemhan RI menyimpan informasi terdokumentasi hasil penanganan Risiko keamanan. dan

3) Data pendukung untuk penangan Risiko tertuang dalam Laporan Mitigasi Risiko.

e. Dokumen Terkait

1) Pedoman Akses Jaringan Nomor: PK/04/VIII/2022/ PUSDATIN.

2) Prosedur Pengelolaan Keamanan Jaringan Nomor: SOP/11/ VIII/2022/PUSDATIN.

3) Prosedur Registrasi Aset, Penilaian Risiko dan Tindaklanjut Nomor: SOP/18/VIII/2022/PUSDATIN

4) Prosedur Penanganan Insiden Keamanan Informasi Nomor: SOP/20/VIII/2022/PUSDATIN tentang Penanganan Insiden Informasi.

BAB IX
EVALUASI KINERJA

9. Evaluasi Kinerja

a. Pemantauan, Pengukuran, Analisis dan Evaluasi

Tinjauan Umum

Untuk melakukan evaluasi kinerja SMKI Pusdatin Kemhan RI, maka perlu ditentukan:

1) Hal-hal yang perlu dipantau dan diukur, termasuk proses dan kontrol terhadap keamanan informasi.

2) Metode yang digunakan dalam melakukan pemantauan, pengukuran, analisis dan evaluasi untuk memastikan validitas hasil evaluasi.

3) Waktu pelaksanaan pemantauan dan pengukuran.

4) Pihak yang melakukan pemantauan dan pengukuran.

5) Pelaksanaan analisa dan evaluasi terhadap hasil dari pemantauan dan pengukuran. dan

6) Pihak yang menganalisis dan mengevaluasi hasil pemantauan.

Seluruh aktivitas ini dicatat, dikomunikasikan, dan digunakan dengan tepat untuk mengevaluasi dan meningkatkan kinerja serta efektivitas SMKI Pusdatin Kemhan RI, termasuk:

1) Memantau kemajuan proses dalam memenuhi kebijakan, pencapaian tujuan dan target, serta perbaikan yang berkelanjutan.

2) Menyediakan data untuk mendukung atau mengevaluasi pengendalian operasional.

3) Menyediakan data untuk mengevaluasi kinerja SMKI.

Pengukuran dilakukan dengan proses yang sesuai untuk memastikan validitas hasil, dengan memperhatikan:

1) Kompetensi personel.

2) Metode kontrol kualitas yang sesuai.

Pusdatin Kemhan RI mengoperasikan dan mengatur konfigurasi untuk memastikan bahwa seluruh peralatan dikalibrasi atau diverifikasi perangkat lunak yang digunakan perlu divalidasi dan dipelihara dengan baik seperti yang telah ditetapkan pada Prosedur Kontrol Kalibrasi, Verifikasi dan Validasi SMKI Pusdatin Kemhan RI.

b. Audit Internal

Cakupan Audit Internal

Pusdatin Kemhan RI melakukan audit internal sesuai kurun waktu yang direncanakan dengan memperhatikan hal-hal sebagai berikut:

1) Kesesuaian dengan kebutuhan Pusdatin Kemhan RI.

2) Implementasi SMKI di Pusdatin Kemhan RI. Dan

3) Efektiftifitas dalam mencapai kebijakan, tujuan, dan target dari SMKI Pusdatin Kemhan RI.

Pengembangan Program Audit

Pusdatin Kemhan RI memastikan bahwa:

1) Penentuan status pemenuhan atas kepatuhan terhadap dokumen SMKI dan pentingnya setiap proses yang akan dilakukan audit.

2) Jumlah frekuensi audit ditetapkan berdasarkan hasil audit yang telah dilaksanakan sebelumnya dan pertimbangan terhadap risiko, keandalan, status, dan pentingnya setiap proses tersebut.

3) Rencana audit dilaksanakan secara terjadwal dan dikomunikasikan dengan baik.

4) Tim Audit Internal terbentuk.

5) Auditor internal yang dipilih harus memenuhi syarat kompetensi dan independensi.

6) Auditor Utama yang ditunjuk untuk setiap audit internal sesuai dengan kebutuhan.

7) Tugas dan Tanggung jawab terkait dengan audit didefinisikan dengan baik, dipahami dan dilaksanakan oleh tim auditor internal. dan

8) Tim audit internal sekurang-kurangnya melakukan audit satu kali dalam setahun.

Pemilihan Auditor Internal

Untuk memastikan objektivitas auditor, perlu dipilih auditor internal independen dari bidang yang akan dilakukan audit dengan mempertimbangkan:

1) Latar belakang pengetahuan dan keterampilan dari auditor internal yang diakui baik oleh lembaga akreditasi nasional maupun internasional.

2) Pengalaman dan pelatihan yang sudah diikuti oleh Auditor.

3) Auditor independen, harus memiliki dasar pemahaman terkait proses atau bidang yang akan diaudit. dan

4) Independensi dari Auditor Internal.

Tahapan Persiapan Audit

Audit disiapkan sesuai dengan *template* pada Laporan Audit Internal, sebagai berikut:

1) Relevansi dari seluruh dokumen dan catatan sistem manajemen.

2) Ketersediaan dokumen yang berhubungan dengan kriteria audit dan Standar nasional ataupun internasional.

3) Daftar *checklist* berdasarkan *template* Laporan Audit Internal dengan standard tertentu,, termasuk pengecekan daftar item tambahan yang diperlukan.

4) Tanggal kegiatan audit. dan

5) Penerbitan daftar audit kepada Kepala Pusdatin Kemhan RI untuk pratinjau.

Tinjauan Manajemen terkait Audit

Pusdatin Kemhan RI memastikan bahwa:

1) Akan dilakukan peninjauan terhadap kesimpulan hasil audit.

2) Rencana perbaikan terhadap hasil rekomendasi audit tersusun.

3) Hasil laporan audit internal diserahkan kepada Kepala Pusdatin Kemhan RI. dan

4) Hasil dari audit internal dan setiap tindakan korektif dilaporkan pada pertemuan tinjauan manajemen untuk mengevaluasi efektivitas dan implementasi audit.

c. Tinjauan Manajemen

1) Tujuan tinjauan manajemen

Pusdatin Kemhan RI secara resmi meninjau kesesuaian, kecukupan, dan efektivitas SMKI melalui pertemuan tinjauan manajemen keamanan informasi secara berkala.

2) Frekuensi tinjauan manajemen

Rapat tinjauan manajemen pada keamanan informasi dijadwalkan, diatur dan diadakan, minimal setiap 6 bulan, dengan dihadiri oleh:

a) Kapusdatin Kemhan RI.

b) Ka Bag TU.

c) Ka Bid Banglola Sisfohan

d) Ka Bid Pamsisfinfosan

e) Ka Bid Infratik

f) Peserta lain.

Jika salah satu dari list peserta berhalangan hadir, maka harus mengirim perwakilan peserta sebagai pengganti pada rapat tinjauan manajemen.Jika ingin menambahkan *item* ke dalam agenda tinjauan manajemen, peserta perlu mengajukan permintaan kepada Kapusdatin Kemhan RI.

3) Tindakan yang dihasilkan

Rapat tinjauan manajemen keamanan informasi menghasilkan laporan tindakan yang bersifat korektif dan/atau Langkah pencegahan, atau persetujuan untuk mengambil tindakan guna meningkatkan seluruh sistem, layanan, proses dan sumber daya manajemen keamanan informasi.

4) Hasil tinjauan manajemen

Hasil tinjauan manajemen dicatat dalam bentuk *form* yang ditetapkan dengan jelas dan mencakup seluruh tanggung jawab pribadi pada Pusdatin Kemhan RI.

Kapusdatin Kemhan RI bertanggung jawab untuk memastikan bahwa *form* disiapkan diterbitkan dan item tindakan ditindaklanjuti.

5) Dokumentasi

Dokumentasi terkait tinjauan manajemen yang dihasilkan, disimpan untuk mendukung prosedur tinjauan manajemen dan dicantumkan dalam Daftar Dokumentasi SMKI serta dikendalikan menurut Prosedur Pengendalian terhadap Dokumentasi Sistem Manajemen Keamanan Informasi Pusdatin Kemhan RI.

BAB X
PERBAIKAN KINERJA

10. Perbaikan Kinerja

a. Ketidaksesuaian dan Tindakan Korektif

Ketidaksesuaian yang terjadi termasuk yang timbul dari keluhan, perlu dilakukan tindakan yang tepat untuk menjaga efektivitas SMKI melalui Prosedur Pengendalian Dokumen Nomor: SOP/22/VIII/2022/PUSDATIN tentang Prosedur Pengendalian Rekaman, dengan langkah:

1) Melakukan pengendalian dan tindakan korektif serta menangani konsekuensinya.

2) Melakukan evaluasi terhadap kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian agar kejadian tersebut tidak terulang atau terjadi di tempat lain dengan:

a) Meninjau dan menganalisis ketidaksesuaian.

b) Menentukan penyebab ketidaksesuaian. Dan

c) Menentukan ketidaksesuaian serupa berpotensi terjadi berulang.

3) Melakukan tindakan apa pun yang diperlukan.

4) Melakukan peninjauan efektivitas tindakan korektif yang akan diambil. dan

5) Membuat perubahan yang diperlukan dalam Sistem Manajemen Keamanan Informasi.

Tindakan korektif harus sesuai dengan efek ketidaksesuaian yang dihadapi. Pusdatin Kemhan RI perlu menyimpan informasi terdokumentasi sebagai bukti dari:

1) Sifat ketidaksesuaian dan tindakan selanjutnya yang diambil.

2) Hasil dari setiap tindakan korektif.

Formulir terkait Permintaan Perubahan Nomor: LI/03/VIII/2022/ PUSDATIN.

b. Perbaikan Berkelanjutan

Pusdatin Kemhan RI perlu memperbaiki kesesuaian, kecukupan dan efektivitas SMKI secara berkala sesuai dengan kebutuhan. Masukan untuk perbaikan berkelanjutan dapat berupa:

1) Perubahan dalam kebijakan dan tujuan keamanan.

2) Hasil audit dan laporan tinjauan manajemen.

3) Laporan insiden keamanan informasi.

4) Analisis monitoring.

5) Tindakan korektif dan pencegahan.

6) Perubahan proses bisnis.

7) Perubahan lingkungan (ancaman dan kerentanan baru). Dan

8) Praktik keamanan informasi yang telah terbukti kehandalannya.

Formulir terkait Notulen Hasil Rapat Tinjauan Manajemen Nomor: LI/26B/VIII/2022/PUSDATIN.

BAB XI
PENUTUP

11. Penutup

a. Demikian Pedoman Kerja Sistem Manajemen Keamana Informasi ini di buat, sebagai acuan dalam pengamanan informasi di Pusdatin.

b. Pedoman ini berlaku sejak di tandatangani dan ketentuan yang belum tercantum dalam pedoman ini akan diatur lebih lanjut dengan memperhatikan perkembangan Sistem Manajemen Keamanan Informasi.

c. Dokumen asli dari prosedur ini dipelihara dan dikendalikan oleh dokumen kontrol di Bidang Pamsisinfosan Pusdatin Kemhan RI.

d. Penggunaan dokumen asli ataupun dokumen salinan harus mengikuti aturan yang tertulis pada Dokumen Prosedur Pengendalian Dokumen Nomor: SOP/22/VIII/2022/PUSDATIN.

Dikeluarkan di Jakarta
Pada tanggal Agustus 2022

Kepala Pusat Data dan Informasi,

Rionardo
Brigadir Jenderal TNI