LEMBAGA ADMINISTRASI NEGARA
REPUBLIK INDONESIA

SALINAN
PERATURAN KEPALA LEMBAGA ADMINISTRASI NEGARA
REPUBLIK INDONESIA
NOMOR 13 TAHUN 2022
TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN LEMBAGA ADMINISTRASI NEGARA

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA LEMBAGA ADMINISTRASI NEGARA,

Menimbang : a. bahwa untuk menjamin keberlangsungan sistem pemerintahan berbasis elektronik di lingkungan Lembaga Administrasi Negara, perlu meminimalkan dampak risiko keamanan informasi;

b. bahwa untuk meminimalkan dampak risiko sebagaimana dimaksud dalam huruf a, perlu menetapkan pedoman pelaksanaan manajemen keamanan informasi sistem pemerintahan berbasis elektronik di lingkungan Lembaga Administrasi Negara;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Lembaga Administrasi Negara tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Lembaga Administrasi Negara;

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

2. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 182);
4. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
5. Peraturan Presiden Nomor 79 Tahun 2018 tentang Lembaga Administrasi Negara (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 162);
6. Peraturan Lembaga Administrasi Negara Nomor 8 Tahun 2020 tentang Organisasi dan Tata Kerja Lembaga Administrasi Negara (Berita Negara Republik Indonesia Tahun 2020 Nomor 494);
7. 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);

8. Peraturan Kepala Lembaga Administrasi Negara Nomor 9 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Lembaga Administrasi Negara;
9. Peraturan Kepala Lembaga Administrasi Negara Nomor 5 Tahun 2020 tentang Satu Data Lembaga Administrasi Negara;

MEMUTUSKAN:

Menetapkan : PERATURAN KEPALA LEMBAGA ADMINISTRASI NEGARA TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN LEMBAGA ADMINISTRASI NEGARA.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Kepala ini yang dimaksud dengan :

1. Lembaga Administrasi Negara yang selanjutnya disingkat LAN adalah lembaga pemerintah non kementerian yang diberi kewenangan melakukan pengkajian dan pendidikan dan pelatihan aparatur sipil negara sebagaimana diatur dalam undang-undang yang mengatur aparatur sipil negara.
2. Sistem Pemerintahan Berbasis Elektronik LAN yang selanjutnya disingkat SPBE LAN adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE LAN.
3. Manajemen Keamanan Informasi SPBE LAN adalah serangkaian proses untuk mencapai penerapan keamanan SPBE LAN yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE

LAN yang berkualitas.

4. Pusat Data dan Informasi adalah unit kerja yang menyelenggarakan tugas dan fungsi di bidang teknologi informasi dan komunikasi dengan melibatkan seluruh unit kerja di lingkungan LAN.

BAB II
PELAKSANAAN

Pasal 2

(1) Manajemen Keamanan Informasi SPBE LAN merupakan serangkaian proses yang terdiri atas:
   a. penetapan ruang lingkup;
   b. penetapan penanggung jawab;
   c. perencanaan;
   d. dukungan pengoperasian;
   e. evaluasi kinerja; dan
   f. perbaikan berkelanjutan.

(2) Manajemen Keamanan Informasi SPBE LAN sebagaimana dimaksud dalam ayat (1) dilaksanakan berdasarkan pedoman Keamanan Informasi SPBE LAN sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Kepala Lembaga ini.

Pasal 3

(1) Pengendalian terhadap Pelaksanaan Manajemen Keamanan Informasi SPBE LAN dilakukan dengan menggunakan dokumen dan rekaman sebagaimana tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Kepala Lembaga ini.

(2) Pengendalian sebagaimana dimaksud pada ayat (1) dilakukan oleh tim sekretariat Manajemen Keamanan Informasi SPBE LAN

BAB III

PEMANTAUAN DAN EVALUASI

Pasal 4

Terhadap pelaksanaan Manajemen Keamanan Informasi SPBE LAN dilakukan pemantauan dan evaluasi.

Pasal 5

(1) Pemantauan sebagaimana dimaksud dalam Pasal 4 dilakukan untuk memastikan prosedur dan pengendalian Manajemen Keamanan Informasi SPBE LAN dilaksanakan secara efektif sesuai ketentuan yang berlaku.
(2) Pemantauan sebagaimana dimaksud pada ayat (1) dilakukan oleh tim yang melakukan fungsi pengawasan.

Pasal 6

(1) Evaluasi terhadap pelaksanaan Sistem Manajemen Keamanan Informasi SPBE LAN dilakukan untuk menjamin efektivitas dan meningkatkan keamanan informasi di lingkungan LAN.
(2) Evaluasi sebagaimana dimaksud pada ayat (1) dilakukan secara berkala oleh Pusat Data dan Informasi.

Pasal 7

Peraturan Kepala Lembaga ini mulai berlaku pada tanggal disebarluaskan.

Agar setiap orang mengetahuinya, memerintahkan penyebarluasan Peraturan Kepala Lembaga ini dengan penempatannya dalam laman resmi LAN.

Ditetapkan di Jakarta
pada tanggal 9 Juni 2022

KEPALA
LEMBAGA ADMINISTRASI NEGARA
REPUBLIK INDONESIA,

Ttd.

ADI SURYANTO

Disebarluaskan di Jakarta
pada tanggal 9 Juni 2022

SEKRETARIS UTAMA
LEMBAGA ADMINISTRASI NEGARA
REPUBLIK INDONESIA,

Ttd.

RENI SUZANA

Salinan ini sesuai dengan aslinya,
KEPALA BIRO HUKUM DAN HUBUNGAN MASYARAKAT
LEMBAGA ADMINISTRASI NEGARA
REPUBLIK INDONESIA,

TRI ATMOJO SEJATI

LAMPIRAN
KEPUTUSAN KEPALA LEMBAGA ADMINISTRASI NEGARA
NOMOR 13 TAHUN 2022
TENTANG
MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN LEMBAGA ADMINISTRASI NEGARA

BAB I

KEBIJAKAN DAN STANDAR MANAJEMEN KEAMANAN INFORMASI SPBE LAN

A. Ruang Lingkup Keamanan Informasi

1. Tujuan

   Kebijakan dan Standar Manajeman Keamanan Informasi ini digunakan sebagai panduan pelaksanaan dalam rangka melindungi aset informasi LAN dari berbagai dari berbagai bentuk ancaman keamanan informasi baik dari dalam maupun luar Lingkungan LAN, yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin kerahasiaan *(confidentiality),* keutuhan *(integrity),* dan ketersediaan *(availibilty)* asset informasi agar selalu terjaga dan terpelihara dengan baik. Untuk memastikan pengelolaan informasi tersebut, LAN berkomitmen menerapkan sistem manajemen keamanan informasi dengan mengacu kepada Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan berbasis Elektronik dan sesuai dengan Standar SNI ISO/IEC 27001:2013 (Sistem Manajamen Keamanan Informasi).

2. Acuan Normatif

   Dalam pelaksanaan Manajemen Keamanan Informasi SPBE LAN selain berpedoman pada Peraturan Kepala Lembaga ini, juga mengacu pada:

   a. Undang-Undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58,

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

b. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
c. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
d. 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);
e. SNI ISO/IEC 27001:2013 Sistem Manajemen Keamanan Informasi;
f. SNI ISO 19011 Panduan Audit Sistem Manajemen;
g. ISO 31000 *Risk Management – Principles and Guidelines*; dan
h. ISO/TR 10013:2001 *Guidelines for Quality Management System Documentation*.

B. Identifikasi Permasalahan Keamanan Informasi

Pengembangan, penerapan dan pemeliharaan Manajemen Keamanan Informasi SPBE LAN tergantung dari berbagai faktor (penguat/pelemah) yang berasal dari pihak internal maupun eksternal LAN. Faktor – faktor tersebut kemudian dijabarkan sebagai berikut.

Tabel 1. Identifikasi Permasalahan dan Faktor Penyebabnya

No	Identifikasi Permasalahan	Faktor Penguat/Pelemah	
		Internal	Eksternal
1.	Pemenuhan persyaratan peraturan perundang-undangan		Sebagai instansi pemerintah, LAN harus memenuhi peraturan perundangan terkait

			manajemen keamanan informasi yang dipersyaratkan
2.	Sistem Penganggaran Lembaga Pemerintah		Keterbatasan alokasi anggaran teknologi informasi dan komunikasi untuk LAN.
3.	Ancaman Kejahatan Internet	Mengunduh dari laman Internet tidak aman	Koneksi komunikasi dengan Internet rawan disusupi oleh pihak lain
4.	Pengetahuan Anggota Tim Keamanan Informasi	Kemampuan Tim Keamanan Informasi LAN masih terbatas baik kuantitas dan kualitas dalam mengembangkan Manajemen Keamanan Informasi SPBE LAN	
5.	Budaya dan Nilai Organisasi	Budaya dan Nilai Organisasi LAN (integritas, Kejujuran, Kecepatan, Keterbukaan, Kerjasama Tim) menjadi dasar kekuatan mengembangkan Manajemen Keamanan Informasi SPBE LAN	
6.	Komitmen Manajemen Puncak	Manajemen puncak LAN memiliki komitmen yang sangat kuat terhadap penerapan Manajemen Keamanan Informasi SPBE LAN	-

7.	Kegagalan aplikasi	a. Kegagalan tim pelaksana menginstalasi aplikasi; b. kegagalan layanan aplikasi; c. Keusangan sistem operasi/aplikasi; dan d. Ketiaadaan pengamanan di level aplikasi (WAF) ~~faktor pelemah).~~	a. Kegagalan vendor menginstal aplikasi; b. serangan virus/malware; dan c. peretasan aplikasi
8.	kegagalan server	a. Kegagalan fungsi server; dan b. Kerusakan fisik server.	a. Pemadaman listrik; dan b. peretasan server.
9.	Kegagalan jaringan	a. Kerusakan fisik switch dan kabel jaringan; b. Kerusakan port/hub kabel; c. Keusangan perangkat jaringan; dan d. Ketiadaan perangkat keamanan jaringan (*firewall*).	serangan virus/*malware*.
10.	Kehilangan data	a. Belum ada SOP backup data; b. Backup data masih sporadis dan belum rutin; c. Media backup data masih lokal, untuk yang beda lokasi belum tersedia; dan d. Belum memiliki NAS (*Network attached*	serangan virus/*malware*.

		Storage) atau DRC (*Data Recovery Center*).	
11.	Pengguna tidak melakukan penggantian password secara berkala dan pembuatan password tidak sesuai standar keamanan	Tingkat pengetahuan keamanan informasi pengguna yang masih rendah.	a. Kejahatan *phising*; dan b. serangan virus/*malware*.

C. Ruang Lingkup Keamanan Informasi

1. Kebijakan dan Standar ini berlaku untuk pengelolaan pengamanan seluruh aset informasi LAN dan dilaksanakan oleh seluruh unit kerja, pegawai LAN baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi (TIK), dan pihak ketiga dilingkungan LAN. Cakupan ruang lingkup sertifikasi SNI ISO/IEC 27001:2013 Sistem Manajemen Keamanan Informasi ada di Pusat Data dan Sistem Informasi Lembaga Administrasi Negara.
2. Aset informasi LAN adalah aset dalam bentuk:
   a. Data, Informasi dan dokumen, meliputi: data anggaran dan keuangan, data perencanaan lembaga, data kepegawaian, data assessment, data rancangan peraturan perundang-undangan, dokumen telaahan hukum, dokumen bantuan hukum (Litigasi dan non Litigasi), data evaluasi kelembagaan dan organisasi, database aplikasi, kode sumber aplikasi, data akses ke database aplikasi, data akses ke sistem aplikasi, data akses ke server, data kajian dan inovasi, data test/seleksi calon pelatihan, data surat keterangan pelatihan, data nilai peserta pelatihan, data evaluasi pelatihan, data akreditasi/sertifikasi, data perencanaan Jabatan Fungsional (JF), data seleksi & *inpassing* JF, data penilaian Angka Kredit JF, Data Uji kompetensi JF, data monitoring dan evaluasi JF, data penilaian akreditasi lembaga pelatihan, data aset dan barang milik negara (BMN), data pengamanan pejabat dan kantor, dokumen pengadaan barang dan jasa, dokumen penawaran kontrak, dokumen perjanjian

kerahasiaan, dokumen rapat pimpinan, dokumen arsip vital, dokumen pengawasan (audit), data mahasiswa, data administrasi kemahasiswaan, data akademik kemahasiswaan, data laboratorium;

b. Perangkat lunak, meliputi: seluruh perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat bantu pengembangan sistem;
c. Perangkat infrastruktur, meliputi: perangkat komputer, perangkat server, perangkat jaringan dan komunikasi, koneksi Internet, perangkat keamanan jaringan/server, akses ke jaringan/infrastruktur, dan perangkat pendukung lainnya; dan
d. Aset tak berwujud (*intangible asset*), meliputi: pengetahuan, pengalaman, keahlian, citra, dan reputasi.

3. Perangkat Lunak aplikasi yang dikelola oleh LAN, antara lain:
   a. Pengelolaan Sistem Informasi Layanan Administrasi

      Pengelolaan Sistem Informasi Layanan Administrasi, antara lain terdiri atas:

No.	Layanan SPBE	Layanan SPBE	Sistem Informasi Pendukung	Keterangan
1.	Perencanaan dan Penganggaran	Layanan Perencanaan Kerja dan Penganggaran	a. SIREVA b. KRISNA c. SAKTI	Aplikasi Disediakan oleh Kemenkeu
		Layanan Monev Perencanaan dan Kinerja Anggaran	a. Monev Bappenas b. SMART	Aplikasi disediakan oleh Kemenkeu, dan Bappenas
2.	Keuangan	Layanan Pembuatan Data Kontrak, RPD Harian, SPM, LPJ Bendahara bagi Satker	SAS	Aplikasi Disediakan oleh Kemenkeu
		Layanan penatausahaan, pembukuan dan pertanggungjawaban Bendahara	SAKTI	Aplikasi Disediakan oleh Kemenkeu
		Pencatatan realisasi dan serapan anggaran per Bendahara LAN	SIK LAN	Aplikasi dikembangkan sendiri oleh LAN
3.	Pengelolaan Barang Milik	Layanan Pengelolaan BMN	SIMAK BMN	Aplikasi Disediakan oleh Kemenkeu

	Negara (BMN)	Layanan Pengelolaan BMN	SAKTI	Aplikasi Disediakan oleh Kemenkeu
4.	Pengadaan Barang dan Jasa	Layanan PerencanaanUmum Pengadaan	SIRUP	Aplikasi disediakan oleh LKPP
		Layanan Pengadaan	LPSE	Aplikasi disediakan oleh LKPP
5.	Kepegawaian	Layanan Manajemen Kepegawaian	Sistem Manajemen Kepegawaian LAN	Aplikasi dikembangkan sendiri oleh LAN
		Layanan pelayanan Kepegawaian Badan Kepegawaian Negara	SAPK	Aplikasi disediakan oleh BKN
		Layanan absensi pegawai	Intranet	Aplikasi dikembangkan sendiri oleh LAN
		Layanan pengelolaan kinerja pegawai	SIKTKP	Aplikasi dikembangkan sendiri oleh LAN
6.	Kearsipan	Layanan Pengelolaan Arsip dan Nota Dinas	a. eSign PersuratanIntranet b. SRIKANDI	Aplikasi dikembangkan sendiri oleh LAN Aplikasi disediakan oleh ANRI
7.	Pengelolaan Akuntabilitas Kinerja	Layanan monitoring dan evaluasi kinerja anggaran	SMART DJA	Aplikasi Disediakan oleh Kemenkeu
		Layanan monitoring dan evaluasi kinerja instansi	E-Monev Bappenas	Aplikasi Disediakan oleh Bappenas
8.	Jaringan Dokumentasi dan Informasi Hukum	Layanan jaringan dokumentasi dan informasi hukum	a. Layanan Produk Hukum (Intranet) b. JDIH LAN	Aplikasi dikembangkan sendiri oleh LAN Aplikasi Disediakan oleh BPIP Kemenkumham
9.	Pengawasan	Layanan pengawasan internal	eGratifikasi	Aplikasi dikembangkan sendiri oleh LAN

10.	Pengaduan Internal	Layanan Pengaduan	Aplikasi LAPOR	Aplikasi Disediakan oleh MenPANRB
11.	Perpustakaan	Layanan perpustakaan	Aplikasi Perpustakaan	Aplikasi Disediakan oleh Perpusnas

b. Pengelolaan Sistem Informasi Layanan Publik

Pengelolaan Sistem Informasi Layanan Publik LAN antara lain terdiri atas:

No.	Bidang	Layanan	Keterangan
1.	Pembinaan Program Pelatihan dan Pengembangan Kompetensi ASN	Layanan SIPKA Smartbangkom (Sertifikat elektronik Pelatihan)	Aplikasi dikembangkan oleh Pusdatin dan dikelola oleh P3K Bangkom
		Layanan SIPKA eManajemen Pelatihan	Aplikasi dikembangkan oleh Pusdatin dan dikelola oleh P3K Bangkom
		Layanan SIPKA eAkreditasi Pelatihan	Aplikasi dikembangkan oleh Pusdatin dan dikelola oleh P3K Bangkom
		Layanan SIPKA Bangkom dan Training Rate	Aplikasi dikembangkan oleh Pusdatin dan dikelola oleh P3K Bangkom
		Layanan eLearning (MOOC & LMS) Pelatsar CPNS, Pelatihan Manajerial, Workshop	Aplikasi dikembangkan oleh Pusdatin & Pustekbangkom dan dikelola oleh P3K Bangkom, Pustekbangkom, dan Lemdik
		Layanan Pangkalan Data SIPKA	Aplikasi dikembangkan oleh Pusdatin dan dikelola oleh P3K Bangkom
2.	Pembinaan Jabatan Fungsional Pengembangan Kompetensi ASN	Layanan Informasi Kewidyaiswaraan dan DUPAK online (SIWI)	Aplikasi dikembangkan oleh Pusdatin dan dikelola oleh Pusbin JF Bangkom
3.	Umum	Layanan Pengaduan Publik (LAPOR)	Aplikasi umum berbagi pakai Instansi pemerintah
		Layanan Data terbuka	Aplikasi dikembangkan dan dikelola oleh Pusdatin

		Layanan jaringan dokumentasi dan informasi hukum (JDIH LAN)	Aplikasi Disediakan oleh BPIP Kemenkumham
4.	Sistem Informasi Kajian dan Inovasi	a. SISKA b. INOVASI c. INOVASI ONLINE (Puslatbang PKASN) d. Innovation Learning Center e. jurnal.bandung (Puslatbang PKASN) f. JWK (Puslatbang PKASN) g. JTA (Puslatbang KHAN) h. JAP (Puslatbang KMP) i. JBA (Puslatbang KDOD)	a. Merevitalisasi sistem eksisting untuk informasi hasil kajian dan kemanfaatan hasil kajian b. Mengintegrasikan sistem sejenis yang berfungsi untuk pengelolaan kajian dan inovasi serta menjadikannya sebagai sistem berbagi pakai c. Mengintegrasikan data dan membangun database hasil kajian d. Database jurnal/policy bief/policy notes e. Inovasi Literasi Data → Hari Data LAN

5.	Sistem Informasi Sekolah Tinggi Administrasi Negara Politeknik STIA LAN	a. Website Utama Politeknik STIA LAN Jakarta; b. SIMAK; c. SIAKAD Politeknik STIA LAN Jakarta d. SIMARU; e. Perpustakaan Online Politeknik STIA LAN Jakarta; f. Presensi Dosen (Presensi Dosen Mengajar); g. Sievo; h. Andal (aplikasi Naskah Dinas Internal); i. SIMaRu (Layanan Manajemen Ruangan); j. E-learning; k. Silakan Setia (Sistem informasi Layanan Dukungan Perkuliahan); l. FiSh <File Sharing (NAS)>; dan m. PIS <Portal Information System STIA LAN Bandung (Single Sign On)>.	a. Pemetaan konsep sistem informasi Politeknik STIA LAN yang terintegrasi; b. Standarisasi pembangunan, pengembangan dan tata kelola teknologi informasin dan komunikasi untuk Politeknik STIA LAN; c. Pembangunan sistem informasi yang mendukung transformasi STIA menjadi politeknik; d. Pengembangan SIMAK; e. Pengembangan SIAKAD; f. Pengembangan SIMARU; g. Pengembangan website; dan h. Tracer study online.

BAB II

PENANGGUNGJAWAB

A. Tujuan

Pada bagian ini dijelaskan panduan pelaksanaan dalam membentuk organisasi fungsional keamanan informasi yang bertanggungjawab untuk mengelola keamanan informasi dan perangkat pengolah informasi dilingkungan LAN.

B. Kepemimpinan dan Komitmen

Manajemen puncak Dalam melaksanakan Manajemen Keamanan Informasi SPBE LAN, LAN berkomitmen untuk:

a. memastikan kebijakan keamanan informasi dan sasaran keamanan informasi ditetapkan dan selaras dengan arah strategis organisasi;
b. memastikan persyaratan S Manajemen Keamanan Informasi SPBE LAN terintegrasi ke dalam proses organisasi;
c. memastikan tersedianya sumber daya yang dibutuhkan untuk Manajemen Keamanan Informasi SPBE LAN;
d. mengomunikasikan pentingnya manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan Manajemen Keamanan Informasi SPBE LAN;
e. memastikan bahwa Manajemen Keamanan Informasi SPBE LAN mencapai manfaat yang diharapkan;
f. memberikan arahan dan dukungan pada personel untuk berkontribusi dalam efektivitas Manajemen Keamanan Informasi SPBE LAN;
g. mempromosikan perbaikan berkelanjutan; dan
h. mendukung peran manajemen yang relevan lainnya untuk menunjukkan kepemimpinannya.

C. Pemangku Kepentingan

Pemangku kepentingan yang menggunakan aset sistem informasi/aplikasi LAN antara lain sebagai berikut:

Tabel 2. Pemangku kepentingan Pengguna Sistem informasi/aplikasi LAN

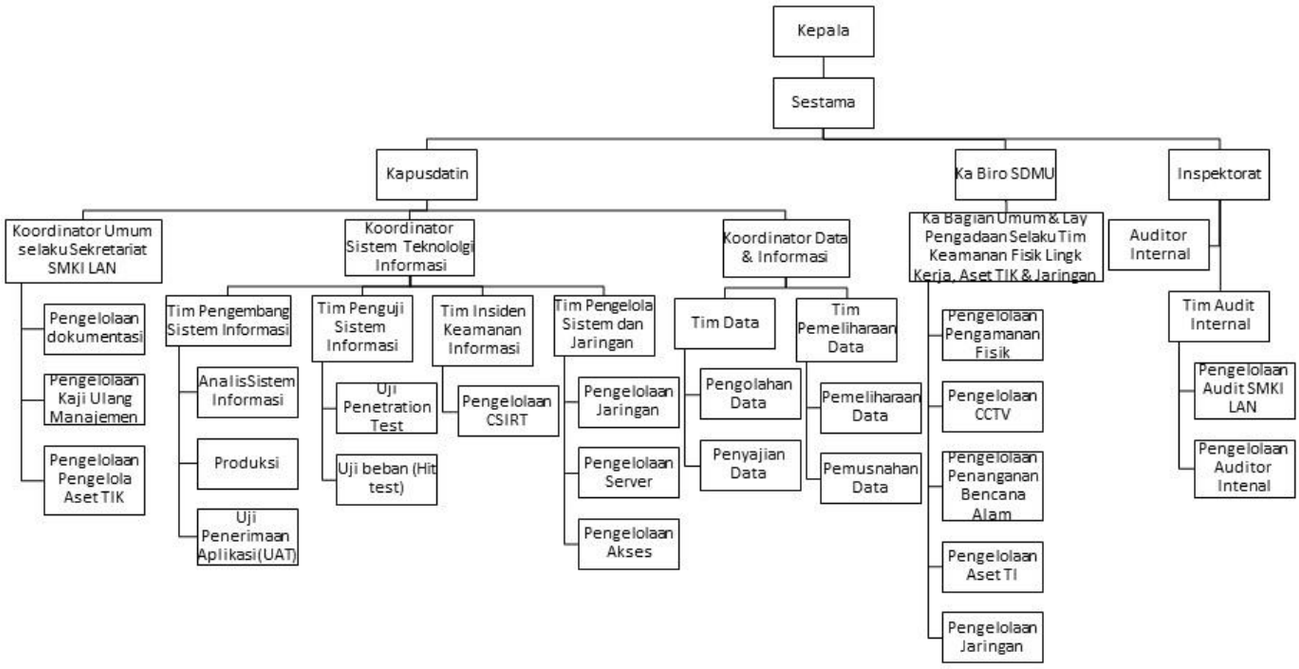
No	Pemangku Kepentingan	Penggunaan Aplikasi Sistem Informasi/Pemenuhan Persyaratan			
		AI	PS	TD	KB
1.	Kementerian/Lembaga Non Kementerian/ Pemerintah Daerah	✓	✓	✓	✓
2.	Widyaiswara	✓	-	✓	✓
3.	Analis Kebijakan	✓	-	✓	✓
4.	Aparatur Sipil Negara	✓	-	-	-
5.	Pegawai LAN	✓	-	✓	✓
6.	Perguruan Tinggi	✓	-	✓	✓
7.	Pemasok	-	-	-	✓
8.	Mahasiswa	✓	-	✓	✓

Keterangan:

- AI : Akses informasi melalui Website
- PS : Pemenuhan Persyaratan
- TD : Pertukaran data
- KB : Kerja bersama

D. Organisasi Keamanan Informasi

Pengembangan dan penerapan Manajemen Keamanan Informasi SPBE LAN dilakukan oleh Pusat Data dan Sistem Informasi didukung oleh unit kerja dan satuan kerja LAN.



Gambar 1. Struktur Organisasi Manajemen Keamanan Informasi SPBE LAN

Tugas dan wewenang unit dan atau tim yang mengelola sistem manajemen keamanan informasi pada tabel dibawah ini:

Tabel 3. Tugas dan Fungsi Tim SMKI - LAN

No	Jabatan	Tugas dan Fungsi
1.	Kepala	a) menetapkan kebijakan keamanan informasi dan sasaran keamanan informasi dan selaras dengan arah strategis organisasi; b) menetapkan persyaratan Manajemen Keamanan Informasi SPBE LAN terintegrasi ke dalam proses organisasi; c) menetapkan ketersediaan sumber daya yang dibutuhkan untuk Manajemen Keamanan Informasi SPBE LAN; d) menetapkan cara mengkomunikasikan manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan Manajemen Keamanan Informasi SPBE LAN;

No	Jabatan	Tugas dan Fungsi
		e) memastikan bahwa Manajemen Keamanan Informasi SPBE LAN mencapai manfaat yang diharapkan; f) memberikan arahan dan dukungan pada tim Manajemen Keamanan Informasi SPBE LAN untuk berkontribusi dalam efektivitas Manajemen Keamanan Informasi SPBE LAN; g) mempromosikan perbaikan berkelanjutan; dan h) mendukung peran manajemen yang relevan lainnya untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya.
2.	Sekretaris Utama	a) memastikan kebijakan keamanan informasi dan sasaran keamanan informasi dijalankan dan selaras dengan arah strategis organisasi; b) memantau persyaratan Manajemen Keamanan Informasi SPBE LAN terintegrasi ke dalam proses organisasi; c) menyetujui ketersedian sumber daya yang dibutuhkan untuk Manajemen Keamanan Informasi SPBE LAN; d) Mengkoordinasikan komunikasi manajemen keamanan informasi; e) mengkaji dan mengevaluasi manfaat yang diharapkan dari Manajemen Keamanan Informasi SPBE LAN; f) memberikan arahan dan dukungan pada tim Manajemen Keamanan Informasi SPBE LAN untuk berkontribusi dalam efektivitas Manajemen Keamanan Informasi SPBE LAN; g) mempromosikan perbaikan berkelanjutan; dan h) memastikan peran manajemen yang relevan lainnya untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya.
3.	Kepala Pusat Data dan	a) menjalankan kebijakan keamanan informasi dan sasaran keamanan informasi agar selaras dengan

No	Jabatan	Tugas dan Fungsi
	Sistem Informasi	arah strategis organisasi; b) mengintegrasikan persyaratan Manajemen Keamanan Informasi SPBE LAN ke dalam proses organisasi; c) mengusulkan ketersedian sumber daya yang dibutuhkan untuk Manajemen Keamanan Informasi SPBE LAN; d) mengomunikasikan pentingnya manajemen keamanan informasi yang efektif dan kesesuaian dengan persyaratan Manajemen Keamanan Informasi SPBE LAN; e) memastikan bahwa Manajemen Keamanan Informasi SPBE LAN mencapai manfaat yang diharapkan; f) memberikan arahan dan dukungan pada tim Manajemen Keamanan Informasi SPBE LAN untuk berkontribusi dalam efektivitas Sistem Manajemen Keamanan Informasi SPBE LAN; g) mempromosikan perbaikan berkelanjutan; dan h) mendukung peran manajemen yang relevan lainnya untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya.
4.	Koordinator Umum Pusdatin	a) menjalankan fungsi Sekretariat Manajemen Keamanan Informasi SPBE LAN; b) mengkoordirnir penyusunan, pengembangan dan pendistribusian dokumen Manajemen Keamanan Informasi SPBE LAN; c) mengkoordirnir pemeriksaan dokumen Manajemen Keamanan Informasi SPBE LAN, pengusulan revisi dan penarikan dokumen Manajemen Keamanan Informasi SPBE LAN; d) mengkoordinir pengelolaan aset teknologi informasi; e) mengkoordinir pengelolaan keamanan fisik lingkungan kerja; f) mengkoordinir pengelolaan manajemen risiko; g) mengkoordinir pengelolaan program audit dan kaji

No	Jabatan	Tugas dan Fungsi
		ulang manajemen; dan h) mengkoordinir pengelolaan auditor;
5.	Koordinator Sistem Teknologi Informasi, Pusdatin	a) mengkoordinir pembuatan, pengembangan, penerapan dan pemeliharaan sistem informasi; b) mengkoordinir pengujiaan aplikasi sistem informasi; c) mengkoordinir penanganan insiden keamanan informasi; d) mengkoordinir pengelolaan server; e) mengkoordinir pengelolaan jaringan;
6.	Koordinator Data dan Informasi, Pusdatin	a) mengkoordinir pengolahan data; b) mengkoordinir pengujian data; dan c) mengkoordinir proses pencadangan basis data *(back up data base)* berjalan sesuai periode yang ditetapkan;
7.	Auditor Internal SMKI SPBE LAN (Tim Inspektorat)	a) menyusun rencana audit; b) melakukan audit internal terhadap penerapan SMKI; c) menyusun dan Menyampaikan laporan audit internal.
8.	Tim Sekretariat SMKI SPBE LAN	a) menyusun dokumentasi umum Manajemen Keamanan Informasi SPBE LAN (misal audit internal, kaji ulang manajemen); b) menerima dan memeriksa kesesuaian usulan dokumen Manajemen Keamanan Informasi SPBE LAN; c) menyimpan dokumen induk Manajemen Keamanan Informasi SPBE LAN; d) menyimpan dokumen usang (*obsolete*) Manajemen Keamanan Informasi SPBE LAN; e) memusnahkan dokumen usang Manajemen Keamanan Informasi SPBE LAN; f) menerima dan memeriksa aset TIK dari unit pengadaan; g) mengidentifikasi dan meregistrasi aset TIK;

No	Jabatan	Tugas dan Fungsi
		h) memelihara aset TIK; i) merekam status aset TIK; j) menerima laporan hasil audit internal; k) menyusun program kaji ulang manajemen; l) melaksanakan kegiatan kaji ulang manajemen.
9.	Tim Audit Internal (Tim Inspektorat)	a) mengelola program audit; b) mengembangkan kompetensi auditor; c) memilih dan menugaskan tim audit internal; d) menerima laporan hasil audit internal.
10.	Tim Keamanan Fisik Lingkungan Kerja, Aset TIK & Jaringan (Tim Bagian Umum dan Layanan Pengadaan)	a) Menyusun klasifikasi lingkungan fisik; b) Melakukan pengamanan lingkungan fisik; c) Memantau dan mencadangkan rekaman CCTV; d) Melakukaan pengamaan saat terjadi bencana alam; e) menerima dan memeriksa aset TIK; f) mengidentifikasi dan meregistrasi aset TIK; g) memelihara aset TIK; h) merekam status aset TIK; i) memantau koneksi data; j) melakukan pemeliharaan jaringan (LAN dan WIFI);.
11.	Tim Pembuatan dan pengembangan aplikasi sistem informasi	a) melaksanakan identifikasi kebutuhan pengguna; b) menyusun desain aplikasi; c) melaksanakan proses produksi aplikasi; d) melaksanakan uji keberterimaan aplikasi (UAT); dan memelihara aplikasi sistem informasi.
12.	Tim Penguji Keamanan Sistem Informasi	a) menyusun rencana kerja uji sistem informasi; b) menyusun uji penetrasi; dan c) melakukan uji beban.
13.	Tim Pengelola server dan jaringan	a) menyiapkan *server development* dan *server* produksi; b) mengunggah aplikasi ke *server development* atau *server* produksi;

No	Jabatan	Tugas dan Fungsi
		c) memelihara *server*; d) memantau koneksi data; e) melakukan pemeliharaan jaringan (LAN dan WIFI); dan f) mengelola akses jaringan dan *server*.
14.	Tim Insiden Keamanan Informasi	a) memantau koneksi aplikasi dan jaringan; b) memutus koneksi aplikasi; c) melokalisir *server*; d) memperbaiki aplikai, *server* dan jaringan; dan e) melaporkan insiden keamanan informasi.
15.	Tim Data	a) Mengolah data; dan b) menyajikan data.
16.	Tim Pemeliharaan data	a) memelihara data; dan b) mencadangkan data.

BAB III

PERENCANAAN

A. Tujuan

Perancanaan Manajemen Keamanan Informasi SPBE LAN digunakan sebagai panduan pelaksanaan dalam menentukan perencanaan keamanan informasi meliputi: menentukan sasaran Manajemen Keamanan Informasi SPBE LAN, dan upaya atau tindakan untuk menangani resiko dan peluang yang terdapat didalam penerapan Manajemen Keamanan Informasi SPBE LAN yang disusun dalam bentuk program kerja dan rencana anggaran keamanan informasi.

B. Perencanaan Keamanan Informasi

Perencanaan Manajemen Keamanan Informasi SPBE LAN dengan cara:

1. menyusun rencana kerja tahunan yang mengacu pada Rencana Strategis LAN dan Arsitektur SPBE LAN.
2. menyusun rancangan anggaran dan biaya tahunan.
3. menyiapkan rencana pemantauan, pengukuran dan evaluasi Manajemen Keamanan Informasi SPBE LAN.

C. Tindakan untuk menangani Resiko dan Peluang

LAN memiliki mekanisme dan prosedur P.SMKI.LAN.1 untuk menangani resiko dan peluang yang terdapat didalam penerapan Manajemen Keamanan Informasi SPBE LAN. Penentuan resiko yang perlu ditangani harus mempertimbangkan permasalahan yng terdapat dalam tabel 1 dan persyaratan perundangan sebagaimana tabel 4 (empat) serta dengan tujuan:

1. memastikan Manajemen Keamanan Informasi SPBE LAN dapat mencapai manfaat yang diharapkan;
2. mencegah, atau mengurangi, efek yang tidak diinginkan;
3. mencapai perbaikan yang berkelanjutan.

Dengan menentukan kriteria dan keberterimaan resiko yang harus ditangani, LAN dapat merencanakan:

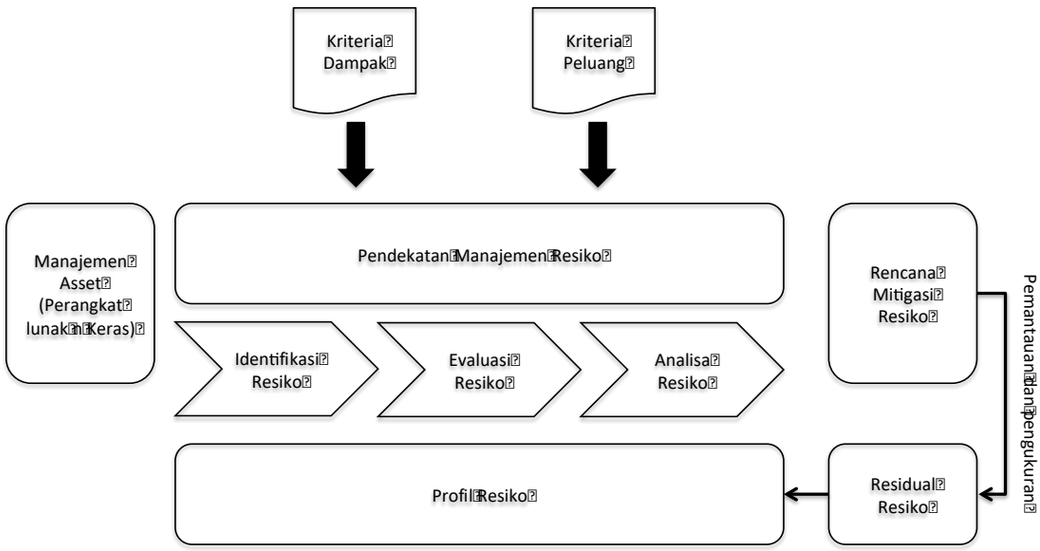
1. tindakan untuk menangani risiko dan peluang;
2. mengintegrasikan dan menerapkan tindakan ke dalam proses SMKI; dan
3. mengevaluasi efektivitas tindakan tersebut.

1. Penilaian Resiko Keamanan Informasi

LAN memiliki komitmen untuk melakukan penilaian resiko keamanan informasi yang dilakukan dan ditetapkan dengan mempertimbangkan:

a. menetapkan dan memelihara kriteria risiko keamanan informasi yang meliputi:
   1) kriteria keberterimaan risiko; dan
   2) kriteria untuk melakukan penilaian risiko keamanan informasi;
b. memastikan bahwa penilaian risiko keamanan informasi yang diulang akan memberikan hasil yang konsisten, valid dan sebanding;
c. mengidentifikasi risiko keamanan informasi:
   1) menerapkan proses penilaian risiko keamanan informasi untuk mengidentifikasi risiko yang terkait dengan hilangnya kerahasiaan, integritas dan ketersediaan informasi dalam ruang lingkup SMKI; dan
   2) mengidentifikasi pemilik risiko;
d. menganalisis risiko keamanan informasi:
   1) menilai konsekuensi potensial yang akan terjadi jika risiko yang teridentifikasi pada poin c.1) terjadi;
   2) menilai kemungkinan realistis terjadinya risiko yang teridentifikasi pada poin c.1); dan
   3) menentukan tingkat risiko;
e. mengevaluasi risiko keamanan informasi:
   1) membandingkan hasil analisis risiko dengan kriteria risiko yang ditetapkan pada poin a. dan
   2) memprioritaskan risiko yang dianalisis untuk penanganan risiko.

Penilaian dan Evaluasi Resiko dilaksanakan untuk mengidentifikasi potensi ancaman terhadap aset sumber daya informasi dan analisa resiko serta penanganan resiko dalam pengelolaan sistem manajemen keamanan informasi. Hal tersebut dilakukan dengan cara meninjau (*review*) analisa resiko serta penanganan resiko yang disusun berdasarkan evaluasi identifikasi permasalahan dalam penanganan keamanan informasi, sehingga dapat merumuskan acuan dalam persiapan implementasi Manajemen Keamanan Informasi SPBE LAN. Acuan tersebut berdasarkan analisa resiko dan kebutuhan terhadap proses pengamanan informasi. Metodologi untuk menangani resiko dan peluang terjadinya gangguan keamanan informasi disampaikan pada gambar 2 berikut:



Gambar 2. Metodologi Penangan Resiko dan Peluang

Penilaian dan evaluasi resiko meliputi kegiatan-kegiatan sebagai berikut:

1. Menentukan kritikalitas aset berdasarkan data aset TIK yang telah diinvetarisasi.
2. Menentukan kriteria penilaian resiko yang terdiri dari kriteria dampak dan kecenderungan/ probabilitas yang dituangkan dalam metodologi penilaian resiko.
3. Melaksanakan penilaian risiko yang terdiri dari kegiatan identifikasi, evaluasi, dan analisa risiko.
4. Menentukan rencana mitigasi risiko sebagai bagian dari proses penerapan Manajemen Keamanan Informasi SPBE LAN dan meminimasi dampak dari risiko tersebut.
5. Menyusun suatu profil risiko yang menggambarkan kondisi keamanan informasi.

Dengan mempertimbangkan hal-hal tersebut, Kriteria Penilaian Risiko dan keberterimaan resiko dapat dilihat pada tabel 4 sampai dengan tabel 8 sebagai berikut:

Tabel 4. Kriteria Penilaian Titik Kritis Aset

Titik Kritis	**Analisa Sensitivitas**	**Kriteria Penilaian**		
		High	**Medium**	**Low**
Confidentiality	Berapa besar kerugian yang mungkin ditimbulkan	Terdapat kerugian yang sangat signifikan (materi dan	Terdapat kerugian yang signifikan (materi dan	Terdapat kerugian namun tidak signifikan karena

Titik Kritis	Analisa Sensitivitas	Kriteria Penilaian		
		High	Medium	Low
	jika terjadi hilangnya kerahasiaan informasi?	nilai strategis) karena informasinya bocor sangat sensitif	nilai strategis) namun informasi yang bocor tidak sensitif dan dapat diakses oleh berbagai pihak	informasi yang bocor bersifat umum dan mudah diperoleh dari berbagai sumber
Integrity	Berapa besar dampak/kerugian terhadap jalannya proses bisnis apabila suatu aset tidak digunakan dengan benar, tidak lengkap, tidak akurat dan tidak terbaharui	• Terdapat dampak yang sangat signifikan yang dapat menyebabkan tidak berjalannya proses bisnis dan • berpotensi menyebabkan kerusakan yang sistemik	• Terdapat kerugian signifikan namun proses bisnis masih dapat berjalan • Tidak menyebabkan kerusakan yang sistemik	• Terdapat kerugian namin tidak signifikan • Proses bisnis masih dapat berjalan • Tidak menyebabkan kerusakan yang sistemik
Availability	Berapa besar dampak kerugian yang ditimbulkan apabila terjadi ketidaktersediaan suatu aset	Terdapat dampak yang sangat signifikan yang mengakibatkan tidak berjalannya proses bisnis	Terdapat kerugian signifikan namun proses bisnis masih dapat berjalan	• Terdapat kerugian namin tidak signifikan • Proses bisnis masih dapat berjalan

Tabel 5. Peluang Terjadinya Resiko

Kemungkinan	Nilai	Uraian
Sangat Jarang	1	Risiko terjadi sekali dalam waktu > 5 Tahun
Jarang	2	Risiko dapat terjadi sekali antara 1 – 5 Tahun

Sedang	3	Risiko mungkin terjadi 1 – 6 kali setahun
Sering	4	Risiko mungkin terjadi rata-rata 1 kali setiap bulan
Sangat Sering	5	Risiko terjadi minimum seminggu 1 kali

Tabel 6. Dampak Terjadinya Resiko

Tingkat Dampak	Reputasi	Finansial	Operasional	Kinerja
1 (Tidak Signifikan)	Terdapat pemberitaan negatif namun tidak mengakibat penurunan kepercayaan	Tidak terdapat kerugian finansial	Terdapat gangguan namun tidak mengakibatkan proses bisnis teraganggu	Menimbulkan penundaan aktifitas ~~maksimal~~ paling lama 24 (dua puluh empat) jam.
2 (Ringan)	Terdapat pemberitaan negatif yang dapat mempengaruhi tingkat kepercayaan *stakeholder*	terdapat kerugian/biaya yang harus dikeluarkan hingga Rp. 50.000.000,- (lima puluh juta rupiah).	terdapat gangguan yang menyebabkan 1 mata rantai proses bisnis terganggu	Menimbulkan penundaan aktifitas maksimal 2 x 24 Jam
3 (Besar)	terdapat pemberitaan negatif yang terus menurunkan kepercayaan *stakeholder*	terdapat kerugian/biaya yang harus dikeluarkan Rp. 50.000.000,- hingga Rp. 250.000.000,-	terdapat gangguan yang menyebabkan 50 % proses bisnis terganggu	Menimbulkan penundaan aktifitas maksimal 7 x 24 Jam
4 (Sangat Besar)	hilangnya kepercayaan *stakeholder*	terdapat kerugian/biaya yang harus dikeluarkan lebih dari Rp. 250.000.000,- Rp. 1.000.000.000,-	terdapat gangguan yang menyebabkan 75 % proses bisnis terganggu	Menimbulkan penundaan aktifitas lebih dari 14 x 24 Jam
5 (kastratope)	hilangnya kepercayaan *stakeholder*	terdapat kerugian/biaya yang harus	terjadi kelumpuhan	Menimbulkan penundaan aktifitas

		dikeluarkan lebih Rp. 1.000.000.000, -	pada proses bisnis	lebih dari 14 x 24 Jam

Nilai Risiko	Uraian
Sangat Tinggi	Risiko tidak dikehendaki dan perlu tindakan perbaikan sangat segera (misal maksimum dalam 2 hari)
Tinggi	Risiko tidak dikehendaki dan perlu tindakan perbaikan segera (dalam 3 –7 hari), tetapi pimpinan dapat menetapkan keputusan lain
Menengah (Sedang)	Risiko tidak dikehendaki dan perlu tindakan perbaikan dalam jangka menengah (di atas 7 hari)
Rendah	Risiko dapat diterima dengan tetap menerapkan control yang ada ataupun memperbaiki kontrol/improvement

Tabel 7. Matriks Nilai Resiko

SKALA KEMUNGKINAN	Tidak Signifikan	Ringan	Besar	Sangat Besar	Kastratrope
Sangat jarang	Rendah	Rendah	Menengah	Tinggi	Tinggi
Jarang	Rendah	Rendah	Menengah	Tinggi	Tinggi
Sedang	Rendah	Rendah	Menengah	Tinggi	Sangat Tinggi
Sering	Rendah	Menengah	Tinggi	Sangat Tinggi	Sangat Tinggi
Sangat Sering	Rendah	Menengah	Tinggi	Sangat Tinggi	Sangat Tinggi

Tabel 8. Kriteria keberterimaan resiko

SKALA KEMUNGKINAN	SKALA DAMPAK				
	Tidak Signifikan	Minor	Menengah	Besar	Sangat Besar
Sangat jarang	Diterima	Diterima	Mitigasi	Mitigasi	Mitigasi
Jarang	Diterima	Diterima	Mitigasi	Mitigasi	Mitigasi
Sedang	Diterima	Diterima	Mitigasi	Mitigasi	Mitigasi
Sering	Diterima	Mitigasi	Mitigasi	Mitigasi	Mitigasi
Sangat Sering	Diterima	Mitigasi	Mitigasi	Mitigasi	Mitigasi

Proses penilaian resiko keamanan informasi dilakukan melalui Prosedur Manajemen Resiko Keamanan Informasi (P.SMKI.LAN.1). LAN menyimpan rekaman tentang proses penilaian risiko keamanan informasi.

2. Penanganan Resiko Keamanan Informasi

LAN menetapkan dan menerapkan proses penanganan risiko keamanan informasi untuk:

a. memilih opsi penanganan risiko keamanan informasi yang tepat, dengan mempertimbangkan hasil penilaian risiko;
b. menentukan semua kendali yang diperlukan untuk menerapkan opsi penanganan risiko keamanan informasi yang dipilih;
c. membandingkan kendali yang ditentukan pada 2. b) di atas dengan yang ada dalam daftar prosedur dan memverifikasi bahwa tidak terlewatnya kendali yang diperlukan;
d. menghasilkan Statement of Applicability (SOA) yang berisi kendali yang diperlukan (lihat 2. b) dan c) dan alasan pencantuman, apakah kendali itu diterapkan atau tidak, dan alasan pengecualian kendali;
e. merumuskan rencana penanganan risiko keamanan informasi, dan
f. mendapatkan persetujuan pemilik risiko terhadap rencana penanganan risiko keamanan informasi dan keberterimaan risiko keamanan informasi yang tersisa.

LAN menyimpan rekaman tentang proses penanganan risiko keamanan informasi.

D. Sasaran keamanan informasi dan perencanaan untuk mencapainya

Sasaran keamanan informasi terdiri dari:

1. Menjamin keamanan informasi di Lembaga Administrasi Negara dari risiko kejahatan internet, kegagalan fungsi sistem aplikasi dan perangkat keras yang dapat ditimbulkan dari pihak internal maupun eksternal.
2. Menjaga aspek kerahasiaan, integritas dan ketersediaan dari seluruh aset informasi milik Lembaga Administrasi Negara dari ancaman pihak internal maupun eksternal.
3. Memastikan bahwa kebijakan ini dimengerti dan dijalankan di seluruh Pegawai LAN, serta ditinjau dan dikembangkan secara terus menerus.
4. Mendorong budaya peningkatan berkelanjutan (*continous improvement*) di seluruh tingkatan dalam Lembaga Administrasi Negara.

Sasaran Manajemen Keamanan Informasi SPBE LAN diterjemahkan juga menjadi sasaran Manajemen Keamanan Informasi SPBE LAN.

Tabel 9. Sasaran

No	**Sasaran** Manajemen Keamanan Informasi SPBE LAN	Indikator	Nilai
1.	Service Level Agreement	Durasi waktu Koneksi jaringan uptime dalam 1 tahun	95%
2.	Service Level Agreement	Durasi waktu aplikasi berfungsi	95%
3.	Terpeliharanya aset teknologi informasi	Prosentase aset TI yang berfungsi dengan baik dalam 1 tahun	95%

Pusat Data dan Sistem Informasi merekam Sasaran Manajemen Keamanan Informasi SPBE LAN dan Sasaran Manajemen Keamanan Informasi SPBE LAN unit kerja serta harus terdapat di setiap unit kerja yang menangani Manajemen Keamanan Informasi SPBE LAN. Penyampaian informasi Sasaran Manajemen Keamanan Informasi SPBE LAN ini dilakukan melalui berbagai sarana komunikasi yang dimiliki LAN.

Sasaran Manajemen Keamanan Informasi SPBE LAN ditinjau dan dievaluasi setiap 3 tahun atau dapat dipercepat jika dipandang perlu oleh manajemen puncak.

Setiap tahun, pencapaian sasaran Manajemen Keamanan Informasi SPBE LAN dievaluasi oleh Manajemen Puncak. Hasil evaluasi digunakan untuk memperbaiki kinerja.

BAB IV

DUKUNGAN PENGOPERASIAN

A. Tujuan

Pada bagian dijelaskan panduan pelaksanaan dalam memberikan dukungan pengoperasian, meliputi: dukungan sumber daya, dukungan sumber daya manusia (SDM), dukungan kepedulian pegawai dan komunikasi didalam penerapan Manajemen Keamanan Informasi SPBE LAN.

B. Dukungan Sumber Daya

Pusat Data dan Sistem Informasi berkomitmen untuk mengalokasikan anggaran, menyediakan gedung dan lingkungan kerja yang nyaman dan aman, peralatan dan perlengkapan kerja, serta ruangan khusus server bagi penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap Manajemen Keamanan Informasi SPBE LAN.

C. Dukungan SDM

Pusat Data dan Sistem Informasi, memiliki komiten untuk menyediakan dan mengelola sumber daya manusia yang dibutuhkan untuk penetapan, penerapan, pemeliharaan dan perbaikan berkelanjutan terhadap Manajemen Keamanan Informasi SPBE LAN.

Untuk mendapatkan SDM yang handal, LAN telah menentukan persyaratan minimal yang harus dipenuhi oleh personel yang akan bekerja di unit yang menangani Manajemen Keamanan Informasi SPBE LAN. Tata cara dan persyaratan rekrutmen tersebut dapat dilihat pada prosedur pengelolaan SDM (P.SMKI.LAN.30).

Untuk meningkatkan kompetensi personel, LAN memiliki komitmen yang tinggi dengan mengalokasikan dana dan waktu bagi pelaksanaan pendidikan/pelatihan teknis bagi pegawai termasuk untuk pegawai yang menangani Manajemen Keamanan Informasi SPBE LAN. Pengelolaan kompetensi diatur pada prosedur pengelolaan SDM (P.SMKI.LAN.30). Lembaga Administrasi Negara merekam seluruh data terkait kompetensi pegawai.

D. Dukungan Kepedulian

LAN melakukan serangkaian kegiatan sosialisasi Manajemen Keamanan Informasi SPBE LAN secara rutin sebagai mana diatur dalam Prosedur Kepedulian dan Komunikasi (P.SMKI.LAN.6 dan P.SMKI.LAN.7) agar seluruh pegawai LAN peduli terhadap:

1. kebijakan keamanan informasi;
2. kontribusinya terhadap efektivitas SMKI, termasuk manfaat peningkatan kinerja keamanan informasi; dan
3. implikasi dari ketidaksesuaian dengan persyaratan SMKI.

E. Komunikasi

LAN menetapkan dua cara dalam komunikasi yaitu komunikasi dalam kondisi normal dan kondisi tidak normal. Kondisi normal artinya kondisi dimana tidak terdapat kejadian luar biasa dan berbahaya. Sedangkan kondisi tidak normal adalah terdapat kejadian luar biasa dan berbahaya seperti adanya bahaya kebakaran, gempa bumi, serangan virus dan hacker.

Dalam kondisi normal, komunikasi kepada seluruh pegawai dilakukan melalui nota dinas, email, telepon, dan whatsapps ditujukan kepada Kepala Pusat Data dan Sistem Informasi. Sedangkan dalam kondisi tidak normal, komunikasi kepada seluruh pegawai LAN dapat dilakukan langsung telelpon, whatsapp, email atau alat komunikasi lainnya dengan dilanjutkan memberikan laporan setelahnya.

Tata cara komunikasi dalam pelaksaan SMKI diatur dalam Prosedur kepedulian dan Komunikasi (P.SMKI.LAN.6 dan P.SMKI.LAN.7). Prosedur tersebut juga mengatur hal-hal sebagai berikut:

1. apa yang perlu dikomunikasikan;
2. kapan komunikasi harus dilakukan;
3. kepada siapa dikomunikasikan;
4. siapa yang harus mengomunikasikan; dan
5. proses yang dipengaruhi oleh komunikasi tersebut.

F. Pengendalian Dokumen dan Rekaman

1. Dokumentasi Manajemen Keamanan Informasi SPBE LAN

   Dokumentasi Sistem Mutu Manajemen Keamanan Informasi SPBE LAN didokumentasikan ke dalam:

a. **Level I: Pedoman Sistem Manajemen Keamanan Informasi (PSMKI)**
   Dokumen yang memuat komitmen dan kebijakan LAN berkaitan dengan penerapan sistem manajemen LAN guna mencapai kepuasan pelanggan/stakeholder, keamanan informasi dan memenuhi peraturan perundang-undangan yang berlaku. Pedoman ini juga mengidentifikasi tanggungjawab pimpinan dan personel, sistem dokumentasi yang terkait serta proses kerja yang diperlukan untuk mencapai sasaran.
b. **Level II: Prosedur (P)**
   Dokumen yang menguraikan elemen sistem untuk melaksanakan komitmen dan kebijakan LAN sebagaimana tercantum pada pedoman sistem manajemen LAN dan menguraikan kegiatan yang dilakukan termasuk penanggungjawab, serta dokumentasi dan/atau rekaman yang disyaratkan.
c. **Level III: Instruksi Kerja (IK)**
   Dokumen yang menerangkan bagaimana seseorang melaksanakan tugas. IK dibuat sesuai dengan kebutuhan.
d. Level IV: Formulir (F)
   Dokumen yang diperlukan untuk merekam pelaksanaan dari suatu aktivitas kegiatan sistem manajemen LAN.
e. **Dokumen Pendukung (DP).**
   Semua dokumen yang digunakan atau diacu untuk mendukung pelaksanaan tugas. Dokumen pendukung termasuk standar, regulasi dan peraturan perundang-undangan terkait, serta keputusan dan kebijakan internal yang ditetapkan LAN.

Dalam membuat dan memperbarui informasi terdokumentasi LAN memastikan kecukupan hal sebagai berikut:

a. identifikasi dan deskripsi (misal judul, tanggal, penulis, atau nomor referensi);
b. format (misal bahasa, versi perangkat lunak, grafis) dan media (misal kertas, elektronik); dan
c. reviu dan persetujuan untuk kesesuaian dan kecukupan.

2. Pengendalian Dokumen
   a. Sekretariat Manajemen Keamanan Informasi SPBE LAN mengendalikan semua dokumentasi Manajemen Keamanan

Informasi SPBE LAN sesuai Prosedur Pengendalian Dokumen dan Rekaman (P.SMKI.LAN.31).

b. Pengendalian dokumen dilakukan dengan maksud untuk memastikan bahwa semua dokumen tersedia saat diperlukan (di lokasi), ditinjau kecukupan dan kemutakhirannya, serta dokumen kadaluarsa diidentifikasi dan dipindahkan dari tempat penggunaan.

c. Semua dokumen diidentifikasi, mudah dipahami dan diimplementasikan serta dipelihara kemutakhirannya.

3. Pengendalian Rekaman

a. Rekaman harus diidentifikasi, disimpan, dipelihara dan dimusnahkan sesuai dengan ProsedurnPengendalian Dokumen dan Rekaman (P.SMKI.LAN.31).

b. Pemeliharaan rekaman dilakukan sesuai dengan periode masa simpan yang ditetapkan oleh masing-masing Unit Kerja LAN dan mengacu pada peraturan perundang-undangan terkait.

c. Tata cara pemusnahan rekaman harus memperhatikan kerahasiaan informasi dari isi rekaman/dokumen tersebut.

G. Pengendalian Operasional

LAN memiliki komitmen untuk mengendalikan seluruh aspek operasional sistem Manajemen Keamanan Informasi SPBE LAN. Pengendalian operasional Manajemen Keamanan Informasi SPBE LAN dilakukan dengan menggunakan sejumlah kendali yang terdapat dalam daftar induk dokumen.

H. Penilaian risiko keamanan informasi

LAN melakukan penilaian risiko keamanan informasi pada secara rutin sesuai dengan waktu yang telah direncanakan atau ketika terjadi perubahan signifikan pada perencanaan. dengan mempertimbangkan kriteria yang ditetapkan dalam III.c.2.1 a). LAN selalu menyimpan informasi terdokumentasi dari hasil penilaian risiko keamanan informasi. Penilaian resiko keamanan informasi dilakukan melalui prosedur Pengelolaan Resiko Keamanan Informasi (P.SMKI.LAN.1).

I. Penanganan risiko keamanan informasi

LAN memiliki prosedur untuk menangani risiko keamanan informasi sesuai dengan risiko/kejadian yang terjadi. Setiap kejadian penyerangan/kegagalan fungsi operasi dan penanganannya harus direkam dan rekamannya dipelihara sebagai bahan evaluasi. Penanganan resiko keamanan informasi dilakukan melalui prosedur Pengelolaan Resiko Keamanan Informasi.

BAB V

EVALUASI KINERJA

A. Tujuan

Pada bagian ini digunakan sebagai panduan pelaksanaan dalam evaluasi kinerja pelaksanaan keamanan informasi di lingkungan LAN.

B. Pemantauan, pengukuran, analisis dan evaluasi

LAN secara rutin melakukan mengevaluasi kinerja keamanan informasi dan efektivitas Manajemen Keamanan Informasi SPBE LAN dengan:

1. Melakukan penetapan apa yang perlu dipantau dan diukur, termasuk proses dan pengendalian keamanan informasi.
2. Menetapkan metode yang digunakan untuk pemantauan, pengukuran, analisis dan evaluasi untuk memastikan hasil yang valid;
3. Menetapkan periode pemantauan dan pengukuran harus dilakukan;
4. Proses pemantauan dan pengukuran dilakukan oleh tim yang bertanggung jawab;
5. Hasil pemantuan dilaporkan dan dievaluasi secara periodik sesuai dengan ketentuan yang ditetapkan. Dalam hal terjadi sesuatu yang tidak normal saat dilakukan pemantauan dan pengukuran, koordinator yang bertanggung jawab diberikan kewenangan untuk melakukan tindakan yang dibutuhkan.
6. Analisa dan evaluasi terhadap laporan pemantauan dan pengukuran dilakukan secara berjenjang sesuai dengan kewenangannya.
7. Pemantauan dan pengukuran harus direkam dan rekamannya dipelihara dengan baik.

C. Audit Internal

LAN melakukan audit internal atas pelaksanaan Manajemen Keamanan Informasi SPBE LAN paling sedikit 1 (satu) kali setiap tahunnya, dengan tujuan:

1. Menyesuikan dengan ketentuan pada:
    a. persyaratan yang ditetapkan LAN dalam penerapan Manajemen Keamanan Informasi SPBE LAN; dan
    b. persyaratan Standar SNI ISO/IEC 27001:2013 Sistem Manajemen Keamanan Informasi.

2. Manajemen Keamanan Informasi SPBE LAN diimplementasikan dan dipelihara secara efektif.

LAN merencanakan, menetapkan, menerapkan dan memelihara program audit, termasuk frekuensi, metode, tanggung jawab, persyaratan perencanaan dan pelaporan.

Program audit dilakukan dengan mempertimbangkan pentingnya proses yang bersangkutan dan hasil audit sebelumnya. Pelaksanaan audit internal dikoordinasikan oleh Sekretariat Manajemen Keamanan Informasi SPBE LAN, dengan:

a. Menyusun dan menentukan kriteria audit dan ruang lingkup untuk setiap audit
b. memilih auditor dan melakukan audit yang menjamin objektivitas dan ketidakberpihakan proses audit;
c. memastikan bahwa hasil audit tersebut dilaporkan kepada manajemen yang relevan; dan
d. menyimpan informasi terdokumentasi sebagai alat bukti dari program audit dan hasil audit.

Pelaksanaan Audit Internal dilakukan dengan menggunakan prosedur Audit Internal (P.SMKI.LAN.32).

D. Kaji Ulang Manajemen

Kepala LAN harus melakukan kaji ulang manajemen organisasi SMKI paling sedikit 1 (satu) kali dalam setahun untuk memastikan kesesuaian, kecukupan dan efektivitas.

Kaji Ulang manajemen harus mencakup pertimbangan:

1. status tindakan dari kaji ulang manajemen sebelumnya;
2. perubahan isu eksternal dan internal yang relevan dengan SMKI;
3. umpan balik dari kinerja keamanan informasi, termasuk kecenderungan dalam hal:
    a. ketidaksesuaian dan tindakan korektif;
    b. hasil pemantauan dan pengukuran;
    c. hasil audit (internal dan eksternal); dan
    d. pemenuhan terhadap sasaran keamanan informasi;
4. umpan balik dari pihak yang berkepentingan;
5. hasil penilaian risiko dan status rencana penanganan risiko; dan

6. peluang untuk perbaikan berkelanjutan.

Keluaran dari kaji ulang manajemen harus mencakup keputusan yang berkaitan dengan peluang perbaikan berkelanjutan dan setiap kebutuhan untuk perubahan Manajemen Keamanan Informasi SPBE LAN. Proses kaji ulang manajemen dilakukan dengan menggunakan Prosedur Kaji Ulang Manajemen (P.SMKI.LAN.33). Hasil dari kaji ulang manajemen harus direkam dan rekamannya dipelihara dengan baik.

BAB VI

PERBAIKAN BERKELANJUTAN

A. Tujuan

Pada bagian ini dijelaskan sebagai panduan pelaksanaan dalam perbaikan berkelanjutan yang merupakan tindaklanjut dari hasil evaluasi kinerja pelaksanaan Manajemen Keamanan Informasi SPBE LAN.

B. Ketidaksesuaian dan tindakan korektif

Dalam hal terjadi ketidaksesuaian, LAN berkomitmen untuk:

1. mengambil tindakan untuk mengendalikan dan mengoreksinya; dan menangani konsekuensinya;
2. mengevaluasi kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian, agar hal itu tidak terulang atau terjadi di tempat lain, dengan cara:
   a. mereviu ketidaksesuaian;
   b. menentukan penyebab ketidaksesuaian; dan
   c. menentukan apakah ada ketidaksesuaian serupa, atau berpotensi terjadi kembali;
3. melaksanakan tindakan apapun yang diperlukan;
4. mengkaji efektivitas tindakan korektif apapun yang diambil; dan
5. membuat perubahan pada Manajemen Keamanan Informasi SPBE LAN
6. Tindakan korektif harus sesuai dengan efek dari ketidaksesuaian yang ditemui.

LAN mendokumentasikan semua tindakan yang dilakukan untuk mengendalikan ketidaksesuaian dan tindakan berikutnya yang diambil, dan hasil dari setiap tindakan korektif.

C. Perbaikan berkelanjutan

LAN memiliki komitmen untuk terus memperbaiki kesesuaian, kecukupan dan efektivitas Manajemen Keamanan Informasi SPBE LAN.

KEPALA
LEMBAGA ADMINISTRASI NEGARA
REPUBLIK INDONESIA,

Ttd.

ADI SURYANTO