



GUBERNUR NUSA TENGGARA TIMUR

**PERATURAN GUBERNUR NUSA TENGGARA TIMUR
NOMOR 53 TAHUN 2023**

TENTANG

PERUBAHAN ATAS PERATURAN GUBERNUR

NUSA TENGGARA TIMUR NOMOR 19 TAHUN 2021

TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH PROVINSI NUSA TENGGARA TIMUR

**DENGAN RAHMAT TUHAN YANG MAHA ESA
GUBERNUR NUSA TENGGARA TIMUR,**

- Menimbang** : a. bahwa sesuai Peraturan Gubernur Nusa Tenggara Timur Nomor 19 Tahun 2021 telah ditetapkan Sistem Manajemen Keamanan Informasi Di Lingkungan Pemerintah Provinsi Nusa Tenggara Timur;
- b. bahwa menindaklanjuti rekomendasi hasil evaluasi Indeks Keamanan Informasi (IKAMI) di Pemerintah Provinsi Nusa Tenggara Timur oleh Badan Siber dan Sandi Negara (BSSN), perlu dilakukan penyesuaian terhadap Peraturan Gubernur Nusa Tenggara Timur Nomor 19 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Di Lingkungan Pemerintah Provinsi Nusa Tenggara Timur;
- c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, dan huruf b, perlu menetapkan Peraturan Gubernur tentang Perubahan Atas Peraturan Gubernur Nusa Tenggara Timur Nomor 19 Tahun 2021 tentang Sistem Manajemen Keamanan Informasi Di Lingkungan Pemerintah Provinsi Nusa Tenggara Timur;

- Mengingat** : 1. 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);

2. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
3. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
4. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi Di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
5. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistim Pemerintahan Berbasis Elektronik dan Standar dan Prosedur Keamanan Sistim Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
6. Peraturan Gubernur Nusa Tenggara Timur Nomor 19 Tahun 2021 tentang Sistim Manajemen Keamanan Informasi Di Lingkungan Pemerintah Provinsi Nusa Tenggara Timur (Berita Daerah Provinsi Nusa Tenggara Timur Tahun 2021 Nomor 19);

MEMUTUSKAN:

Menetapkan : PERATURAN GUBERNUR TENTANG PERUBAHAN ATAS PERATURAN GUBERNUR NUSA TENGGARA TIMUR NOMOR 19 TAHUN 2021 TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH PROVINSI NUSA TENGGARA TIMUR.

Pasal I

Beberapa ketentuan dalam Peraturan Gubernur Nusa Tenggara Timur Nomor 19 Tahun 2021 tentang Sistim Manajemen Keamanan Informasi Di Lingkungan Pemerintah Provinsi Nusa Tenggara Timur (Berita Daerah Provinsi Nusa Tenggara Timur Tahun 2021 Nomor 19), diubah sebagai berikut :

1. Ketentuan Pasal 1 angka 4 (empat) diubah dan ditambahkan 2 (dua) angka baru sehingga berbunyi sebagai berikut :

Pasal 1

1. Daerah adalah Provinsi Nusa Tenggara Timur.
2. Pemerintah Daerah adalah Pemerintah Provinsi Nusa Tenggara Timur.
3. Gubernur adalah Gubernur Nusa Tenggara Timur.
4. Perangkat Daerah/Unit Kerja yang selanjutnya disebut PD/Unit Kerja adalah perangkat daerah atau unit kerja lingkup Pemerintah Provinsi Nusa Tenggara Timur.
5. Dinas adalah perangkat daerah tingkat provinsi yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.
6. Pegawai Aparatur Sipil Negara yang selanjutnya disebut Pegawai Aparatur Sipil Negara adalah Pegawai Negeri Sipil dan Pegawai Pemerintah dengan Perjanjian Kerja yang diangkat oleh pejabat pembina kepegawaian dan diserahi tugas dalam suatu jabatan pemerintahan atau diserahi tugas negara lainnya dan digaji berdasarkan ketentuan peraturan perundang-undangan.
7. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah Sistem, metode manajemen untuk melindungi, membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan Keamanan Informasi berdasarkan pendekatan risiko yang sistimatis.
8. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non elektronik.
9. Sistem adalah suatu kesatuan yang terdiri dari komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran informasi, materi atau energi untuk mencapai suatu tujuan.
10. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan Informasi Elektronik.

11. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek Keamanan Informasi seperti kerahasiaan data, keabsahan data, integritas data, otentikasi, otorisasi dan nirpenyangkalan.
12. Komputer adalah alat untuk memproses data elektronik, mengetik, optik, atau system yang melaksanakan fungsi logika, aritmatika, dan menyimpan.
13. Keamanan Informasi adalah suatu kondisi terjaganya aspek kerahasiaan, integritas keutuhan dan ketersediaan dari informasi.
14. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja pelayanan Sistem Elektronik.
15. Aset Informasi adalah sesuatu yang terdefinisi dan terkelola sebagai suatu unit informasi Teknologi Informasi dan Komunikasi sehingga dapat dipahami, dibagi, dilindungi dan dimanfaatkan bagi penyelenggaraan Sistem Pemerintahan Berbasis Elektronik.
16. Aset Pengolahan dan Penyimpanan Informasi adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi.
17. Data Center adalah suatu fasilitas untuk menempatkan system komputer dan perangkat-perangkat terkait, seperti Sistem komunikasi data dan penyimpanan data.
18. Standar Nasional Indonesia ISO/IEC 27001 yang selanjutnya disebut ISO adalah badan yang menetapkan standar internasional yang terdiri dari wakil-wakil dari badan standardisasi nasional setiap negara.
19. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
20. *Brute Force Attacks* adalah upaya mendapatkan akses sebuah akun dengan menebak *user name* dan *password* yang digunakan.
21. *Virtual Private Network* yang selanjutnya VPN adalah layanan koneksi yang memberikan akses ke *website* secara aman (*secure*) dan pribadi (*private*) dengan mengubah jalur koneksi melalui server dan menyembunyikan pertukaran data yang terjadi.
22. *Local Area Network* yang selanjutnya disebut LAN adalah suatu jaringan komputer dengan cakupan wilayah jaringan sangat kecil atau terbatas.
23. *Wide Area Network* yang selanjutnya disingkat WAN adalah jaringan komputer yang membentang di wilayah geografis yang luas, meskipun mungkin terbatas dalam batas-batas Negara dan dapat juga berupa koneksi LAN yang satu ke LAN yang lain.

24. *Personal Identification Number* yang selanjutnya disingkat PIN adalah sebuah fitur keamanan untuk mengunci atau mengamankan perangkat, akun atau data agar tidak dapat terakses oleh orang lain yang tidak bertanggungjawab.
 25. *User Identification* yang selanjutnya disebut User ID adalah serangkaian huruf yang merupakan tanda pengenal untuk masuk dan mengakses internet.
 26. Kode Program adalah suatu rangkaian pernyataan atau deklarasi yang ditulis dalam bahasa pemrograman komputer yang terbaca.
 27. *Logical* adalah metode akses ke Kode Program secara non fisik.
 28. *Versioning* adalah metode yang dibutuhkan setiap kali merilis aplikasi atau *software*, agar pengguna tahu pada tahap atau versi berapa aplikasi yang sedang dipakai.
 29. Hashing adalah suatu kode dari hasil enkripsi yang umumnya terdiri dari huruf maupun angka yang diacak.
 30. Hak Akses Khusus adalah hak yang melekat pada individu atau kelompok yang telah mendapat otorisasi untuk dapat mengakses suatu *file*, data atau program yang tidak dapat diakses oleh orang lain.
 31. Anggaran Pendapatan dan Belanja Daerah yang selanjutnya disingkat APBD adalah Anggaran Pendapatan dan Belanja Daerah Provinsi.
 32. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
 33. Penyelenggara Teknologi Informasi adalah orang, Badan Usaha, Penyelenggara Negara dan/atau masyarakat yang mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisa dan/atau menyebarkan informasi baik secara sendiri-sendiri maupun bersama-sama untuk keperluan dirinya dan/atau keperluan pihak lain.
2. Di antara Pasal 17 dan Pasal 18 disisipkan 1 (satu) pasal, yakni Pasal 17A yang berbunyi sebagai berikut:

Pasal 17A

- (1) PD/Unit Kerja harus menyusun standar dan prosedur pengendalian kegiatan Teknologi Informasi yang memenuhi prasyarat keamanan informasi dan untuk mengimplementasikan tindakan dalam mengelola Risiko.
- (2) Prasyarat keamanan informasi sebagaimana dimaksud pada ayat (1), meliputi aspek sebagai berikut :
 - a. organisasi keamanan informasi;
 - b. keamanan sumber daya manusia;
 - c. pengelolaan aset;

- d. pengendalian akses;
- e. kriptografi;
- f. keamanan fisik dan lingkungan;
- g. keamanan operasional;
- h. keamanan komunikasi;
- i. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
- j. hubungan kerja dengan pemasok (*supplier*);
- k. penanganan insiden keamanan informasi;
- l. kelangsungan usaha; dan
- m. kepatuhan.

3. Di antara Pasal 18 dan Pasal 19 disisipkan 1 (satu) pasal yakni Pasal 18A yang berbunyi sebagai berikut:

Pasal 18A

- (1) Untuk mengurangi Risiko sebagaimana dimaksud dalam Pasal 17A ayat (2) huruf g, PD/Unit Kerja sebagai Penyelenggara Teknologi Informasi wajib menerapkan proses manajemen Risiko dalam SMKI.
 - (2) Proses manajemen Risiko sebagaimana dimaksud pada ayat (1), meliputi:
 - a. identifikasi;
 - b. pengukuran;
 - c. pemantauan; dan
 - d. pengendalian atas risiko terkait penggunaan Teknologi Informasi.
 - (3) Manajemen Risiko sebagaimana dimaksud pada ayat (2), meliputi:
 - a. pengembangan sistem;
 - b. operasional Teknologi Informasi;
 - c. jaringan komunikasi, penggunaan perangkat komputer;
 - d. pengendalian terhadap informasi; dan
 - e. penggunaan pihak ketiga sebagai penyedia jasa Teknologi Informasi.
 - (4) Penerapan manajemen Risiko harus dilakukan secara terintegrasi pada setiap penggunaan operasional Teknologi Informasi terkait sistem informasi.
4. Di antara Pasal 20 dan Pasal 21 disisipkan 2 (dua) pasal, yakni Pasal 20A dan Pasal 20B, yang berbunyi sebagai berikut:

Pasal 20A

- (1) PD/Unit Kerja harus menerapkan prinsip pengendalian terhadap aktivitas Teknologi Informasi melalui proses evaluasi dan monitoring secara berkala.

- (2) Setiap PD/Unit Kerja wajib melakukan kegiatan pemantauan dan tindakan koreksi penyimpangan terhadap kontrol keamanan informasi yang meliputi :
 - a. kegiatan pemantauan secara terus menerus; dan
 - b. pelaksanaan fungsi pemeriksaan intern yang efektif dan menyeluruh.
- (3) PD/Unit Kerja Penyelenggara Teknologi Informasi berdasarkan hasil audit, umpan balik maupun evaluasi terhadap pengendalian keamanan informasi yang dilakukan, meningkatkan efektivitas sistim manajemen keamanan informasi secara berkesinambungan melalui perbaikan terhadap akibat penyimpangan kegiatan Teknologi Informasi.
- (4) Hasil dari tindakan perbaikan dan peningkatan sebagaimana dimaksud pada ayat (3), harus dilaporkan kepada kepala PD/Unit Kerja dan didokumentasikan sebagai bagian dari proses pembelajaran atau *lesson learned* bagi PD/Unit Kerja.

Pasal 20B

- (1) Apabila terjadi kebocoran informasi pada PD/Unit Kerja terkait yang berdampak sangat luas, Pemerintah Daerah dapat menunjuk auditor independen untuk melakukan investigasi yang diperlukan.
 - (2) PD/Unit Kerja Penyelenggara Teknologi Informasi wajib menyediakan akses kepada auditor independen sebagaimana dimaksud pada ayat (1) untuk melakukan pemeriksaan seluruh aspek terkait penyelenggaraan Teknologi Informasi.
 - (3) Pimpinan PD/Unit Kerja menyediakan sumber daya yang dibutuhkan untuk membentuk, mengimplementasikan, memelihara dan meningkatkan penerapan SMKI secara berkesinambungan.
 - (4) Uraian lebih lanjut mengenai SMKI sebagaimana dimaksud pada ayat (3) adalah sebagaimana tercantum dalam Lampiran dan merupakan bagian yang tidak terpisahkan dari Peraturan Gubernur ini.
5. Di antara Bab X dan Bab XI disisipkan 1 (satu) bab baru yakni Bab XA, yang berbunyi sebagai berikut :

BAB XA

SANKSI ADMINISTRATIF

Pasal 21A

- (1) PD/Unit Kerja yang melanggar ketentuan sebagaimana dimaksud dalam Pasal 18A ayat (1), Pasal 20A ayat (1) dan Pasal 20B ayat (2), dikenakan sanksi administratif oleh Gubernur.
- (2) Sanksi administratif sebagaimana dimaksud pada ayat (1), berupa :
 - a. teguran tertulis; dan
 - b. penghentian sementara Nama Domain NTT Prov.go.id.

- (3) Teguran tertulis sebagaimana dimaksud pada ayat (2) huruf a, diberikan setelah ditemukannya pelanggaran.
- (4) Penghentian sementara Nama Domain NTT Prov.go.id sebagaimana dimaksud pada ayat (2) huruf b, dikenakan apabila dalam waktu 6 (enam) bulan PD/Unit Kerja tidak mematuhi teguran tertulis sebagaimana dimaksud pada ayat (3).

Pasal II

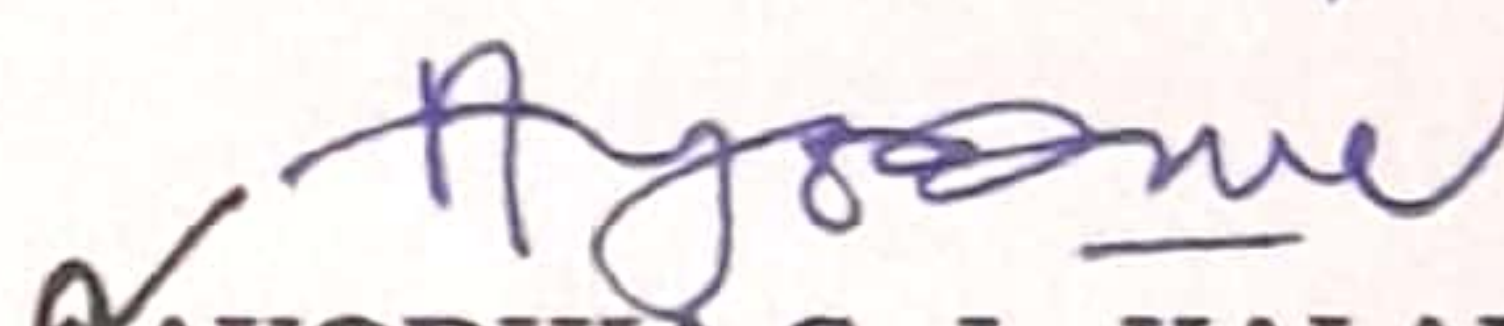
Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan Pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Nusa Tenggara Timur.

Ditetapkan di Kupang

pada tanggal 6 Oktober 2023

PJ. GUBERNUR NUSA TENGGARA TIMUR,

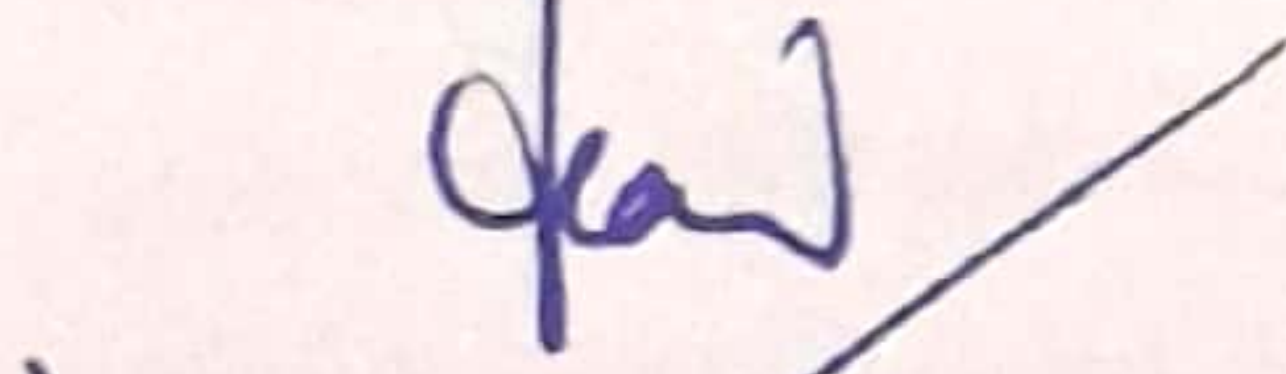

AYODHIA G. L. KALAKE

Diundangkan di Kupang

pada tanggal 6 Oktober 2023

SEKRETARIS DAERAH

PROVINSI NUSA TENGGARA TIMUR,


KOSMAS D. LANA

BERITA DAERAH PROVINSI NUSA TENGGARA TIMUR TAHUN 2023 NOMOR 053

LAMPIRAN

PERATURAN GUBERNUR NUSA TENGGARA TIMUR

NOMOR : 63 TAHUN 2023

TAHUN : 2023

TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN
PEMERINTAH PROVINSI NUSA TENGGARA TIMUR

BAB I

SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Tujuan

Sistem Manajemen Keamanan Informasi (SMKI) ini disusun sebagai arahan dan pedoman dalam pengelolaan sistem manajemen keamanan informasi secara terpadu serta untuk pengamanan aset informasi guna memastikan terjaganya aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

B. Kebijakan

1. PD/Unit Kerja berkomitmen untuk mengembangkan, mengimplementasikan, memelihara dan meningkatkan Sistem Manajemen Keamanan Informasi (SMKI) secara berkesinambungan untuk menjamin keamanan informasi organisasi dari risiko keamanan informasi, baik dari pihak internal maupun eksternal.
2. Seluruh informasi dalam bentuk fisik maupun elektronik, yang dikomunikasikan langsung atau melalui teknologi komunikasi harus dilindungi dari kemungkinan kerusakan, kesalahan penggunaan baik secara sengaja atau tidak, dicegah dari akses oleh pengguna yang tidak berwenang dan dari ancaman terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).
3. PD/Unit Kerja berkomitmen untuk mendukung pemenuhan prasyarat internal maupun eksternal keamanan informasi PD/Unit Kerja yang relevan.
4. PD/Unit Kerja berkomitmen untuk mematuhi seluruh peraturan perundang-undangan, regulasi dan kewajiban kontrak yang relevan.
5. PD/Unit Kerja berkomitmen untuk memastikan ketersediaan dari sumber daya yang dibutuhkan oleh SMKI di PD/Unit Kerja untuk menjamin terciptanya SMKI yang efektif dan efisien.

6. Kontrol keamanan informasi beserta sasaran masing-masing ditetapkan oleh Kepala Dinas Komunikasi dan Informatika Provinsi Nusa Tenggara Timur secara tahunan, didasarkan atas hasil identifikasi dan analisis resiko yang sesuai dengan ruang lingkup kebijakan SMKI, serta prioritas dengan mempertimbangkan ketersediaan dan kemampuan sumber daya.
7. Kebijakan keamanan informasi harus dikomunikasikan ke seluruh pegawai dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.
8. PD/Unit Kerja berkomitmen meningkatkan kepedulian (*awareness*), pengetahuan dan keterampilan tentang keamanan informasi bagi pegawai, serta mitra pihak ketiga lain sejauh diperlukan.
9. Seluruh kelemahan keamanan informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan TIK atau gangguan keamanan informasi harus segera dilaporkan kepada penanggung jawab TIK terkait.
10. Seluruh pimpinan di semua tingkatan bertanggung jawab menjamin kebijakan ini diterapkan di seluruh unit kerja di bawah pengawasannya.
11. Seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan aset informasi serta mematuhi kebijakan dan prosedur keamanan informasi yang telah ditetapkan.
12. Setiap pelanggaran terhadap kebijakan ini dapat dikenai sanksi administratif sesuai ketentuan peraturan perundang-undangan.
13. Setiap pengecualian terhadap kebijakan ini dan kebijakan turunannya harus mendapat persetujuan dari Dinas.
14. Dokumen ini harus ditinjau paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau apabila terdapat perubahan signifikan dalam proses bisnis organisasi untuk menjamin kesesuaian dan kecukupan dengan kondisi terkini.
15. Setiap perubahan terhadap dokumen ini harus didokumentasikan dan disetujui melalui proses manajemen perubahan.

BAB II

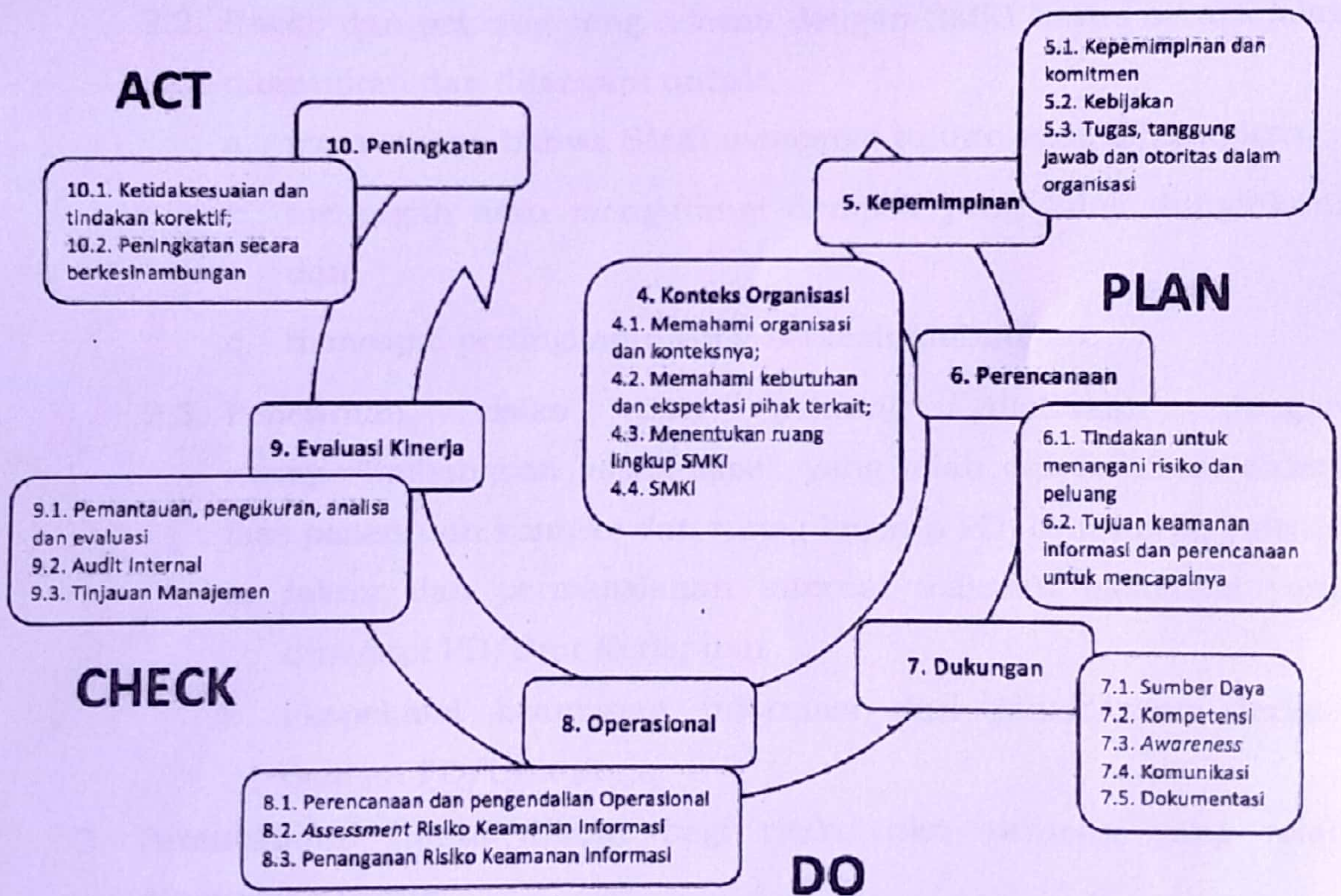
PEDOMAN PELAKSANAAN SISTIM MANAJEMEN KEAMANAN INFORMASI

A. Tujuan

Tata kelola Sistem Manajemen Keamanan Informasi (SMKI) disusun dalam rangka untuk memastikan efektivitas dan efisiensi dari sistem manajemen keamanan informasi. Kerangka kerja ini akan menjabarkan proses-proses dan aktivitas-aktivitas yang harus dijalankan oleh PD/Unit Kerja dalam rangka menetapkan, mengimplementasikan, memelihara SMKI dan meningkatkan secara berkesinambungan.

B. Kebijakan

1. PD/Unit Kerja harus merencanakan suatu sistem manajemen keamanan informasi dengan mengadopsi siklus proses pada standard ISO 27001:2013. Deskripsi umum tentang siklus proses berdasarkan arahan standar ISO/IEC 27001:2013 dapat dilihat dari Gambar 1 sebagai berikut :



Gambar 1: Penggunaan siklus proses PDCA dalam proses SMKI

2. Proses perencanaan dalam pengembangan sistem manajemen keamanan informasi meliputi:

- 2.1. PD/Unit Kerja harus menentukan konteks dan ruang lingkup SMKI organisasi dengan cara:

- a. menentukan dan secara berkala meninjau faktor serta permasalahan internal dan eksternal yang dihadapi oleh organisasi yang :

- 1) Relevan dengan tujuan dari PD/Unit Kerja dan SMKI;
 - 2) Mempengaruhi kemampuan PD/Unit Kerja untuk mencapai tujuan SMKI yang diharapkan oleh PD/Unit Kerja.
- b. menentukan dan secara berkala meninjau pihak - pihak yang terkait dengan PD/Unit Kerja dan dapat mempengaruhi SMKI di PD/Unit Kerja;
 - c. menentukan dan secara berkala meninjau kebutuhan dan ekspektasi terkait keamanan informasi dari pihak-pihak yang terkait tersebut;
 - d. menentukan dan secara berkala meninjau hubungan dan ketergantungan antar proses dan aktivitas PD/Unit Kerja yang dilaksanakan oleh pihak internal maupun pihak eksternal PD/Unit Kerja;
 - e. menentukan dan secara berkala meninjau ruang lingkup dari SMKI di organisasi.
- 2.2. Risiko dan peluang yang relevan dengan SMKI harus secara jelas ditentukan dan ditangani untuk:
- a. memastikan bahwa SMKI mencapai tujuan yang diharapkan;
 - b. mencegah atau mengurangi dampak yang tidak diinginkan; dan
 - c. mencapai peningkatan yang berkesinambungan.
- 2.3. Penentuan risiko dan peluang dilakukan dengan mempertimbangkan aspek-aspek yang telah didefinisikan dalam fase penentuan konteks dan ruang lingkup PD/Unit Kerja, yaitu:
- a. faktor dan permasalahan internal maupun eksternal yang dihadapi PD/Unit Kerja; dan
 - b. ekspektasi keamanan informasi dari pihak yang terkait dengan PD/Unit Kerja.
3. Perencanaan harus dibuat bagi risiko dan peluang yang telah ditentukan untuk:
- a. menangani risiko dan peluang;
 - b. mengintegrasikan dan mengimplementasikan tindakan untuk menangani risiko dan peluang dengan proses SMKI; dan
 - c. mengevaluasi efektivitas dari tindakan yang diambil dalam rangka menangani risiko dan peluang.
4. Proses manajemen risiko dilakukan melalui proses literatif yang mencakup aktivitas assessment risiko, penanganan risiko, penerimaan risiko dan pengkomunikasian risiko.

5. Seluruh manajemen risiko di organisasi harus dilakukan paling tidak 1 (satu) kali dalam satu tahun atau apabila terdapat usulan atau telah terjadi perubahan yang relevan dan signifikan pada organisasi. Seluruh catatan (*record*) terkait dengan seluruh proses manajemen risiko harus dibuat dan dipelihara.
6. Dalam proses pemilihan dari kontrol terhadap pengendalian risiko tersebut dilakukan pada saat aktifitas penanganan risiko yang merupakan bagian dari proses manajemen risiko.
7. Pemilihan dari kontrol tersebut dapat memperhatikan kontrol keamanan informasi berdasarkan standar ISO 27001:2013 atau kontrol lainnya sesuai ketentuan peraturan perundang-undangan.
8. Dalam hal proses pendokumentasian SMKI perlu memperhatikan aspek sebagai berikut:
 - 8.1. Dokumentasi SMKI di PD/Unit Kerja perlu mencakup informasi terdokumentasi yang disyaratkan oleh ISO 27001:2013 yang mencakup namun tidak terbatas pada:
 - a. ruang lingkup SMKI;
 - b. kebijakan dan tujuan keamanan informasi;
 - c. metodologi assessment dan penanganan risiko;
 - d. *statement of applicability*;
 - e. rencana penanganan risiko;
 - f. laporan *assessment* risiko;
 - g. pendefinisian tugas dan tanggung jawab keamanan informasi;
 - h. inventarisasi aset;
 - i. aturan terkait penggunaan aset;
 - j. kebijakan pengendalian akses;
 - k. prosedur operasional untuk manajemen TI;
 - l. prinsip rekayasa sistem secara aman;
 - m. kebijakan keamanan terkait penyedia jasa;
 - n. prosedur pengelolaan insiden;
 - o. prosedur keberlanjutan bisnis;
 - p. prasyarat hukum, regulasi dan kontraktual;
 - q. catatan terkait pelatihan, kemampuan, pengalaman dan kualifikasi;
 - r. hasil pemantauan dan pengukuran SMKI;

- s. program audit internal;
- t. hasil audit internal;
- u. hasil dari tinjauan manajemen;
- v. hasil dari tindakan korektif;
- w. log dari aktifitas pengguna, pengecualiaan dan kejadian keamanan; dan
- x. informasi terdokumentasi yang dibutuhkan untuk menjamin efektifitas dari SMKI.

8.2. Dokumen yang relevan dengan SMKI dan berasal dari pihak eksternal seperti dokumen peraturan perundang-undangan harus diidentifikasi dan dikendalikan juga;

8.3. Terkait proses peninjauan dan pembaruan dokumentasi, hal-hal berikut berlaku:

- a. semua dokumentasi SMKI harus ditinjau paling sedikit satu kali dalam 1 (satu) tahun atau apabila terdapat perubahan dalam SMKI dan/atau organisasi untuk menjamin kesesuaian dan kecukupannya dengan kondisi terkini SMKI dan keamanan informasi di organisasi;
- b. peninjauan harus dilakukan oleh pemilik dari dokumentasi dan dapat melibatkan pihak-pihak yang terkait dengan dokumentasi dan/atau proses yang relevan dengan dokumentasi tersebut;
- c. setiap pengkinian terhadap dokumentasi SMKI sebagai hasil dari peninjauan dokumentasi harus disetujui oleh manajemen yang relevan di PD/Unit Kerja;

8.4. Terkait proses salinan, distribusi dan retensi dokumentasi, hal-hal berikut berlaku:

- a. salinan dari dokumentasi SMKI harus didistribusikan kepada pihak internal yang terkait untuk memastikan operasional SMKI secara efektif;
- b. akses ke dokumentasi SMKI untuk pihak internal akan diberikan berdasarkan kebutuhan pengguna untuk mengakses dokumentasi tersebut (*need to know basis*);
- c. pihak eksternal yang memerlukan akses kepada dokumentasi SMKI akan diberikan akses hanya setelah kontrol keamanan informasi yang memadai telah diimplementasikan. Hal ini mencakup namun tidak terbatas pada akses *read only* atau perjanjian kerahasiaan;

- d. daftar distribusi harus ditetapkan dan dipelihara untuk mengendalikan distribusi dari dokumentasi SMKI; dan
 - e. kecuali diputuskan berbeda, seluruh dokumen SMKI memiliki masa retensi selama 10 tahun.
9. Instansi harus mempertimbangkan penyediaan sumber daya dalam melaksanakan sistem manajemen keamanan informasi yang mencakup:
- 9.1. ketersediaan sumber daya yang dibutuhkan bagi pelaksanaan SMKI secara efektif dan efisien sangatlah penting. Oleh karena itu perencanaan yang baik sangatlah penting untuk memastikan ketersediaan sumber daya yang tepat pada waktu yang tepat pula;
 - 9.2. sumber daya yang dibutuhkan oleh SMKI mencakup sumber daya dengan kompetensi dan pemahaman yang memadai, dokumentasi, proses dan solusi teknis, baik berupa perangkat keras maupun perangkat lunak;
 - 9.3. perencanaan sumber daya SMKI dapat dilakukan bersamaan dengan proses perencanaan dan penyusunan anggaran tahunan organisasi; dan
 - 9.4. pelatihan dan program peningkatan kesadaran terkait dengan SMKI dan keamanan informasi organisasi akan dilakukan secara berkala bagi seluruh pengguna sistem informasi organisasi. Program pelatihan dan peningkatan kesadaran tersebut akan dirancang sesuai dengan fungsi dan tanggung jawab pengguna.
10. Komunikasi yang relevan dengan SMKI, baik internal maupun eksternal, harus dikendalikan dan dikoordinasikan untuk memastikan:
- a. efektivitas alur pertukaran informasi dalam organisasi SMKI dan/atau dari dan ke pihak eksternal;
 - b. tidak ada kebocoran informasi sensitif milik PD/Unit Kerja;
 - c. jalur komunikasi SMKI mencakup:
 - 1) komunikasi tatap muka;
 - 2) surat dan memo internal;
 - 3) *email*;
 - 4) *website*PD/Unit Kerja;
 - 5) pengumumanPD/Unit Kerja; dan
 - 6) material cetak.

- d. personil PD/Unit Kerjayang tidak ditunjuk untuk memberikan materi informasi tidak diperbolehkan untuk memberikan informasi apapun;
 - e. informasiterkait dengan SMKI dan/atau keamanan informasi yang berasal dari sumber eksternal harus dikirimkan kepada koordinator SMKI untuk peninjauan dan pendistribusian kepada pihak yang relevan dalam SMKI organisasi. Hal ini mencakup:
 - 1) penerbitan peraturan hukum dan perundangan yang baru maupun perubahan terhadap peraturan lama;
 - 2) usulan perubahan terhadap prasyarat keamanan informasi;
 - 3) teknologi, ancaman dan kelemahan baru terkait keamanan informasi.
11. Proses perencanaan dan pengendalian operasional SMKI harus dikoordinasikan dan dikomunikasikan. Proses perencanaan operasional SMKI harus dilakukan secara tahunan serta didokumentasikan dan dikomunikasikan kepada pihak yang terkait dengan SMKI. Proses pengendalian operasional SMKI adalah proses yang dilakukan untuk memastikan pelaksanaan operasional SMKI PD/Unit Kerja telah sesuai dengan perencanaan yang telah dibuat. Proses pengendalian ini dapat mencakup aktifitas rapat peninjauan dan harus dilakukan paling sedikit 1 (satu) kali dalam tiga bulan serta melibatkan personil yang terlibat di SMKI PD/Unit Kerja.
12. Metode untuk mencegah, mendeteksi dan menindaklanjuti pelanggaran terhadap hukum terkait HAKI perlu disusun dan diimplementasikan. Hal ini dapat mencakup aktivitas pemantauan, pengukuran, peninjauan dan/atau audit.
13. Pemantauan, pengukuran, analisis dan evaluasi dari implementasi dan operasional SMKI organisasi adalah aktivitas periodik yang dilakukan untuk mengevaluasi kinerja keamanan informasi dan efektivitas SMKI organisasi. Proses pemantauan, pengukuran, analisis, dan evaluasi mencakup:
- 13.1. metrik pemantauan dan pengukuran harus dipilih secara seksama untuk memastikan bahwa aktivitas pengukuran akan memberikan pemahaman mendalam mengenai kinerja SMKI dan kontrol pengendalian keamanan informasi PD/Unit Kerja;
 - 13.2. proses pengukuran tersebut mencakup proses-proses berikut:
 - a. penentuan dari metrik pengukuran;

- b. pengukuran dari metrik yang telah ditentukan;
- c. analisis dan evaluasi dari hasil pengukuran.

13.3. dalam menentukan metrik pengukuran, aspek-aspek berikut harus dipertimbangkan:

- a. sasaran SMKI yang diberikan pada kebijakan SMKI PD/Unit Kerja;
- b. kontrol keamanan informasi yang diimplementasikan;
- c. metode dalam mengumpulkan data dan mengkalkulasi metrik;
- d. target pencapaian dari metrik;
- e. jadwal untuk melakukan pengukuran;
- f. personil yang bertanggung jawab untuk proses pengukuran.

13.4. metrik pengukuran yang telah ditentukan harus memungkinkan evaluasi dari pencapaian sasaran SMKI';

13.5. metrik yang telah ditetapkan harus dipantau dengan mengumpulkan data yang relevan dengan metrik;

13.6. proses pengukuran harus dilakukan minimal 1 (satu) kali dalam satu tahun terutama untuk mengukur pencapaian dari sasaran SMKI;

13.7. hasil dari pengukuran harus dianalisis dan dievaluasi untuk menentukan pencapaian dari target pengukuran tersebut;

13.8. hasil dari pengukuran harus dilaporkan kepada manajemen puncak SMKI dalam rapat tinjauan manajemen SMKI;

13.9. hasil dari proses pemantauan dan pengukuran efektivitas SMKI harus dianalisis dan dievaluasi untuk menentukan apakah implementasi dan operasi SMKI organisasi:

- a. sesuai dengan kebijakan, tujuan, standar dan prosedur SMKI organisasi;
- b. memadai untuk menghadapi kebutuhan dan tantangan bisnis serta teknologi terkini; dan
- c. sesuai dengan rencana SMKI yang sudah dibuat.

14. Peninjauan keamanan informasi secara independen harus secara rutin dilakukan.

14.1. peninjauan tersebut harus mencakup:

- a. kontrol dan area keamanan informasi, seperti keamanan fisik, jaringan atau akses *logical*;

- b. kebijakan, proses dan prosedur yang relevan dengan SMKI;
 - c. kepatuhan implementasi SMKI dan keamanan informasi dengan kebijakan, proses dan prosedur keamanan informasi PD/Unit Kerja serta prasyarat hukum, perundangan serta kewajiban kontraktual terkait dengan SMKI;
 - d. peninjauan teknis terhadap fasilitas pengolahan informasi dan sarana pendukungnya.
- 14.2. hasil dari peninjauan harus didokumentasikan dan dilaporkan kepada manajemen SMKI yang relevan.
- 14.3. setiap permasalahan dan/atau ketidaksesuaian harus segera ditindaklanjuti dengan cara mengidentifikasi tindakan korektif dan/atau peningkatan yang sesuai.
15. Instansi harus melakukan proses audit internal dengan ketentuan sebagai berikut:
- 15.1. audit internal SMKI di PD/Unit Kerja harus dilaksanakan minimal satu kali dalam satu tahun dan harus mencakup seluruh ruang lingkup SMKI;
 - 15.2. audit internal SMKI harus dilakukan oleh auditor yang memiliki kompetensi yang memadai serta memiliki objektivitas dan imparialitas terhadap proses audit;
 - 15.3. auditor yang dipilih untuk proses audit harus ditunjuk secara formal oleh manajemen puncak SMKI;
 - 15.4. sebuah program audit tahunan SMKI harus ditetapkan oleh koordinator audit internal SMKI dan harus dikomunikasikan kepada koordinator SMKI;
 - 15.5. program audit harus mencakup jadwal, metode, kriteria dan ruang lingkup, tanggung jawab serta prasyarat pelaporan dari audit;
 - 15.6. proses audit harus dilakukan sesuai dengan program audit yang telah ditetapkan secara formal;
 - 15.7. temuan audit harus diklasifikasikan berdasarkan kritikalitas dan cakupan dari temuan tersebut menjadi:
 - a. mayor, ketidaksesuaian ini mengindikasikan tidak berjalannya sama sekali sebuah proses SMKI atau kontrol keamanan informasi, atau apabila sebuah temuan dapat menyebabkan dampak buruk terhadap proses atau sistem kritikal organisasi;

- b. minor, ketidaksesuaian ini mengindikasikan sebuah kealpaan/problem kecil yang tidak mengindikasikan bahwa sebuah proses SMK I atau kontrol keamanan informasi tidak berjalan sama sekali, atau apabila sebuah temuan tidak akan menyebabkan dampak buruk terhadap proses atau sistem kritikal perusahaan; dan
 - c. peluang untuk perbaikan, kategori temuan ini bukan merupakan sebuah ketidaksesuaian namun mengindikasikan bahwa sebuah area dapat diperbaiki untuk meningkatkan kinerja dari proses atau sistem.
- 15.8. setiap ketidaksesuaian dan/atau peluang untuk perbaikan yang ditemukan dalam proses audit harus dicatat secara formal oleh auditor dan diterima oleh *auditee*;
- 15.9. setiap ketidaksesuaian harus dikoreksi dan ditingkatkan oleh *auditee* dalam jangka waktu yang disepakati dengan cara merencanakan dan melaksanakan koreksi dan tindakan korektif;
- 15.10. laporan audit harus dilaporkan kepada manajemen puncak PD/Unit Kerja dan dikomunikasikan kepada koordinator SMK I;
- 15.11. koordinator SMK I dan auditor internal SMK I bertanggung jawab untuk memantau dan memverifikasi koreksi, tindakan korektif maupun peningkatan terkait ketidaksesuaian yang ditemukan dalam audit;
- 15.12. verifikasi dari auditor internal SMK I dibutuhkan sebelum ketidaksesuaian yang ditemukan dapat dinyatakan ditutup secara formal.
16. Manajemen SMK I PD/Unit Kerja wajib untuk melaksanakan tinjauan manajemen SMK I minimal satu kali dalam satu tahun atau apabila terjadi perubahan signifikan terhadap SMK I di PD/Unit Kerja. Tinjauan ini dilakukan untuk menjamin terjaganya kesesuaian, kecukupan dan efektivitas dari SMK I di PD/Unit Kerja, dengan memperhatikan hal-hal sebagai berikut:
- 16.1. Tinjauan manajemen SMK I harus dihadiri oleh:
- a. manajemen puncak dari SMK I di PD/Unit Kerja;
 - b. koordinator SMK I PD/Unit Kerja;
 - c. koordinator atau petugas fungsional SMK I.

- 16.2. Apabila dibutuhkan, tinjauan manajemen SMKI dapat dihadiri oleh:
- a. pemangku kepentingan yang relevan dari SMKI di unit kerja yang membidangi teknologi informatika;
 - b. *subject matter expert* yang memadai.
- 16.3. Tinjauan manajemen SMKI harus mencakup masukan sebagai berikut:
- a. status dari tindakan yang diputuskan pada tinjauan manajemen terdahulu;
 - b. perubahan baik internal maupun eksternal yang terkait dengan SMKI;
 - c. masukan terkait kinerja keamanan informasi yang mencakup *trend* pada:
 - 1) ketidaksesuaian dan tindakan korektif;
 - 2) hasil pemantauan dan pengukuran;
 - 3) hasil audit, baik internal maupun eksternal; dan
 - 4) pemenuhan dari sasaran keamanan informasi.
 - d. masukan dari pihak terkait;
 - e. hasil dari *assessment* risiko dan status rencana penanganan risiko;
 - f. peluang untuk peningkatan secara berkesinambungan.
- 16.4. Berdasarkan dari masukan tersebut, tinjauan manajemen SMKI harus menghasilkan keluaran sebagai berikut:
- a. keputusan terkait peningkatan SMKI secara berkesinambungan; dan
 - b. peluang dan kebutuhan untuk perubahan SMKI.
- 16.5. setiap keluaran dari tinjauan manajemen SMKI harus digunakan sebagai dasar bagi peningkatan dan perencanaan tahunan SMKI.
17. Ketidaksesuaian SMKI didefinisikan sebagai kondisi dimana adanya prasyarat SMKI yang tidak terpenuhi. Setiap ketidaksesuaian atau tidak terpenuhinya prasyarat SMKI harus diidentifikasi dan di laporkan:
- 17.1. identifikasi dan laporan dari setiap ketidaksesuaian dapat didapatkan melalui:
- a. proses pengelolaan insiden keamanan informasi;
 - b. peninjauan internal SMKI;
 - c. proses audit internal SMKI;
 - d. proses pemantauan dan pengukuran SMKI;

- e. peninjauan dan/atau proses audit eksternal terhadap SMK atau keamanan informasi; dan
 - f. laporan dan masukan dari *stakeholder* yang terkait.
- 17.2. setiap ketidaksesuaian yang terjadi, harus ditangani secara tepat dengan cara:
- a. melakukan koreksi yang sesuai untuk mengendalikan dan memperbaiki ketidaksesuaian yang telah diidentifikasi; dan
 - b. menangani setiap akibat dari ketidaksesuaian yang mungkin terjadi.
- 17.3. untuk setiap ketidaksesuaian, evaluasi harus dilakukan untuk mengevaluasi kebutuhan untuk mengambil tindakan korektif untuk menghilangkan penyebab dari ketidaksesuaian supaya ketidaksesuaian tersebut tidak terjadi lagi atau terjadi ditempat lain.
- 17.4. tindakan korektif yang diambil harus sesuai dengan dampak dari ketidaksesuaian tersebut untuk memastikan bahwa ketidaksesuaian tersebut tidak berulang atau terjadi ditempat lain dalam ruang lingkup SMK.
- 17.5. evaluasi untuk menentukan apakah perlu untuk mengambil setiap tindakan korektif harus dilakukan dengan melakukan:
- a. peninjauan terhadap ketidaksesuaian yang terjadi;
 - b. menentukan penyebab dari ketidaksesuaian;
 - c. menentukan jika ada kejadian dimana ketidaksesuaian yang sama telah terjadi, atau dapat berpotensi untuk terjadi.
- 17.6. apabila ditentukan bahwa tindakan korektif memang perlu untuk diambil maka harus dilakukan perencanaan dan implementasi dari tindakan korektif.
- 17.7. setelah koreksi dan tindakan korektif telah diambil, sebuah peninjauan harus dilakukan untuk menjamin efektifitasnya dalam mencegah terjadinya kembali atau terjadinya ketidaksesuaian tersebut ditempat lain.
18. Kesesuaian, kecukupan dan efektifitas dari SMK PD/Unit Kerja harus secara berkesinambungan ditingkatkan.
19. Inisiatif peningkatan harus secara formal diidentifikasi, direncanakan, diimplementasikan dan ditinjau.
20. Identifikasi dari peningkatan harus dilakukan berdasarkan *log*, laporan dan hasil dari:

- a. proses pengelolaan insiden keamanan informasi;
 - b. peninjauan internal SMKI;
 - c. proses audit internal SMKI;
 - d. proses pemantauan dan pengukuran SMKI;
 - e. peninjauan dan/atau proses audit eksternal terhadap SMKI atau keamanan informasi; dan
 - f. laporan dan masukan dari *stakeholder* yang terkait.
21. Perencanaan dan implementasi dari inisiatif peningkatan harus ditinjau untuk memastikan bahwa inisiatif tersebut dapat mencapai tujuannya.
22. Dokumentasi yang relevan dengan proses peningkatan secara berkesinambungan harus dibuat dan dipelihara.

BAB III

MANAJEMEN RISIKO

A. Tujuan

Tujuan dari manajemen resiko adalah untuk mengelola risiko keamanan informasi yang dihadapi oleh organisasi dalam rangka untuk mempersiapkan diri terhadap terjadinya risiko beserta dampaknya.

B. Kebijakan

1. Kriteria penerimaan risiko dan penilaian keamanan informasi harus ditetapkan untuk memberikan arahan bagi PD terhadap penanganan risiko yang harus dilakukan.
2. PD harus menerapkan konteks terkait rencana perencanaan identifikasi Risiko yang meliputi isu-isu, pihak terkait dan prasyarat keamanan informasi internal dan eksternal yang terkait dengan keamanan informasi harus diidentifikasi dan ditetapkan sebagai pertimbangan dalam mengidentifikasi risiko keamanan informasi. Hal ini setidaknya mencakup:
 - a. kegiatan utama yang dilakukan oleh organisasi;
 - b. kebijakan internal organisasi;
 - c. proses bisnis organisasi;
 - d. kewajiban hukum, perundangan dan kewajiban kontrak yang dimiliki oleh organisasi;
 - e. kondisi teknologi informasi dan keamanan informasi, baik internal maupun eksternal yang relevan dengan organisasi.

3. PD harus melaksanakan penilaian risiko yang berpengaruh terhadap kegagalan sistem dan operasional TI terkait dengan aspek keamanan informasi yang mencakup aktivitas:

3.1. identifikasi risiko :

- a. mengidentifikasi ancaman, merupakan aktifitas untuk mengidentifikasi ancaman terhadap risiko keamanan informasi;
- b. ancaman didefinisikan sebagai potensi penyebab insiden yang tidak diinginkan yang dapat menyebabkan kerusakan/kerugian bagi organisasi dan sistemnya;
- c. sebuah ancaman tidak dapat dikatakan sebuah risiko apabila tanpa kombinasi dengan kelemahan yang dapat dieksploitasi;
- d. mengidentifikasi kelemahan dilakukan setelah pengidentifikasian ancaman dilakukan;
- e. kelemahan didefinisikan sebagai potensi kekurangan pada proses dan kontrol keamanan yang dapat dieksploitasi oleh satu ancaman atau lebih;
- f. mengidentifikasi dampak merupakan aktifitas yang dilakukan untuk mengidentifikasi potensi dampak jika ancaman yang teridentifikasi, mengeksploitasi kelemahan yang ada;
- g. risiko harus dialokasikan ke pemilik risiko; dan
- h. pemilik risiko bertanggung jawab untuk mengelola risiko yang telah teridentifikasi.

3.2. analisis risiko :

- a. menilai dampak potensial yang akan terjadi apabila risiko yang teridentifikasi terwujud;
- b. kriteria dampak merupakan parameter untuk menentukan tingkat kerugian terhadap risiko yang terjadi.

Contoh kriteria dampak adalah sebagai berikut :

Tabel 1 : dampak risiko SMKI

No	Tingkat Dampak	Operasional	Peraturan/ Hukum	Aset Informasi	Reputasi
1.	Ringan	Penundaan proses bisnis setengah hari	Tidak ada pelanggaran hukum	Tidak ada kebocoran atau kehilangan asset informasi	Tidak ada dampak terhadap reputasi PD/Unit Kerja
2.	Sedang	Penundaan proses bisnis 1 hari	Pelanggaran ringan dengan surat	Berdampak pada kebocoran	Mengganggu kepercayaan sebagian kecil

			peringatan	atau kehilangan aset informasi yang bersifat PUBLIK.	pihak eksternal. Berdampak pada reputasi PD/Unit Kerja namun reputasi dapat dipulihkan dalam waktu tidak terlalu lama.
3.	Berat	Penundaan proses bisnis 3 hari	Pelanggaran sedang yang dikenakan sanksi administratif	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat TERBATAS.	Mengganggu kepercayaan sebagian besar pihak eksternal. Berdampak pada reputasi PD/Unit Kerja dan pemulihan reputasi membutuhkan waktu yang lama.
4.	Sangat Berat	Penundaan proses bisnis lebih dari 3 hari	Pelanggaran berat dengan sanksi hukum	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat RAHASIA.	Mengganggu kepercayaan sebagian besar pihak eksternal, Berdampak pada reputasi SKPD/Unit Kerja dan sangat sulit dilakukan pemulihan reputasi.

c. Menilai kemungkinan realistis terjadinya risiko yang teridentifikasi; dan

d. Kriteria- kecenderungan merupakan parameter untuk menentukan tingkat kejadian terhadap Risiko.

Contoh kriteria kecenderungan adalah sebagai berikut:

Nilai Tingkat Frekuensi terjadinya	Kriteria Kecenderungan
1 Rendah	Kejadian tidak lebih dari 2 kali / tahun
2 Sedang	Kejadian lebih dari 2 kali / tahun, namun tidak lebih dari 5 kali / tahun
3 Tinggi	Kejadian lebih dari 5 kali / tahun, namun tidak lebih dari 10 kali / tahun
4 Ekstrim	Kejadian lebih dari 10 kali / tahun

e. Evaluasi Risiko :

- 1) membandingkan hasil analisis risiko dengan kriteria risiko yang sudah ditetapkan;
- 2) risiko yang masuk dalam kriteria penerimaan risiko akan diterima;
- 3) risiko yang tidak masuk dalam kriteria penerimaan risiko perlu mendapatkan penanganan; dan
- 4) setiap penanganan risiko harus diberikan prioritas.

4. Hasil evaluasi risiko harus dianalisis terkait risiko tersebut dapat diterima dalam level tertentu berdasarkan kriteria penerimaan risiko yang telah ditetapkan atau memerlukan penanganan risiko lebih lanjut.

Tabel risiko adalah matriks antara nilai dari dampak dan kecenderungan yang menghasilkan tingkat risiko.

Contoh tabel risiko adalah sebagai berikut:

		DAMPAK			
		1	2	3	4
KECENDERUNGAN	1	RENDAH			
	2				
	3			SEDANG	
	4				

5. Dalam hal risiko tersebut tidak dapat diterima, PD/Unit Kerja harus menerapkan penanganan risiko yang diperlukan yang mencakup :

- a. mengendalikan/*control* adalah merupakan tindakan pengendalian risiko dengan mengurangi dampak maupun kemungkinan terjadinya risiko melalui menerapkan suatu sistem atau aturan;
- b. menghindari/*avoid* adalah tindakan pengendalian risiko dengan tidak melakukan suatu aktivitas atau memilih aktivitas lain dengan output yang sama untuk menghindari terjadinya risiko;
- c. mengalihkan/*transfer* adalah tindakan pengendalian risiko dengan mengalihkan seluruh atau sebagian tanggung jawab pelaksanaan suatu proses kepada pihak ketiga.

6. Penanganan risiko harus memadai untuk mengurangi risiko ke tingkat yang dapat diterima berdasarkan kriteria penerimaan risiko.

7. Pemilik risiko harus memastikan setiap rencana penanganan risiko telah memadai dan relevan bagi risiko yang ada.
8. Setiap rencana penanganan risiko harus diberikan prioritas oleh pemilik risiko.
9. Setiap keputusan terkait dengan penanganan risiko dan kontrol keamanan risiko yang relevan harus disetujui oleh Pimpinan PD/Unit Kerja terkait.
10. PD/Unit Kerja harus melakukan proses pemantauan dan peninjauan risiko untuk memastikan efektifitas kontrol yang dilakukan yang mencakup:
 - a. proses pemantauan dan peninjauan risiko adalah proses berkesinambungan untuk memastikan bahwa :
 - 1) risiko baru telah teridentifikasi, di-assess dan ditangani;
 - 2) setiap perubahan terhadap risiko yang sudah ada telah teridentifikasi, di-assess dan ditangani;
 - 3) kontrol keamanan yang sudah ada telah memadai dan efektif dalam menangani risiko.
 - b. proses pemantauan dan peninjauan risiko harus dilakukan secara formal dan rutin;
 - c. PD/Unit Kerja harus menentukan frekuensi pemantauan dan peninjauan risiko.
11. PD/Unit Kerja harus melakukan proses komunikasi dan koordinasi risiko untuk memastikan pengelolaan penanganan kontrol terkendali dan efektif dalam mengurangi tingkat Risiko yang diharapkan.
12. Metode komunikasi dan koordinasi risiko harus ditetapkan yang meliputi:
 - a. proses komunikasi dan koordinasi risiko merupakan proses berkesinambungan untuk mengkomunikasi dan mengkoordinasikan setiap informasi, aktifitas dan keputusan terkait dengan risiko keamanan informasi dan proses manajemen risiko;
 - b. setiap informasi, aktifitas dan keputusan harus dikomunikasikan dan dikoordinasikan dengan pemilik risiko, personil terkait dan Kepala PD/Unit Kerja; dan
 - c. setiap komunikasi dan koordinasi eksternal terkait risiko keamanan informasi dan manajemen risiko harus disetujui oleh Kepala PD/Unit Kerja.

BAB IV

ORGANISASI SISTEM MANAJEMEN KEAMANAN INFORMASI

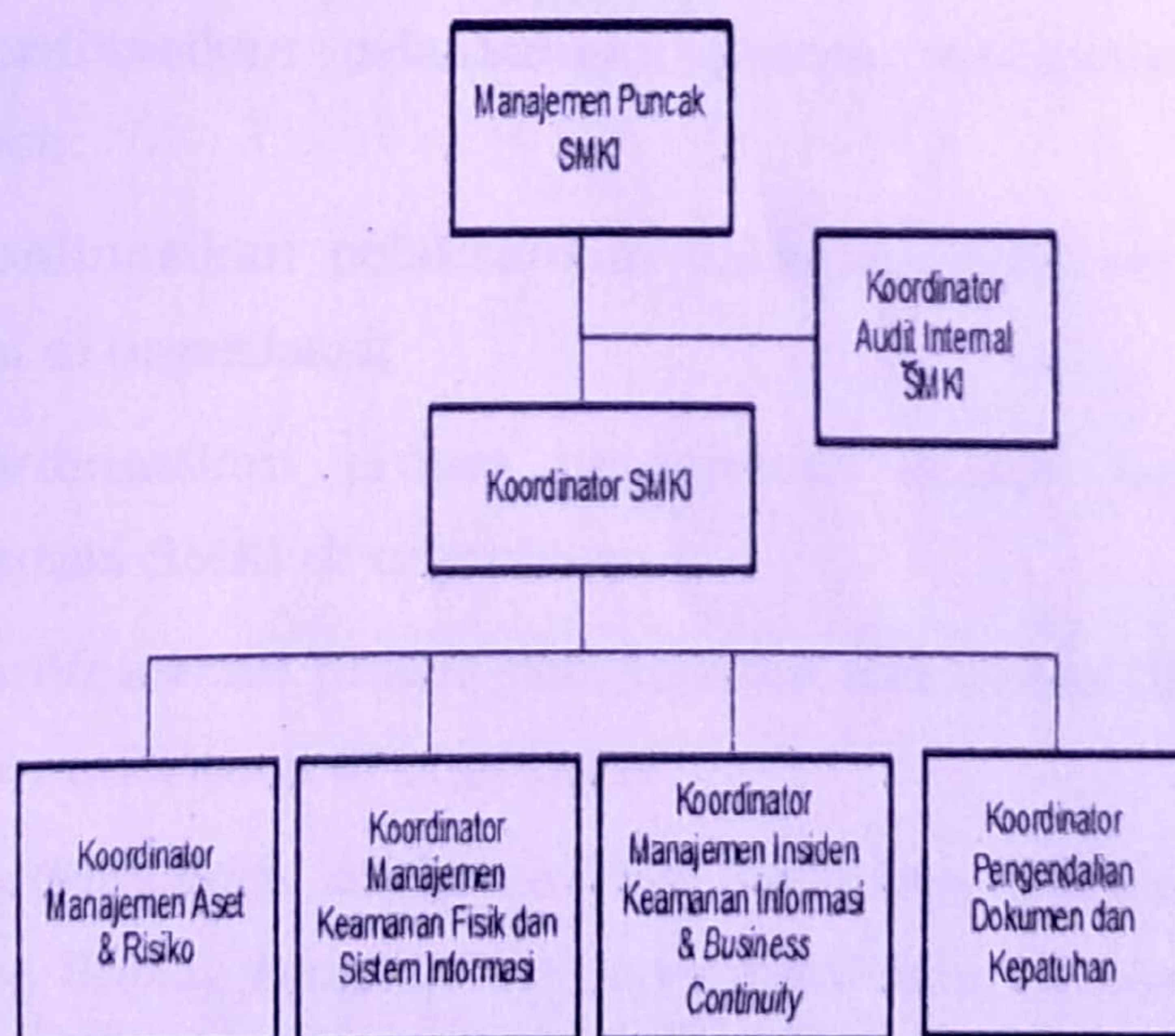
A. Tujuan

Organisasi Tim Keamanan Informasi Pemerintah Daerah Provinsi Nusa Tenggara Timur dibentuk dengan tujuan sebagai berikut:

1. Sebagai pedoman dalam pembentukan organisasi fungsional keamanan informasi yang bertanggung jawab dalam pengelolaan keamanan informasi serta hubungan kerja dengan pihak eksternal.
2. Menumbuhkan kesadaran pada SDM Pemerintah Daerah Provinsi Nusa Tenggara Timur tentang arti penting keamanan informasi.
3. Memastikan keamanan informasi terkait penggunaan perangkat *mobile* dan pelaksanaan aktivitas *teleworking*.

B. Kebijakan

1. PD/Unit Kerja wajib membentuk struktur organisasi berbasiskan Sistem Manajemen Keamanan Informasi untuk memastikan pelaksanaan keamanan informasi sesuai dengan standar ISO 27001:2013.
2. Organisasi Sistem Manajemen Keamanan Informasi merupakan organisasi fungsional yang memiliki struktur seperti yang tampak pada gambar berikut:



Gambar : Struktur Organisasi SMKI di PD/Unit Kerja

3. Manajemen puncak SMKI memiliki tugas dan tanggung jawab sebagai berikut:

- a. memberikan arahan dan tujuan umum dari SMKI organisasi, dalam bentuk kebijakan Sistem Manajemen Keamanan Informasi (SMKI);
- b. memastikan bahwa tujuan dan rencana dari SMKI organisasi telah ditetapkan;
- c. menetapkan struktur organisasi beserta alokasi tugas dan tanggung jawab dalam SMKI organisasi;
- d. mengkomunikasikan kepada personil dalam organisasi terkait pentingnya pemenuhan aturan terkait keamanan informasi organisasi sesuai ketentuan peraturan perundang-undangan serta perlunya peningkatan SMKI organisasi secara berkesinambungan;
- e. menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan SMKI organisasi;
- f. menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;
- g. menyetujui tingkat risiko residual keamanan informasi;
- h. memastikan pelaksanaan audit internal SMKI;
- i. menghadiri dan memimpin rapat tinjauan manajemen SMKI.

4.. Koordinator SMKI memiliki tugas dan tanggung jawab sebagai berikut:

- a. menyusun, mengkoordinasikan serta memantau pelaksanaan program kerja SMKI;
- b. mengkoordinasikan pelaksanaan proses manajemen risiko SMKI organisasi;
- c. mengkoordinasikan pelaksanaan aktifitas SMKI serta pengamanan informasi di organisasi;
- d. mengkoordinasikan proses peninjauan secara berkala terhadap implementasi SMKI di organisasi;
- e. mengkoordinasikan proses pengukuran efektivitas SMKI dan kontrol keamanan informasi di organisasi;
- f. mengkoordinasikan aktivitas dan tindakan untuk meningkatkan efektivitas SMKI, yang mencakup antara lain koreksi dan tindakan korektif untuk ketidaksesuaian yang ditemukan serta pelaksanaan rencana penanganan risiko; dan
- g. memberikan laporan secara berkala terkait kondisi SMKI dan keamanan informasi organisasi kepada manajemen puncak SMKI.

5. Koordinator audit internal SMKI memiliki tugas dan tanggung jawab sebagai berikut :
 - a. menyusun dan memantau program dan jadwal audit internal SMKI;
 - b. mengkoordinasikan pelaksanaan proses audit internal SMKI;
 - c. merangkum dan melaporkan hasil audit internal SMKI kepada manajemen puncak SMKI;
 - d. memberikan rekomendasi terkait kontrol keamanan informasi yang diperlukan untuk meningkatkan efektivitas SMKI; dan
 - e. mengkoordinasikan proses verifikasi koreksi dan tindakan korektif yang diambil terhadap ketidaksesuaian yang ditemukan dalam proses audit internal SMKI.
6. Koordinator manajemen aset dan risiko SMKI memiliki tugas dan tanggung jawab sebagai berikut :
 - a. mengkoordinasikan dan memantau pengelolaan aset informasi dan aset pengolahan dan penyimpanan informasi organisasi, hal ini mencakup proses registrasi, inventarisasi serta pemeliharaan inventarisasi aset tersebut;
 - b. menyusun dan memelihara dokumen registrasi aset informasi dan aset pengolahan dan penyimpanan informasi organisasi;
 - c. melakukan peninjauan terkait proses penanganan aset informasi dan aset pengolahan dan penyimpanan informasi organisasi berdasarkan kebijakan dan prosedur terkait pengelolaan aset SMKI organisasi;
 - d. menyusun dan mengkoordinasikan aktivitas proses pengelolaan manajemen risiko SMKI di organisasi, bekerja sama dengan pemilik risiko, berdasarkan kebijakan dan prosedur terkait pengelolaan risiko SMKI organisasi;
 - e. mengkoordinasikan proses registrasi terhadap risiko SMKI di organisasi, bekerja sama dengan pemilik risiko;
 - f. mengkoordinasikan pengkinian secara rutin terhadap registrasi risiko organisasi, bekerja sama dengan pemilik risiko; dan
 - g. menyusun dan memelihara dokumen *risk profile* dan *risk treatment plan* SMKI organisasi.
7. Koordinator manajemen keamanan fisik dan sistem informasi SMKI memiliki tugas dan tanggung jawab sebagai berikut :
 - a. mengkoordinasikan dan memantau proses dan aktifitas pengamanan fisik dan lingkungan dalam organisasi;

- b. melaksanakan proses pengelolaan dan pemeliharaan fasilitas pengamanan fisik organisasi berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan SMKI organisasi;
 - c. melaksanakan proses pengelolaan dan pemeliharaan hak akses fisik ke fasilitas organisasi berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan SMKI organisasi;
 - d. mengkoordinasikan dan memantau proses dan aktifitas pengelolaan akses *logical*;
 - e. melaksanakan proses pengelolaan dan pemeliharaan akses *logical* dari pengguna ke sistem informasi organisasi berdasarkan kebijakandan prosedur terkait keamanan akses *logical* ke sistem informasi organisasi, hal ini mencakup proses pendaftaran, pemeliharaan dan pencabutan hak akses *logical* pengguna ke sistem informasi;
 - f. mengakomodasi penyusunan dan pemeliharaan *access control matrix* bersama-sama dengan PD/Unit Kerja pemilik aplikasi dan/atau informasi;
 - g. mengkoordinasikan dan memantau pengelolaan keamanan operasional sistem informasi organisasi berdasarkan kebijakan dan prosedur terkait pengelolaan keamanan operasional sistem informasi organisasi; dan
 - h. merancang, memantau dan memelihara sistem keamanan dari sistem informasi organisasi yang mencakup perangkat keras, lunak maupun aktif jaringan dan keamanan jaringan dalam sistem informasi organisasi.
8. Koordinator manajemen insiden keamanan informasi dan *business continuity* SMKI memiliki tugas dan tanggung jawab sebagai berikut:
- a. mengkoordinasikan proses pendokumentasian laporan terkait kejadian, kelemahan dan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi organisasi;
 - b. mengkoordinasikan dan memantau pengelolaan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi organisasi;
 - c. mendokumentasikan proses pengelolaan insiden keamanan informasi di organisasi;
 - d. mengkoordinasikan dan memantau pengelolaan *business continuity management* di organisasi berdasarkan kebijakan dan prosedur terkait *business continuity management* organisasi;
- 

- e. mengkoordinasikan penyusunan, pengujian dan pemeliharaan *business continuity plan* dan *disaster recovery plan* organisasi;
 - f. memastikan terjaganya aspek keamanan informasi dalam proses *business continuity management*.
9. Koordinator pengendalian dokumen dan kepatuhan SMKI memiliki tugas dan tanggung jawab sebagai berikut :
- a. mengkoordinasikan dan memantau proses pengelolaan dokumentasi terkait SMKI organisasi hal ini mencakup kebijakan dan prosedur terkait SMKI organisasi;
 - b. mengidentifikasi dan mendokumentasikan peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi organisasi;
 - c. melakukan pemantauan berkala terhadap kepatuhan SMKI organisasi dengan prasyarat dari kebijakan dan prosedur SMKI organisasi serta peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi organisasi;
 - d. menyusun dan mengkoordinasikan pelaksanaan program *security awareness* bagi personil organisasi;
 - e. menyusun metrik pengukuran efektivitas SMKI dan kontrol keamanan informasi organisasi.
10. Pengelolaan Data Center di lingkungan Pemerintah Provinsi Nusa Tenggara Timur harus ditetapkan dalam keputusan Gubernur yang berkekuatan hukum mengikat dalam Peraturan Gubernur ini.
11. Pengelola Data Center tersebut berkewajiban melakukan pengamanan dan pemeliharaan berkelanjutan atas aset pengolahan serta penyimpanan informasi yang dikelola di *data center* dan aset informasi yang disimpan di *Data Center*.
12. Aset informasi yang merupakan isi (*content*) dari sistem informasi yang dimiliki oleh PD/Unit Kerja, dikelola oleh PD/Unit Kerja masing-masing sesuai kepemilikannya (*ownership*).
13. Penanggung jawab Pemilik Aset Informasi adalah Kepala PD/Unit Kerja terkait. Pemilik Aset Informasi bertanggung jawab melakukan pengamanan dan pemeliharaan secara berkelanjutan atas aset informasi.

14. PD/Unit Kerja harus menentukan tim keamanan informasi yang mempunyai tanggung jawab dalam berkoordinasi dengan pihak lain:

- a. mengidentifikasi pihak-pihak berwenang terkait keamanan informasi pada tingkat pemerintahan yang lebih tinggi (NTT Prov.CSIRT, Gov-CSIRT, Kementerian Komunikasi dan Informatika, penegak hukum, *Indonesia security incident response team on internet infrastructure (idsirtii)* dan sebagainya) serta menjalin kerja sama dalam rangka pelaporan dan koordinasi penanganan bersama atas gangguan keamanan informasi;
- b. tim keamanan informasi wajib berpartisipasi dalam keanggotaan komunitas atau forum yang relevan terkait keamanan informasi sebagai sarana meningkatkan keterampilan dan pengetahuan serta *best practice* terkini atas keamanan informasi; dan
- c. seluruh anggota Tim Keamanan Informasi dan pihak ketiga wajib menandatangani Perjanjian Kerahasiaan (*Non-Disclosure Agreements*) yang mengikat para pihak untuk menjaga kerahasiaan aset informasi.

Kebijakan dalam penggunaan Perangkat *Mobile* dan *Teleworking*

1. Penggunaan perangkat *mobile*, baik milik pribadi atau milik PD/Unit Kerja untuk mengakses dan/atau menyimpan informasi milik PD/Unit Kerja harus sangat dibatasi sesuai dengan kebutuhan pekerjaan dengan mempertimbangkan prinsip kehati-hatian saat menggunakan perangkat *mobile* dengan menghindari meninggalkan perangkat tanpa pengawasan.
2. Perangkat *mobile* harus mengaktifkan fitur otentikasi pengguna, seperti penggunaan *user name* dan *password*, sesuai dengan kebijakan terkait pengendalian akses.
3. Informasi sensitif harus dienkripsi atau dilindungi dengan *password* pada saat disimpan di *mobile device*, sesuai dengan klasifikasi informasinya.
4. Informasi sensitif milik PD/Unit Kerja yang disimpan pada perangkat *mobile device* harus di-*backup* secara berkala untuk menghindari hilangnya aspek ketersediaan dari informasi.
5. Aktivitas *teleworking* sebagai sarana pegawai untuk bekerja dari lokasi di luar area kerja PD/Unit Kerja dengan mengakses jaringan internal secara *remote* melalui jaringan internet diperbolehkan namun sangat dibatasi hanya untuk personil yang diberi izin berdasarkan kebutuhan pekerjaannya.

6. Akses ke jaringan internal PD/Unit Kerja dari jaringan internet harus menggunakan koneksi aman dengan menggunakan antara lain teknologi VPN.
7. Kebijakan terkait teknologi *teleworking* sebagai sarana pegawai bekerja pada lokasi di luar PD/Unit Kerja dengan mengakses jaringan internal PD/Unit Kerja. Teknologi ini diperbolehkan untuk digunakan dalam kondisi sebagai berikut :
 - a. perangkat akses (misalnya computer, *notebook*) yang digunakan untuk *teleworking* harus terinstalasi *firewall* dan antivirus;
 - b. mekanisme akses terhadap sistem atau aplikasi disesuaikan dengan klasifikasi aset informasi:
 - 1) informasi publik : dapat diakses langsung.
 - 2) informasi rahasia :
 - harus menggunakan protokol HTTPS atau SSH; dan
 - harus menggunakan VPN, sebelum kemudian mengakses melalui protokol HTTPS atau SSH.

BAB V

KEAMANAN SUMBER DAYA MANUSIA

A. Tujuan

Kebijakan keamanan Sumber Daya Manusia ditetapkan untuk memberikan pedoman dalam mengelola keamanan Sumber Daya Manusia dalam ruang lingkup SMKI di Pemerintah Daerah Provinsi Nusa Tenggara Timur.

B. Kebijakan

1. Calon pegawai di lingkungan Pemerintah Daerah Provinsi Nusa Tenggara Timur dan pegawai dari pihak eksternal, harus melalui proses *screening* untuk memastikan kesesuaian mereka dengan tugas dan tanggung jawab yang akan mereka dapatkan.
2. Proses *screening* perlu mencakup verifikasi terhadap latar belakang kandidat sesuai dengan peraturan perundang-undangan serta etika yang ada.
3. Pegawai dalam lingkungan Pemerintah Provinsi Nusa Tenggara Timur dan pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Provinsi Nusa Tenggara Timur harus menandatangani perjanjian kerahasiaan (*non-disclosure agreement*) dengan memperhatikan tingkat sensitivitas dari aset yang diakses.

4. Setiap pegawai internal maupun eksternal harus mematuhi seluruh kebijakan dan prosedur PD/Unit Kerja terkait keamanan informasi.
5. Setiap pegawai internal maupun eksternal harus diberikan informasi yang memadai tentang tugas dan tanggung jawab terkait keamanan informasi yang mereka miliki.
6. Program peningkatan kesadaran keamanan informasi (*awareness*) secara berkelanjutan untuk menjaga dan meningkatkan kesadaran keamanan informasi dari pegawai harus dilaksanakan.
7. Setiap pelanggaran terhadap kebijakan dan prosedur terkait keamanan informasi harus ditindaklanjuti dan apabila diperlukan, tindakan pendisiplinan harus diambil sesuai dengan peraturan yang berlaku.
8. Tanggung jawab dan kewajiban terkait keamanan informasi yang tetap berlaku setelah pemberhentian atau perubahan status kepegawaian harus didefinisikan, dikomunikasikan dan ditegakkan kepada pegawai internal maupun eksternal.
9. Hal ini mencakup tanggung jawab keamanan informasi yang tercakup dalam perjanjian kerja seperti:
 - a. seluruh aset organisasi harus dikembalikan setelah pemberhentian kepegawaian;
 - b. seluruh hak akses organisasi harus dinonaktifkan atau dihapus setelah pemberhentian kepegawaian; dan
 - c. seluruh hak akses organisasi harus disesuaikan setelah perubahan status kepegawaian.

BAB VI

PENGELOLAAN ASET

A. Tujuan

Pengelolaan aset informasi bertujuan untuk memberikan pedoman dalam mengelola aset yang terkait informasi serta fasilitas fisik pengolahan informasi, sehingga aset informasi mendapatkan perlindungan yang sesuai dengan tingkat kepentingannya.

B. Kebijakan

1. Kepala Dinas Komunikasi dan Informatika Provinsi Nusa Tenggara Timur menetapkan pemilik aset informasi di setiap PD/Unit Kerja, beserta perangkat fisik pengolah informasi yang terkait.



2. Pemilik aset informasi memiliki tanggung jawab untuk:
 - a. mengidentifikasi seluruh aset informasi dan fasilitas pengolahan dan penyimpanan informasi;
 - b. mendokumentasikannya dalam daftar inventaris aset SMKI, serta senantiasa memperbaharui daftar inventaris aset SMKI tersebut sesuai kondisi terkini; dan
 - c. memastikan bahwa setiap aset telah diklasifikasikan dan dilindungi secara memadai.
3. Aset pengolahan dan penyimpanan informasi yang diinventaris adalah aset dalam bentuk:
 - a. perangkat keras, meliputi perangkat keras yang digunakan untuk mengolah dan menyimpan informasi dalam bentuk fisik maupun elektronik, yang mencakup namun tidak terbatas pada komputer, *notebook*, *server*, *harddisk drive*, *USB disk*;
 - b. perangkat lunak, meliputi perangkat lunak yang digunakan untuk mengolah informasi dalam bentuk elektronik, yang mencakup namun tidak terbatas pada sistem operasi, aplikasi, dan *database*;
 - c. perangkat jaringan, meliputi perangkat keras dan lunak yang digunakan untuk membentuk dan infrastruktur jaringan telekomunikasi, yang mencakup namun tidak terbatas pada *hub*, *switch*, *router*, *firewall*, *IDS*, *IPS*, dan *network monitoring tools*;
 - d. perangkat pendukung meliputi perangkat yang digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada *genset*, *UPS*, *AC*, *rak server*, lemari penyimpanan informasi dan *CCTV*;
 - e. layanan, meliputi layanan yang digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada layanan jaringan komunikasi, layanan *hosting* dan *co-location*, layanan pemeliharaan perangkat dan sistem, dan layanan pemasangan infrastruktur; dan
 - f. sumber daya manusia meliputi personil baik internal maupun eksternal yang terlibat dalam pengolahan dan penyimpanan informasi.
4. Pemilik aset dapat mendelegasikan tugas pengamanan dan pemeliharaan aset kepada kustodian aset, namun tanggung jawab akhir terhadap aset tetap berada pada pemilik aset.
5. Aset pengolahan dan penyimpanan informasi harus secara berkala dipelihara dengan memadai.

6. Apabila dalam pemeliharaan aset pengolahan dan penyimpanan informasi tersebut harus menggunakan jasa pihak ketiga/penyedia, maka:
 - a. kontrak pemeliharaan perlu dibuat dengan pihak ketiga penyedia jasa yang kompeten dan relevan; dan
 - b. peralatan yang dibawa keluar untuk pemeliharaan harus diperiksa untuk mencegah kebocoran informasi.
7. Dalam proses penghapusan aset harus dilakukan secara aman dengan metode yang dapat mencegah kebocoran informasi seperti menghancurkan secara fisik harddiskdrive.
8. Semua aset informasi serta pengolahan dan penyimpanan informasi milik Pemerintah Daerah Provinsi Nusa Tenggara Timur harus dikembalikan setelah personil pengguna tidak memiliki hubungan kepegawaian lagi dengan Pemerintah Daerah Provinsi Nusa Tenggara Timur, misalnya karena pengunduran diri dan pensiun.
9. Ketentuan dalam proses pengembalian aset tersebut mencakup:
 - a. pengembalian aset harus terdokumentasi secara formal;
 - b. untuk pengembalian aset yang disebabkan oleh terhentinya status kepegawaian, informasi yang tersimpan dalam aset harus di-backup dan informasi yang tersimpan dalam aset harus dihapus secara aman, antara lain dengan secureformat atau melakukan instalasi ulang sistem operasi secara menyeluruh; dan
 - c. media penyimpanan backup informasi harus diamankan secara fisik, antara lain dengan menyimpan dalam lemari terkunci dengan akses yang terbatas.
10. Aset pengolahan informasi, seperti komputer dan laptop yang akan digunakan kembali baik oleh pihak internal maupun eksternal harus diperiksa untuk menjamin tidak ada informasi sensitif yang tersimpan dalam aset tersebut.
11. PD/Unit Kerja harus mendefinisikan klasifikasi aset informasi dengan mempertimbangkan hal-hal sebagai berikut:
 - a. aset informasi diklasifikasikan berdasarkan tingkat sensitivitas informasi serta tingkat kritikalitas sistem, yang meliputi:
 - 1) klasifikasi aset informasi secara berkala; dan
 - 2) pengguna yang diijinkan mengakses aset informasi.
 - b. pemberian label klasifikasi informasi harus dilakukan secara konsisten terhadap seluruh aset informasi;

- c. klasifikasi aset informasi dan seberapa tingkat kerahasiaan aset informasi, didefinisikan sesuai ketentuan peraturan perundang-undangan, diuraikan sesuai tabel berikut:

Klasifikasi Aset Informasi	Deskripsi
Rahasia (Confidential)	Aset informasi yang sangat peka dan berisiko tinggi yang pembocoran atau penyalahgunaan akses terhadapnya bisa mengganggu kelancaran operasional secara temporer atau mengganggu citra dan reputasi instansi.
Internal (Internal Use Only)	Informasi yang telah terdistribusi secara luas di lingkungan internal instansi/lembaga yang penyebarannya secara internal tidak lagi memerlukan izin dari pemilik informasi dan risiko penyebarannya tidak menimbulkan kerugian signifikan.
Publik	Aset informasi yang secara sengaja dipublikasikan secara luas, merupakan informasi yang wajib disediakan dan diumumkan secara berkala, informasi yang wajib diumumkan secara serta-merta, dan informasi yang wajib tersedia setiap saat.

7. Untuk kepentingan penyelenggaraan pengelolaan aset informasi dalam kebijakan Sistem Manajemen Keamanan Informasi perlu diberikan penjelasan contoh-contoh aset informasi rahasia dan internal, yang antara lain:

Klasifikasi Aset Informasi	Contoh
Rahasia (Confidential)	User ID, password, Personal Identification Number (PIN), Log sistem, hasil penetration test, data konfigurasi sistem, Internet Protocol Address (IP Address)
Internal (Internal Use Only)	Panduan penggunaan sistem dan aplikasi, kebijakan dan prosedur SMKI, dokumen Business Continuity Plan.

13. Setiap pemilik informasi harus memperhatikan keamanan informasi yang tersimpan dalam media penyimpanan informasi antara lain:

- a. dalam hal data yang tersimpan di dalam media bersifat rahasia, perlu diberikan proteksi kata sandi untuk melindungi data;
- b. dalam hal tidak lagi dibutuhkan atau digunakan, seluruh data yang tersimpan di dalam media harus sepenuhnya dihapus sehingga tidak lagi dapat dipulihkan;
- c. data yang tersimpan di dalam media yang akan dibuang harus mendapatkan perlakuan khusus guna meminimalkan terjadinya kebocoran informasi kepada pihak yang tidak sah, yaitu:
 - 1) data yang tersimpan di dalam media yang memuat informasi rahasia harus dibuang dengan cara dihancurkan atau dibakar; dan
 - 2) data yang tersimpan di dalam media yang memuat informasi lainnya harus dilakukan penghapusan total dengan cara-cara tertentu yang tidak lagi dapat dipulihkan.

14. Panduan terkait pelabelan dan penanganan aset informasi berdasarkan klasifikasi aset informasi adalah sebagai berikut:

Klasifikasi Tipe	Publik	Internal	Rahasia
Dokumen dan catatan (<i>record</i>) dalam bentuk non elektronik (<i>hardcopy</i>).	Tidak diperlukan penanganan khusus.	Diberi label " Internal ".	Diberi label " Rahasia ".
Map penyimpanan dokumen.	Tidak diperlukan penanganan khusus.	Tidak diperlukan penanganan khusus.	Diberi label " Rahasia ".
Amplop pengiriman surat internal (di dalam kantor).	Tidak diperlukan penanganan khusus.	Tidak diperlukan penanganan khusus.	Amplop diberi label " Rahasia ".
Amplop untuk surat eksternal (ke luar kantor).	Tidak diperlukan penanganan khusus.	Pada amplop ditandai " Internal ".	• Menggunakan 2 amplop, dimana amplop pertama dimasukkan kedalam amplop kedua;

			• Pada amplop pertama ditandai "Rahasia", dan pada amplop kedua tidak diberikan tanda apapun.
Dokumen dan catatan (<i>record</i>) dalam bentuk elektronik (<i>softcopy</i>).	Tidak diperlukan penanganan khusus.	Memberikan label "Internal" pada bagian awal dari nama <i>file</i> atau pada bagian tertentu dari <i>file properties</i> .	Memberikan label "Rahasia" pada bagian awal dari nama <i>file</i> atau pada bagian tertentu dari <i>file properties</i> .
Publikasi / Distribusi	Tidak ada pembatasan.	• Tersedia untuk personil internal PD/Unit Kerja pemilik informasi. • Distribusi kepada pihak eksternal dibatasi berdasarkan kebutuhan pekerjaan maupun operasional di lingkungan Pemda Provinsi Nusa Tenggara Timur. • Distribusi kepada pihak eksternal perlu seijin pemilik informasi.	• Tersedia untuk personil internal PD/Unit Kerja pemilik informasi. • Distribusi kepada pihak eksternal dibatasi berdasarkan kebutuhan pekerjaan maupun operasional di lingkungan Pemda Provinsi Nusa Tenggara Timur. • Distribusi kepada pihak eksternal perlu seijin pemilik informasi. • Sensitifitas dan kritikalitas informasi perlu diberitahukan kepada pihak eksternal. • Pihak ketiga harus disertai perjanjian kerahasiaan (<i>NDA - non disclosure agreement</i>).

		• Sensitifitas dan kritikalitas informasi perlu diberitahukan kepada pihak eksternal.	
Pencetakan informasi	Tidak ada pembatasan.	Dibatasi hanya untuk kebutuhan internal.	• Pencetakan hanya pada <i>printer</i> organisasi dan diusahakan tidak mencetak menggunakan jasa pencetakan eksternal.
Surat menyurat internal (di dalam kantor)	Pastikan nama dan alamat tujuan sudah benar.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat internal.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat internal. • Menginformasikan kepada penerima akan pengiriman informasi tersebut. • Mengkonfirmasi kepada penerima bahwa informasi yang dikirim sudah diterima.

Surat menyurat eksternal (ke luar kantor)	Pastikan nama dan alamat tujuan sudah benar.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat eksternal. • Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat eksternal. • Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman. • Menginformasikan kepada penerima akan pengiriman informasi tersebut. • Mengkonfirmasi kepada penerima bahwa informasi yang dikirim sudah diterima.
Pengiriman ke pihak internal melalui <i>email</i>	• Pengiriman e-mail harus menggunakan <i>account</i> e-mail PD/Unit Kerja • Tidak diperlukan penanganan khusus.	• Pengiriman e-mail harus menggunakan <i>account</i> e-mail PD/Unit Kerja • Pastikan alamat email tujuan sudah benar. • Pengiriman informasi, termasuk forwarding / meneruskan email hanya boleh dilakukan oleh pemilik informasi.	• Pengiriman e-mail harus menggunakan <i>account</i> e-mail PD/Unit Kerja • Memberi <i>password</i> pada informasi yang dikirim melalui email dan <i>password</i> diinformasikan kepada penerima secara terpisah • Tidak mencantumkan informasi rahasia di <i>body text</i> e-mail

			• Pengiriman informasi, termasuk <i>forwarding</i> / meneruskan <i>email</i> hanya boleh dilakukan oleh pemilik informasi.
Pengiriman ke pihak eksternal melalui <i>email</i>	• Pengiriman e-mail harus menggunakan <i>account</i> e-mail PD/Unit Kerja • Tidak diperlukan penanganan khusus.	• Pengiriman e-mail harus menggunakan <i>account</i> e-mail PD/Unit Kerja • Pastikan alamat email tujuan sudah benar.	• Tidak disarankan menggunakan e-mail untuk mengirim informasi dengan klasifikasi ini. • Pengiriman e-mail harus menggunakan <i>account</i> e-mail PD/Unit Kerja • Pastikan alamat email tujuan sudah benar. • Memberi <i>password</i> pada informasi yang dikirim melalui email dan <i>password</i> diinformasikan kepada penerima secara terpisah
Penyimpanan informasi <i>hardcopy</i>	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Disimpan secara aman dalam tempat penyimpanan yang terkunci.
Penyimpanan informasi <i>softcopy</i>	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	• Penyimpanan pada komputer atau media penyimpanan harus yang menggunakan <i>password</i>. • <i>File</i> yang disimpan harus diberi <i>password</i>.

			Media penyimpanan eksternal (<i>external harddisk</i>, atau <i>flashdisk</i>) harus disimpan pada tempat penyimpanan yang terkunci.
Penyimpanan pada pihak ketiga	Tidak diperlukan penanganan khusus	Harus disertai dengan perjanjian kerahasiaan (<i>non disclosure agreement</i> - NDA).	Harus disertai dengan perjanjian kerahasiaan (<i>non disclosure agreement</i> - NDA).
Penghancuran (<i>disposal</i>)	- Tidak diperlukan penanganan khusus. - Masih dapat digunakan kembali sebagai kertas untuk pekerjaan (<i>scrap paper</i>).	- Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi. - Masih dapat digunakan kembali untuk kebutuhan mencetak informasi dengan klasifikasi yang sama.	- Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi - Dihancurkan dengan metode pemusnahan dan informasi tidak dapat diakses kembali (<i>dihancurkan secara fisik atau secure format</i>).
Pengamanan pada komputer penyimpan informasi	Tidak diperlukan penanganan khusus.	<i>Screen saverlock</i> harus aktif jika meninggalkan komputer / terminal.	<i>Screen saverlock</i> harus aktif jika meninggalkan komputer / terminal.

		• <i>Sign-off</i> komputer / terminal jika tidak digunakan atau pulang kerja.	• <i>Sign-off</i> komputer / terminal jika tidak digunakan atau pulang kerja. • <i>File perlu</i> dienkripsi / <i>password</i>.
Kehilangan atau kebocoran informasi	Tidak diperlukan penanganan khusus.	Harus dilaporkan kepada pemilik informasi	Harus dilaporkan kepada pemilik informasi dan unit kerja pengelola insiden keamanan informasi di lingkungan Pemerintah Daerah Provinsi Nusa Tenggara Timur.

15. informasi yang dianggap kritikal oleh PD/Unit Kerja harus di-*backup* secara memadai untuk menjamin ketersediaannya.
16. hal yang perlu dipertimbangkan dalam proses *backup* informasi meliputi:
 - a. pemilik informasi bertanggung jawab untuk menentukan informasi yang membutuhkan *backup*, frekuensi dan metode *backup* serta waktu retensi untuk setiap *backup* informasi yang ada;
 - b. pernyataan formal terkait informasi yang dibutuhkan untuk di-*backup* beserta metode dan frekuensi dari *backup* harus ditentukan bersama dengan personil yang bertugas melaksanakan proses *backup* serta harus dinyatakan secara jelas dalam sebuah rencana *backup* resmi;
 - c. *backup* informasi harus disimpan sesuai dengan masa retensi dari informasi utama;
 - d. masa retensi harus dinyatakan secara jelas dalam rencana *backup*; dan
 - e. perlindungan terhadap *backup* informasi harus dilakukan berdasarkan klasifikasi dari informasi utama.

17. PD/Unit Kerja menyediakan akses *internet* dan *email* kepada pegawainya hanya untuk kebutuhan pekerjaan dan operasional Pemerintah Daerah Provinsi Nusa Tenggara Timur.
18. Ketentuan dalam penggunaan *internet* dan *email* adalah sebagai berikut:
 - a. pengguna dilarang menggunakan akses *internet* dan *email* PD/Unit Kerja untuk kegiatan melanggar hukum dan aktifitas yang dapat membahayakan keamanan jaringan Pemerintah Daerah Provinsi Nusa Tenggara Timur;
 - b. pengguna dilarang untuk menggunakan akses *internet* dan *email* PD/Unit Kerja untuk mengakses, mendistribusikan, mengunggah dan/atau mengunduh:
 - 1) materi pornografi;
 - 2) materi bajakan seperti, perangkat lunak, *file* musik dan *video/film*;
 - 3) materi yang melecehkan, mendiskriminasi, yang membakar emosi atau menimbulkan kebencian atau membuat pernyataan palsu atau yang bersifat merusak mengenai orang lain;
 - 4) situs yang dapat menimbulkan risiko serangan malware, penyusupan atau *hacking* ke jaringan Pemerintah Daerah Provinsi Nusa Tenggara Timur.
19. pengguna disarankan untuk tidak membagi informasi pribadi melalui situs *internet* atau media sosial.
20. pengguna dilarang untuk mendistribusikan informasi Pemerintah Daerah Provinsi Nusa Tenggara Timur yang bersifat rahasia tanpa izin dari pemilik informasi.
21. pesan penyangkalan ini harus dituliskan pada akhir setiap e-mail.
"Pesan ini mungkin berisi informasi rahasia dan hanya ditujukan kepada pihak yang dituju. Apabila anda bukanlah pihak yang dituju, anda dilarang untuk mengungkapkan, menyebarkan atau menyalin isi email ini. Apabila anda mendapatkan email ini tanpa sengaja mohon segera hubungi pengirim email dan hapus email ini segera. Pemerintah Daerah Provinsi Nusa Tenggara Timur tidak bertanggung jawab untuk pengiriman informasi ini secara lengkap dan tepat dan juga tidak bertanggung jawab untuk keterlambatan dalam pengiriman email ini."
22. unit kerja yang mengelola akun *email* PD berhak untuk mem-block akun *email* Pemerintah Daerah Provinsi Nusa Tenggara Timur pada saat terdapat bukti memadai terkait penyalahgunaan dan/atau pelanggaran keamanan.

BAB VII

PENGENDALIAN AKSES

A. Tujuan

Tujuan dari pengendalian akses adalah untuk:

1. membatasi akses terhadap informasi serta fasilitas fisik (data center);
2. memastikan sistem dan aplikasi diakses oleh pengguna yang telah diotorisasi, serta mencegah akses oleh yang tidak berhak; dan
3. memastikan pengguna bertanggung jawab untuk melindungi informasi otentikasi sensitif masing-masing.

B. Kebijakan

1. Persyaratan pengendalian akses pada suatu sistem meliputi:
 - a. akses ke aset informasi serta aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah Provinsi Nusa Tenggara Timur harus dikendalikan menggunakan metode pengendalian akses yang memadai;
 - b. pemberian hak akses dikelola secara formal pada seluruh siklusnya, mulai dari proses pengajuan, persetujuan serta pencabutan, serta dilaksanakan oleh para pihak terkait sesuai jenjang kewenangannya;
 - c. pengguna yang mengakses sistem informasi dalam lingkungan Pemerintah Daerah Provinsi Nusa Tenggara Timur diharuskan untuk mengotentikasi dirinya dengan menggunakan kombinasi *user ID* dan informasi otentikasi pribadi seperti *password* atau PIN;
 - d. pengembangan aturan pemberian akses perlu mempertimbangkan:
 - 1) klasifikasi dari informasi;
 - 2) kritikalitas dari aset yang digunakan untuk mendukung operasional bisnis;
 - 3) prasyarat hukum perundang-undangan, kontraktual serta keamanan yang relevan;
 - 4) didasarkan atas prinsip *need to know* dan *need to use*, yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional dalam lingkungan Pemerintah Daerah Provinsi Nusa Tenggara Timur;
 - e. aturan pemberian akses harus dikembangkan dan didokumentasikan oleh setiap pemilik system dalam bentuk daftar atau matriks akses;

- f. peninjauan terhadap aturan pemberian akses harus dilakukan oleh pemilik aset/sistem secara berkala tergantung tingkat kritikalitas sistem tersebut;
 - g. peninjauan terhadap hak akses pengguna harus didokumentasikan secara formal; dan
 - h. setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan cara menyesuaikan atau mencabut hak akses yang menyimpang.
2. pengendalian akses jaringan di lingkungan PD/Unit Kerja meliputi:
- a. penggunaan layanan jaringan (*network services*) hanya diperbolehkan secara terbatas, sesuai kebutuhan ketugasan dan kepentingan PD/Unit Kerja, layanan lainnya yang tidak diperlukan harus dinonaktifkan;
 - b. jaringan komunikasi dalam lingkungan PD/Unit Kerja harus dipisahkan kedalam *domain* jaringan yang terpisah sesuai dengan kebutuhan bisnis dan operasional, dalam rangka untuk mengamankan jaringan internal PD dan aset di jaringan tersebut;
 - c. akses secara *remote* ke jaringan internal PD/Unit Kerja dari jaringan publik harus sangat dibatasi baik dari perangkat yang digunakan maupun waktu untuk kebutuhan *troubleshooting* dan harus dilakukan melalui *secure channel*, antara lain dengan menggunakan teknologi VPN; dan
 - d. pemberian akses pengguna terhadap jaringan, baik LAN maupun WAN, dilakukan melalui mekanisme formal.
3. pengelolaan akses terhadap pengguna di PD/Unit Kerja harus memenuhi ketentuan sebagai berikut:
- a. pemilik Aset Informasi harus memiliki manajemen identitas pengguna yang mencakup proses pendaftaran dan terminasi pengguna, yang didalamnya termasuk:
 - 1) identitas pengguna (*user account*) harus unik, melekat ke setiap individu tunggal, sehingga setiap tindakan pengguna dapat dipertanggungjawabkan;
 - 2) tidak diijinkan menggunakan satu identitas pengguna yang digunakan secara bersama-sama oleh lebih dari satu individu, kecuali untuk tujuan tertentu yang sebelumnya harus mendapatkan persetujuan dari pihak berwenang; dan
 - 3) memastikan secara berkala bahwa tidak ada identitas pengguna yang terduplikasi atau redundan sehingga seluruh identitas pengguna aktif adalah sesuai dengan pegawai PD/Unit Kerja aktif.

- b. pendaftaran, modifikasi dan pencabutan hak akses pengguna mencakup proses pembuatan *user ID*, memberikan hak akses kepada *user ID* serta mencabut hak akses dan *user ID*.
- c. pendaftaran, modifikasi dan pencabutan hak akses pengguna harus disetujui oleh atasan dari pengguna yang memohon hak akses tersebut dan pemilik informasi dan/atau sistem. Persetujuan tersebut harus diberikan sesuai dengan aturan pemberian akses.
- d. identitas pengguna harus diotorisasi secara formal oleh pejabat berwenang pada pemilik aset informasi. Akses atas sistem dan aplikasi hanya dapat diaktifkan jika proses otorisasi telah selesai.
- e. identitas pengguna pada sistem, seperti *user ID*, harus bersifat unik untuk memungkinkan mengidentifikasi dan meminta pertanggungjawaban pengguna.
- f. pemberian informasi otentikasi suatu pengguna yang bersifat rahasia harus dilakukan melalui proses formal yang mencakup:
 - 1) informasi otentikasi perdana yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama pada saat mengakses sistem atau aplikasi;
 - 2) informasi otentikasi bawaan (*default*) dari penyedia barang/jasa harus segera diganti pada saat instalasi sistem atau aplikasi;
- g. pemilik Aset harus melakukan tinjauan secara berkala atas seluruh hak akses pengguna secara berkala, dengan tambahan tinjauan insidental yang dilakukan pada saat:
 - 1) terjadinya proses kepegawaian, seperti promosi, mutasi, terminasi; dan
 - 2) terjadinya perubahan struktur organisasi.
- h. hak akses khusus (*privileged access rights*) dari sistem informasi dalam lingkungan PD/Unit Kerja, seperti *administrator*, *root*, hak akses untuk memodifikasi *database* atau hak akses untuk membuat, memodifikasi atau mencabut pengguna dalam sistem aplikasi, harus sangat dibatasi kepada personil yang terotorisasi.
- i. hak akses khusus harus disetujui dan didokumentasikan secara formal.
- j. alokasi dari hak akses khusus harus ditinjau secara berkala dan setiap terdapat perubahan dalam status penggunaan akses tersebut.
- k. setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan menyesuaikan atau menghapus hak akses khusus yang menyimpang.

- l. apabila memungkinkan, hak akses khusus harus dialokasikan secara individual dan tidak di-*share*. Hal ini dilakukan untuk menjamin akuntabilitas dari pengguna khusus.
 - m. apabila hak akses khusus tidak bisa dialokasikan secara individual, kontrol tambahan seperti *dual custody*, harus diimplementasikan untuk menghindari penyalahgunaan.
 - n. jejak audit (*log*) untuk hak akses khusus pada sistem informasi dalam lingkungan Pemerintah Daerah Provinsi Nusa Tenggara Timur harus diaktifkan.
4. Setiap pengguna harus mempunyai tanggung jawab dalam penggunaan *User ID* dan *password* yaitu:
- a. pengguna harus menjaga kerahasiaan dan keamanan *password* pribadi atau kelompok serta informasi otentikasi rahasia lainnya;
 - b. pengguna harus segera mengganti informasi otentikasi rahasia jika terindikasi bahwa informasi tersebut telah diketahui oleh orang lain;
 - c. *password* yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama pada saat mengakses sistem atau aplikasi;
 - d. *password* untuk mengakses sistem informasi dalam lingkungan PD harus memiliki karakteristik sebagai berikut:
 - 1) memiliki panjang minimum 8 karakter;
 - 2) mengandung kombinasi huruf besar, huruf kecil dan nomor;
 - 3) tidak terdiri dari kata atau nomor yang mudah ditebak seperti *password*, *admin*, 12345678 atau abc123; dan
 - 4) tidak terdiri dari informasi pribadi seperti ulang tahun pengguna, nama perusahaan atau nama pengguna;
 - e. *password* untuk mengakses sistem informasi dalam lingkungan Pemerintah Daerah Provinsi Nusa Tenggara Timur harus diganti paling sedikit setiap 3 (tiga) bulan sekali;
 - f. pada saat penggantian, *password* sebelumnya tidak boleh digunakan kembali sampai setelah 3 siklus pergantian *password*;
 - g. prosedur *login* dari sistem harus menjamin keamanan dari *password* dengan cara:
 - 1) tidak menampilkan *password* yang dimasukkan;
 - 2) tidak menyediakan pesan bantuan pada saat proses *login* yang dapat membantu pengguna yang tidak berwenang;
 - h. pengguna wajib menggunakan kata sandi yang berbeda untuk keperluan ketugasan dan pribadi.
5. pengendalian akses sistem dan aplikasi yang dikelola oleh PD/Unit Kerja meliputi:

- a. pemilik aset informasi harus memastikan bahwa sistem dan aplikasi dibawah pengelolaannya memiliki fasilitas manajemen hak akses pengguna, manajemen kata sandi yang baik, serta mekanisme otentikasi pengguna yang aman;
- b. fasilitas manajemen hak akses pengguna harus mampu membatasi akses informasi sesuai ketugasannya (*role based access control*);
- c. fasilitas manajemen kata sandi harus memastikan dihasilkannya kata sandi yang berkualitas, yaitu:
 - 1) menegakkan akuntabilitas pengguna melalui penggunaan identitas pengguna tunggal untuk setiap individu;
 - 2) memberikan fasilitas penggantian kata sandi mandiri;
 - 3) membantu memberikan rekomendasi kata sandi yang berkualitas;
 - 4) mewajibkan pengguna untuk mengganti kata sandi pada saat pertama kali login;
 - 5) mewajibkan pengguna untuk mengganti kata sandi secara berkala;
 - 6) menyimpan riwayat kata sandi pengguna dan mencegah agar pengguna tidak menggunakan kata sandi yang sebelumnya telah digunakan;
 - 7) tidak menampilkan kata sandi saat sedang dientrikan; dan
 - 8) kata sandi disimpan dalam bentuk terlindungi (*dienkripsi*), demikian juga pada saat kata sandi ditransmisikan.
- d. mekanisme otentikasi pengguna perlu dirancang agar meminimalkan peluang terjadinya akses yang tidak sah, yaitu:
 - 1) kata sandi tidak ditransmisikan melalui jaringan secara *plaintext*;
 - 2) memiliki mekanisme penguncian sistem sementara sebagai perlindungan terhadap *brute force attacks*;
 - 3) adanya pencatatan terhadap seluruh upaya otentikasi yang sukses dan gagal;
 - 4) adanya pembatasan jumlah akses pengguna yang sama secara simultan;
- e. parameter otentikasi pengguna disesuaikan dengan klasifikasi aset informasi sebagai berikut:

Parameter Otentikasi	Rahasia dan Internal	Publik
Jumlah gagal login sebelum penguncian	3	10
Durasi <i>timeout</i> sebelum terminasi sesi otomatis	5 menit	16 menit

6. penggunaan program *utility khusus* dalam operasional sistem di lingkungan PD/Unit Kerja harus mempertimbangkan keamanan sebagai berikut yaitu penggunaan program *utility khusus* seperti *registry cleaner* atau *system monitoring* yang dapat mengambil alih kendali sistem/aplikasi atau mendapatkan hak akses khusus pada sistem/aplikasi harus sangat dibatasi berdasarkan kebutuhan operasional pengguna.
7. PD/Unit Kerja yang mengelola aplikasi harus memastikan bahwa *source code* dikelola dan disimpan secara memadai baik yang dikembangkan oleh internal PD/Unit Kerja maupun yang dikembangkan oleh penyedia jasa aplikasi.
8. Apabila *source code* dari penyedia jasa aplikasi tidak dapat diserahkan kepada pengelola aplikasi, PD/Unit Kerja bersama penyedia jasa aplikasi tersebut harus mempertimbangkan *escrow agreement* untuk memastikan kelangsungan operasional sistem aplikasi jika ada pengembangan selanjutnya.
9. Pengendalian terhadap akses ke *source code* aplikasi sebagai berikut:
 - a. Untuk sistem aplikasi yang dikembangkan secara internal dan/atau dibeli dengan *source code*, pengendalian akses harus diimplementasikan untuk mencegah akses tanpa izin ke *source code* tersebut.
 - b. Pengendalian tersebut mencakup:
 - 1) tidak menyimpan *source code* pada sistem operasional;
 - 2) menyimpan *source code* pada lokasi fisik yang aman dari ancaman akses tanpa izin maupun ancaman kerusakan karena kondisi lingkungan;
 - 3) membatasi akses secara fisik maupun logical ke *source code* program hanya kepada pengembang dan personil yang berwenang;
 - 4) mengimplementasikan metode *versioning* dan proses manajemen perubahan untuk menjamin integritas dari *source code* aplikasi.

BAB VIII

KRIPTOGRAFI

A. Tujuan

Tujuan dari kebijakan terkait teknologi kriptografi adalah untuk memastikan penggunaan teknologi kriptografi yang sesuai dan efektif untuk melindungi kerahasiaan, keaslian dan/atau integritas dari informasi dalam lingkungan Pemerintah Daerah Daerah Istimewa Yogyakarta.

B. Kebijakan

1. Kontrol kriptografi dapat digunakan untuk menjamin kerahasiaan dan integritas dari informasi sensitif di lingkungan PD.
2. Kontrol kriptografi dapat mencakup namun tidak terbatas pada:
 - a. enkripsi informasi dan jaringan komunikasi;
 - b. pemeriksaan integritas informasi, seperti hashing;
 - c. otentikasi identitas;
 - d. digital *signatures*;
3. implementasi dari kontrol kriptografi harus mempertimbangkan klasifikasi dari informasi yang akan diamankan.
4. pemilihan kontrol kriptografi harus mempertimbangkan:
 - a. jenis dari kontrol kriptografi;
 - b. kekuatan dari algoritma kriptografi; dan
 - c. panjang dari kunci kriptografi.
5. implementasi dari kontrol kriptografi harus secara berkala ditinjau untuk memastikan kecukupan dan kesesuaian dari kontrol tersebut dalam mengamankan kerahasiaan dan integritas dari informasi.
6. pengelolaan dari kunci kriptografi harus dikendalikan secara ketat dan dibatasi hanya pada personil yang terotorisasi.
7. pengelolaan dari kunci kriptografi didasarkan pada prinsip *dual custody* untuk mengurangi risiko penyalahgunaan.

BAB IX

KEAMANAN FISIK DAN LINGKUNGAN

A. Tujuan

Tujuan dari kebijakan keamanan fisik dan lingkungan adalah untuk:

1. Mencegah akses atas aset informasi dan aset pengolahan dan penyimpanan informasi secara fisik oleh pihak yang tidak berwenang pada lingkungan Pemerintah Daerah Provinsi Nusa Tenggara Timur; dan
2. Mencegah terjadinya kerusakan atau gangguan pada aset informasi dan aset pengolahan dan penyimpanan informasi pada lingkungan Pemerintah Daerah Provinsi Nusa Tenggara Timur karena ancaman dari kondisi lingkungan.

B. Kebijakan

1. Setiap area yang didalamnya terdapat informasi dan fasilitas pengolahan informasi PD/Unit Kerja harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut.
2. Setiap area harus merupakan akses terbatas, dimana akses masuk hanya diberikan bagi personil yang telah mendapatkan otorisasi. Mekanisme pembatasan ini dapat dilakukan aturan penerimaan tamu yang diterapkan berdasarkan kritikalitas area tersebut.
3. Untuk area *Data center*, *disaster recovery center* dan ruang arsip PD/Unit Kerja harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut dengan kriteria:
 - a. konstruksi dinding, atap dan lantai yang kuat;
 - b. pintu akses menuju area harus dilengkapi dengan mekanisme kontrol akses, seperti: *access door lock*;
 - c. pintu dan jendela harus senantiasa dalam kondisi terkunci, khususnya pada saat tanpa penjagaan;
 - d. perangkat CCTV perlu terpasang pada sisi eksterior dan interior area;
 - e. tidak diperbolehkan menyimpan bahan-bahan berbahaya yang mudah terbakar;
 - f. area bongkar muat atau penerimaan barang harus diamankan dan dipantau untuk mencegah akses tanpa izin ke *data center*, *disaster recovery center* dan ruang arsip Pemerintah Daerah Provinsi Nusa Tenggara Timur; dan

- g. *delivery* dari barang harus dilaporkan dan diperiksa sebelum barang tersebut dapat dipindahkan dari area bongkar muat atau penerimaan barang ke *data center*, *disaster recovery center* dan ruang arsip Pemerintah Daerah Provinsi Nusa Tenggara Timur.
4. Pengendalian akses pengunjung ke dalam area di lingkungan PD/Unit Kerja harus memperhatikan keamanan fisik yang meliputi:
- a. kunjungan ke dalam area tersebut harus disetujui secara formal oleh pengelola area tersebut;
 - b. selama kunjungan di dalam area tersebut, pengunjung harus senantiasa didampingi oleh petugas yang telah mendapatkan otorisasi;
 - c. kartu identitas pengunjung perlu diverifikasi, disimpan oleh petugas selama kunjungan, dan dikembalikan sesudah selesai kunjungan; dan
 - d. setiap kunjungan ke dalam area harus tercatat, mencakup jam masuk dan keluar, serta selalu dimonitor kesesuaiannya dengan rekaman CCTV.
5. PD/Unit Kerja harus memperhatikan aspek pengamanan terhadap perangkat yang digunakan melalui:
- a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya pencurian, akses oleh pihak yang tidak berwenang, kebakaran, air, debu, dan sebagainya;
 - b. seluruh perangkat di dalam area harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang berwenang untuk menjamin keberlangsungan efektivitas fungsionalnya;
 - c. pemeliharaan yang dilakukan oleh pihak ketiga, harus dilaksanakan sesuai dengan kesepakatan tingkat layanan (*service level agreement/SLA*) yang menjabarkan tingkat pemeliharaan dan kinerja yang harus dipenuhi pihak ketiga;
 - d. bagi pemeliharaan yang tidak dapat dilakukan di lokasi kantor PD/Unit Kerja, maka informasi rahasia dan kritikal yang tersimpan dalam peralatan tersebut harus dipindahkan terlebih dahulu;
 - e. pemeliharaan perangkat yang mengharuskan dibawa dari luar area harus atas persetujuan pejabat berwenang.
 - f. peralatan pengolahan dan penyimpanan informasi yang tidak digunakan lagi oleh Pemerintah Daerah Daerah Istimewa Yogyakarta, baik karena rusak, diganti, atau karena sebab lainnya harus dipastikan tidak lagi menyimpan informasi sensitif dan kritikal; dan
- 

g. media penyimpan informasi yang sudah tidak digunakan lagi harus dihancurkan, atau dihapus isinya agar tidak bisa dibaca dan digunakan lagi oleh pihak yang tidak berwenang.

6. Khusus pengamanan area fisik di *data center* harus mempertimbangkan hal-hal sebagai berikut:

- a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya kebakaran, kebocoran, debu, dan sebagainya;
- b. seluruh perangkat di dalam *data center* harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang kompeten dan berwenang sesuai dengan rekomendasi dari pembuat perangkat tersebut;
- c. *data center* harus dilengkapi dengan ups, generator listrik cadangan, perangkat pemadam kebakaran, dan diusahakan terdapat perlindungan kejut listrik (petir, tegangan tidak stabil);
- d. *data center* dan *disaster recovery center* dilengkapi dengan sistem sensor deteksi asap, air, suhu dan kelembaban, yang dapat terpantau;
- e. parameter temperatur dan kelembaban berikut perlu dijaga untuk *data center* meliputi:
 - 1) temperatur antara 18° - 26° celcius;
 - 2) kelembaban (rh) antara 40% - 60%.
- f. kabel listrik dan jaringan telekomunikasi yang membawa data atau mendukung layanan sistem informasi harus dilindungi dari penyambungan yang tidak sah (penyadapan) atau kerusakan.

BAB X

KEAMANAN OPERASIONAL SISTEM INFORMASI

A. Tujuan

Tujuan dari kebijakan keamanan operasional sistem informasi adalah untuk:

1. Memastikan pengoperasian aset pengolahan dan penyimpanan informasi di Pemerintah Daerah Provinsi Nusa Tenggara Timur secara benar dan aman;
2. Memastikan terlindunginya aset informasi beserta aset pengolahan dan penyimpanan informasi di Pemerintah Daerah Provinsi Nusa Tenggara Timur dari ancaman *malware*;
3. melindungi terjadinya kehilangan atas aset informasi;
4. tersedianya catatan (*log*) atas aktivitas sistem informasi sebagai barang bukti; dan
5. mencegah terjadinya eksploitasi atas kelemahan sistem informasi pada Pemerintah Daerah Provinsi Nusa Tenggara Timur.

B. Kebijakan

1. Aktivitas operasional terkait fasilitas pengolahan informasi serta fasilitas komunikasi harus memiliki prosedur yang terdokumentasi dengan baik;
2. Prosedur operasional tersebut harus tersedia bagi pengguna yang memerlukannya;
3. Seluruh perubahan pada fasilitas pengolahan informasi yang dapat berimplikasi pada keamanan informasi, perlu diperlakukan secara terkendali, mencakup antara lain:
 - a. menyusun perencanaan mengenai perubahan yang mungkin terjadi serta melakukan pengujian terkait terpenuhinya persyaratan keamanan;
 - b. melakukan kajian atas implikasi keamanan informasi yang mungkin terjadi;
 - c. mengajukan persetujuan secara formal atas perubahan yang akan dilakukan; dan
 - d. mencatat seluruh perubahan yang telah dilakukan.
4. Kinerja dan utilisasi atas fasilitas pengolahan informasi harus senantiasa dipantau dengan alat bantu peringatan dini, dioptimalkan pemanfaatannya, serta diproyeksikan kebutuhan kapasitasnya untuk masa yang akan datang.

5. Untuk mengurangi risiko perubahan tanpa izin atau penyalahgunaan hak akses, pemisahan fasilitas pengembangan, pengujian, dan operasional harus dilakukan.
6. Setiap sistem informasi di lingkungan PD/Unit Kerja harus terlindungi dari *malware* secara memadai melalui:
 - a. instalasi dari perangkat lunak *antivirus* pada sistem informasi;
 - b. mem-*block* akses ke *website* yang dapat menimbulkan ancaman kepada sistem informasi;
 - c. program peningkatan kesadaran bagi personil organisasi untuk menangani ancaman *malware*; dan
 - d. setiap insiden terkait dengan *malware* harus dilaporkan kepada *administrator* sistem dan dikategorikan sebagai insiden keamanan informasi.
7. Seluruh aset informasi yang berada di dalam fasilitas pengolahan informasi wajib dilakukan *backup*, dengan persyaratan berikut:
 - a. backup mencakup aplikasi, database, dan *system image*;
 - b. frekuensi *backup* dilakukan secara harian, bulanan, dan tahunan;
 - c. salinan *backup* harus disimpan secara aman sesuai dengan periode retensi. periode retensi *backup* adalah 1 tahun, dimana:
 - 1) *backup* harian disimpan selama 31 hari;
 - 2) *backup* bulanan disimpan selama 12 bulan;
 - d. seluruh hasil *backup* harus dilakukan uji *restore* secara berkala;
 - e. media *backup* disimpan pada perangkat *storage* yang terpisah dari perangkat pengolahan informasi utama;
 - f. *backup* merupakan tanggung jawab pengelola data center, sedangkan pengujian *restore* merupakan tanggung jawab pemilik aset informasi;
 - g. parameter *backup* disesuaikan dengan klasifikasi sistem sebagai berikut:

Parameter Backup	Klasifikasi Sistem	
	Vital	Sensitive/Non Sensitive
Cakupan backup	Aplikasi, Database	Aplikasi, Database
Frekuensi backup (recovery point objective)	Harian	Bulanan
Pengujian restore	Triwulanan	Semesteran

8. Sistem harus dikonfigurasi untuk melakukan pencatatan (*logging*) atas seluruh aktivitas pengguna, jaringan, sistem, aplikasi, *error* yang terjadi (*exceptions*). Pemilik aset informasi harus menganalisis *log* terkait pola-pola penggunaan yang tidak wajar.
9. Fasilitas pencatatan *log* dan informasi *log* yang dicatat harus dilindungi dari penghapusan dan akses oleh pihak yang tidak berwenang.
10. Semua fasilitas pemrosesan informasi yang terhubung ke jaringan internal PD/Unit Kerja harus disinkronisasi dengan sumber waktu yang akurat dan telah disepakati.
11. Proses dan prosedur untuk mengendalikan instalasi perangkat lunak pada sistem operasional harus ditetapkan dan diimplementasikan untuk memastikan terjaganya kerahasiaan, integritas dan ketersediaan informasi.
12. Instalasi software harus dilakukan oleh administrator sistem yang relevan.
13. Pemilik aset informasi wajib melakukan upaya-upaya identifikasi atas kelemahan teknis (*vulnerabilities*) dari seluruh aset informasi dibawah pengelolaannya, serta melakukan tindakan pengendalian yang sesuai untuk meminimalkan resiko atas hilangnya aset informasi. Tindakan pengendalian dapat berupa menonaktifkan fitur tertentu, perbaikan/upgrade sistem, aplikasi, atau *patching*.
14. Setiap sistem informasi di lingkungan SKPD/Unit Kerja dapat dilakukan proses audit yang mencakup proses verifikasi terhadap sistem informasi dan/atau informasi SKPD/Unit Kerja dengan mempertimbangkan sebagai berikut:
 - a. harus direncanakan dan dikelola dengan baik untuk meminimalisasi gangguan terhadap proses bisnis;
 - b. setiap proses audit yang membutuhkan akses kepada sistem informasi dan/atau informasi PD/Unit Kerja harus disetujui oleh pemilik dari sistem dan/atau informasi tersebut;
 - c. hak akses untuk kebutuhan audit harus dibatasi hanya hak akses read only; dan
 - d. instalasi dari tools yang digunakan untuk proses audit hanya dapat dilakukan oleh personil yang berwenang yaitu administrator jaringan dan sistem TI di PD/Unit Kerja, dan harus segera dihapus setelah proses audit telah selesai dilakukan.

BAB XI

KEAMANAN KOMUNIKASI

A. Tujuan

Tujuan dari kebijakan keamanan komunikasi adalah untuk:

1. Memastikan perlindungan atas informasi pada jaringan komputer beserta fasilitas pendukung pengolahan informasi;
2. Menjaga keamanan informasi yang dipertukarkan, baik di dalam PD/Unit Kerja maupun antar PD/Unit Kerja eksternal.

B. Kebijakan

1. Jaringan internal PD/Unit Kerja harus diamankan untuk menjamin:
 - a. pencegahan akses tanpa izin ke jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan;
 - b. keamanan dari informasi milik organisasi yang dikirimkan melalui jaringan; danintegritas dan ketersediaan dari layanan jaringan organisasi.
2. Tugas dan tanggung jawab untuk pengelolaan jaringan dan keamanan harus dialokasikan dan apabila memungkinkan dipisahkan dari penanggung jawab operasional sistem aplikasi dan *data center*.
3. Konfigurasi dari jaringan, perangkat aktif dan perangkat keamanan jaringan harus ditinjau secara berkala untuk:
 - a. memastikan kesesuaian dengan kondisi terkini; dan
 - b. mengidentifikasi kerawanan pada jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan.
4. Jaringan internal PD/Unit Kerja harus dipisahkan dari jaringan eksternal dengan menggunakan *security gateway* atau *firewall* dan harus dikonfigurasi untuk:
 - a. memfilter *traffic* tanpa izin maupun *traffic* yang mencurigakan; dan
 - b. apabila memungkinkan memfilter dan mencegah infeksi *malware* ke jaringan internal;
5. Koneksi ke *security gateway* atau *firewall* harus diotentikasikan, diotorisasi dan diamankan dengan metode pengamanan yang sesuai, misalnya dengan *virtual private network* (VPN), *secure shell* (SSH) atau metode kriptografi.
6. Kebijakan dan log *firewall* harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan.
7. Koneksi eksternal harus diputuskan secara otomatis setelah tidak aktif selama 5 menit.

8. Akses dari jaringan eksternal yang dilakukan oleh *vendor* pihak ketiga hanya dapat diberikan untuk kebutuhan *troubleshooting* dan harus secara formal disetujui dan didokumentasikan dan harus dibatasi waktunya sesuai dengan kebutuhan dari akses.
9. Jaringan internal organisasi harus disegmentasi baik secara fisik maupun *logical* untuk meningkatkan keamanan dan untuk mengendalikan akses dan *traffic* jaringan berdasarkan kritikalitas dari sistem dalam jaringan PD/Unit Kerja.
10. Segmentasi jaringan harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan untuk menjamin kesesuaian dengan prasyarat keamanan terkini.
11. *Routing* jaringan harus dilakukan berdasarkan pengendalian terhadap alamat sumber dan tujuan.
12. Tanggung jawab untuk merubah *routing* jaringan hanya diberikan kepada administrator jaringan yang diberi izin.
13. Aturan untuk *routing* harus ditinjau paling tidak satu kali dalam tiga bulan untuk mendeteksi dan mengoreksi adanya kesalahan atau *routing* tanpa otorisasi.
14. Perangkat jaringan harus ditempatkan pada lokasi yang aman untuk menghindari akses tanpa izin dan ancaman fisik maupun lingkungan.
15. Akses, baik fisik maupun *logical* ke perangkat jaringan harus dibatasi untuk tujuan administrasi dan pemeliharaan jaringan.
16. *Port* dan layanan jaringan, baik fisik maupun *logical*, yang tidak digunakan tidak boleh diaktifkan.
17. Akses ke *port* yang digunakan untuk kebutuhan *diagnostic* dan konfigurasi perangkat jaringan dan keamanan jaringan, seperti *console port*, harus sangat dibatasi dan diberikan kepada:
 - a. administrator jaringan dan keamanan jaringan PD/Unit Kerja;
 - b. pihak ketiga yang telah disetujui dan bekerja untuk kepentingan PD/Unit Kerja;
 - c. aplikasi monitoring jaringan dan keamanan jaringan yang telah disetujui.
18. Semua perangkat jaringan harus dapat diidentifikasi secara fisik maupun *logical* dengan penamaan yang disepakati dan konsisten.
19. Perangkat jaringan yang dimiliki oleh pihak eksternal harus secara memadai dipisahkan dari perangkat jaringan milik PD/Unit Kerja.
20. Mekanisme keamanan, tingkat layanan dan prasyarat lain untuk semua layanan jaringan harus diidentifikasi dan dimasukkan kedalam perjanjian layanan jaringan.

21. Akses ke layanan jaringan PD/Unit Kerja hanya diberikan kepada personil yang terotorisasi berdasarkan prinsip *need to have*.
22. Penggunaan pihak ketiga penyedia layanan jaringan harus dimonitor untuk menjamin kesesuaian dengan prasyarat keamanan PD/Unit Kerja.
23. Layanan jaringan organisasi harus diamankan menggunakan metode yang dapat mencakup metode otentikasi atau metode kriptografi yang kuat untuk menjamin keamanan dari pengiriman informasi menggunakan jaringan dan layanan jaringan.
24. Terkait aspek pertukaran informasi melalui fasilitas jaringan komunikasi, PD/Unit Kerja harus memperhatikan perjanjian kerahasiaan merupakan perikatan formal antara pemilik aset informasi dengan penerima informasi, yang ketentuan didalamnya memuat:
 - a. pemberian izin penggunaan informasi dari pemilik aset informasi kepada penerima informasi untuk keperluan dan periode waktu yang spesifik, dimana pihak penerima informasi wajib menjaga kerahasiaan informasi serta mengupayakan pencegahan terjadinya kebocoran atau penyebaran informasi secara tidak sah;
 - b. hak dari pemilik aset informasi untuk melakukan audit dan pemantauan aktivitas penerima informasi berkaitan dengan penggunaan informasi sensitif; dan
 - c. konsekuensi yang harus ditanggung penerima informasi apabila terjadi pelanggaran atas perjanjian kerahasiaan.

BAB XII

AKUISISI, PENGEMBANGAN DAN PEMELIHARAAN SISTEM

A. Tujuan

Tujuan dari kebijakan akuisisi, pengembangan dan pemeliharaan sistem adalah untuk :

1. Memastikan keamanan informasi sebagai bagian tak terpisahkan dari siklus hidup (*lifecycle*) sistem informasi, termasuk persyaratan untuk sistem informasi yang menyediakan layanan melalui jaringan publik.
2. Memastikan keamanan informasi didesain dan diimplementasikan dalam siklus hidup (*lifecycle*) pengembangan dari sistem informasi.
3. Memastikan perlindungan terhadap penggunaan data untuk pengujian.

B. Kebijakan

1. PD/Unit Kerja harus menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengembangan, perluasan, atau pengadaan sistem informasi baru.
2. Persyaratan keamanan harus diidentifikasi secara jelas di dalam dokumen persyaratan dan spesifikasi perangkat lunak (*Software Requirement and Specification*).
3. Spesifikasi ini harus disetujui oleh pemilik informasi, pemilik proses bisnis dan pengembang sistem, sebelum fase pengkodean (*coding*) dalam pengembangan sistem.
4. Informasi yang digunakan oleh aplikasi PD/Unit Kerja yang ditransmisikan melalui jaringan publik (internet) harus diamankan dari aktivitas penipuan, kemungkinan adanya perselisihan kontrak, dan pengungkapan dan/atau perubahan informasi tanpa izin.
5. Pengamanan informasi terhadap informasi yang ditransmisikan melalui sistem informasi yang digunakan dapat mencakup namun tidak terbatas pada :
 - a. proses otentikasi dan otorisasi terhadap pengguna aplikasi;
 - b. perlindungan untuk memastikan kerahasiaan dan integritas informasi yang dipertukarkan melalui jaringan publik;
 - c. Perlindungan terhadap *session* transaksi untuk menghindari duplikasi dan/atau modifikasi;
 - d. mengamankan jalur komunikasi antara pihak-pihak yang terlibat
6. Keamanan dalam proses pengembangan dan dukungan yang perlu dipertimbangkan oleh PD/Unit Kerja meliputi:
 - a. aturan untuk pengembangan sistem harus ditetapkan dan diimplementasikan untuk proses pengembangan sistem di PD/Unit Kerja yang mencakup:
 - 1) pengamanan dari lingkungan pengembangan, seperti pemisahan lingkungan pengembangan baik secara fisik dan/atau logical, pengendalian akses, pengelolaan perubahan;
 - 2) panduan *secure coding*;
 - 3) pengendalian versi aplikasi;
 - 4) penyimpanan dari *source code*;
 - 5) metode pengujian untuk mengidentifikasi dan memperbaiki *vulnerability*.
7. Perubahan terhadap sistem selama siklus pengembangan sistem harus dikendalikan melalui proses manajemen perubahan yang berlaku di PD/Unit Kerja;

8. Apabila *platform* operasional, misalnya sistem operasi, *database* dan/atau *middleware*, dari sistem informasi PD/Unit Kerja mengalami perubahan, aplikasi kritikal PD/Unit Kerja harus ditinjau dan diuji untuk memastikan tidak ada dampak buruk terhadap operasional dan keamanan organisasi;
9. PD/Unit Kerja harus menetapkan lingkungan pengembangan yang aman untuk pengembangan dan integrasi sistem PD/Unit Kerja. Hal ini dapat mencakup namun tidak terbatas pada:
 - a. pemisahan lingkungan pengembangan baik secara fisik dan/atau logical;
 - b. pengendalian akses;
 - c. perpindahan data dari dan ke lingkungan pengembangan;
10. PD/Unit Kerja harus mengawasi aktivitas pengembangan sistem yang dialihdayakan (*outsourced*). Hal ini dapat mencakup:
 - a. perjanjian terkait lisensi dan kepemilikan sistem;
 - b. pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari sistem;
 - c. prasyarat dokumentasi untuk sistem;
 - d. perjanjian dengan pihak ketiga sebagai penjamin;
 - e. hak untuk melakukan audit proses pengembangan dan kontrol yang diimplementasikan oleh vendor.
11. Pengujian dari fitur keamanan sistem harus dilakukan pada saat pengembangan sistem informasi PD/Unit Kerja;
12. Pengujian ini dilakukan berdasarkan prasyarat keamanan sistem yang telah ditetapkan;
13. Kriteria dan jadwal untuk pengujian penerimaan sistem harus ditetapkan untuk sistem informasi baru, *upgrade* dan versi baru dari sistem informasi PD/Unit Kerja;
14. Pengujian penerimaan sistem harus dilakukan sesuai dengan kriteria dan jadwal yang ditetapkan.
15. Pengamanan terhadap data hasil pengujian perlu diperhatikan sebagai berikut:
 - a. data untuk pengujian sistem harus dipilih secara hati-hati untuk menghindari pengungkapan atau perubahan informasi sensitif oleh pihak yang tidak berhak; serta melindungi dari kemungkinan kerusakan dan kehilangan informasi;
 - b. *masking* data harus dilakukan apabila data operasional yang sensitif digunakan untuk keperluan pengujian;
 - c. data operasional yang digunakan untuk keperluan pengujian harus dihapus segera setelah proses pengujian telah selesai dilaksanakan.

BAB XIII

HUBUNGAN KERJA DENGAN PEMASOK (*SUPPLIER*)

A. Tujuan

Tujuan dari kebijakan mengenai hubungan kerja dengan pemasok (*supplier*) adalah untuk memastikan perlindungan atas aset PD/Unit Kerja dalam jangkauan akses pemasok dan memelihara tingkat layanan yang dsetujui dari keamanan informasi sesuai dengan perjanjian dengan pemasok.

B. Kebijakan

1. PD/Unit Kerja harus mempertimbangkan aspek keamanan informasi dalam hubungan dengan pemasok mulai dari pemilihan, penunjukan, monitoring, evaluasi, sampai dengan terminasi.
2. Pemilihan dari penyedia jasa PD/Unit Kerja harus mengikuti kriteria berikut:
 - a. kompetensi, pengalaman dan catatan dari organisasi;
 - b. kepastian dari kemampuan penyedia jasa untuk menyediakan layanan;
 - c. kepastian dari kemampuan penyedia jasa untuk menjaga ketersediaan dari penyediaan layanan pada saat kondisi normal atau kondisi bencana (apabila terjadi bencana alam atau kegagalan dalam penyediaan layanan);
3. Berdasarkan pengelompokan pemasok yang telah bekerjasama, PD/Unit Kerja wajib mendefinisikan pembatasan aset dan aset informasi apa saja yang diperbolehkan untuk diakses oleh setiap kelompok pemasok, serta senantiasa memantau akses yang telah dilakukan.
4. PD/Unit Kerja menetapkan persyaratan keamanan informasi bagi setiap pemasok yang mengakses aset informasi, serta senantiasa memantau kepatuhan pemasok terhadap persyaratan tersebut. Pemasok yang menangani aset informasi dengan klasifikasi rahasia perlu menandatangani Perjanjian Kerahasiaan.
5. Kewajiban *supplier* dan tingkat layanan harus ditetapkan secara formal dalam kontrak kerja;
6. PD/Unit Kerja harus memastikan pengelolaan *delivery* layanan dari pemasok dengan memperhatikan:
 - a. layanan yang diserahkan kepada PD/Unit Kerja oleh pihak *supplier* harus secara berkala dipantau, dan ditinjau;

- b. proses pemantauan dilakukan untuk memverifikasi kesesuaian dari tingkat layanan yang diberikan dan prasyarat keamanan informasi dengan perjanjian kerja;
 - c. proses peninjauan dilakukan untuk mengidentifikasi problem terkait penyediaan layanan dan aspek keamanan informasi dalam penyediaan layanan oleh *supplier*;
 - d. peninjauan dari penyediaan layanan oleh *supplier* harus dilaksanakan paling sedikit satu kali dalam tiga bulan;
7. PD/Unit Kerja dapat melakukan audit terhadap penyediaan layanan yang diberikan pemasok.
8. Ketentuan dalam pelaksanaan audit kepada pemasok sebagai berikut:
- a. tanggung jawab untuk mengaudit tingkat layanan dimiliki oleh pihak, baik internal maupun eksternal, yang memiliki independensi dari pengguna layanan yang diberikan oleh *supplier* dan ditunjuk secara formal;
 - b. audit terhadap penyediaan layanan oleh *supplier* harus dilakukan paling sedikit satu kali dalam satu tahun;
 - c. setiap ketidaksesuaian yang ditemukan dalam proses peninjauan dan audit harus dikelola dan ditindaklanjuti;
9. Perubahan terhadap layanan yang diberikan oleh *supplier* harus dikelola, dengan memperhatikan kritikalitas dari proses bisnis pengguna layanan dan layanan yang diberikan oleh *supplier*;
10. Perubahan terhadap layanan yang diberikan oleh *supplier* harus dipastikan tidak akan mengganggu aspek kerahasiaan dari informasi PD/Unit Kerja serta integritas dan ketersediaan dari informasi dan layanan PD/Unit Kerja;
11. Perubahan terhadap layanan yang diberikan oleh *supplier* harus disetujui oleh manajemen PD/Unit Kerja yang relevan dan diformalisasikan dalam kontrak kerja.

BAB XIV

PENANGANAN INSIDEN KEAMANAN INFORMASI

A. Tujuan

Tujuan dari kebijakan penanganan insiden keamanan informasi adalah untuk memastikan adanya pendekatan yang konsisten dan efektif atas penanganan insiden keamanan informasi.

B. Kebijakan

1. Kejadian keamanan informasi adalah sebuah kejadian pada sistem, layanan ataupun jaringan yang dapat mengindikasikan adanya pelanggaran keamanan informasi atau kegagalan keamanan atau kejadian yang mungkin memiliki keterkaitan dengan keamanan informasi.
2. Kelemahan keamanan informasi adalah sebuah kelemahan yang teridentifikasi pada sistem, layanan atau jaringan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab dan dapat menyebabkan pelanggaran terhadap kebijakan keamanan informasi.
3. Insiden keamanan informasi adalah kejadian keamanan informasi yang tidak diinginkan dan tidak diperkirakan dimana kejadian tersebut menimbulkan gangguan terhadap operasional bisnis dan mengancam keamanan informasi.
4. Guna memastikan proses penanganan insiden yang responsif dan efektif, perlu dikembangkan berbagai prosedur yang mencakup:
 - a. perencanaan dan persiapan penanganan insiden;
 - b. pemantauan, analisis, dan pelaporan atas insiden;
 - c. pencatatan atas aktivitas penanganan insiden;
 - d. penanganan bukti forensik;
 - e. penilaian dan pengambilan keputusan atas insiden dan kelemahan keamanan informasi; dan
 - f. pemulihan insiden.
5. Seluruh pegawai dan pihak ketiga wajib melaporkan berbagai kejadian insiden keamanan informasi maupun yang masih bersifat dugaan atas kelemahan keamanan informasi sesegera mungkin, sesuai prosedur pelaporan insiden yang berlaku.
6. Setiap kejadian insiden keamanan informasi harus dianalisis, diklasifikasikan, dan ditentukan skala prioritas penanganannya. Penanganan insiden beserta pemulihannya dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.

7. PD/Unit Kerja harus mengklasifikasikan insiden keamanan informasi untuk memprioritaskan penanganan insiden. Klasifikasi insiden tersebut adalah sebagai berikut :
- a. insiden keamanan informasi diklasifikasikan berdasarkan dampaknya menjadi berikut :
 - 1) mayor, apabila insiden tersebut menyebabkan terhentinya proses operasional pekerjaan PD/Unit Kerja;
 - 2) minor, apabila insiden tersebut menyebabkan gangguan yang tidak menghentikan proses operasional pekerjaan PD/Unit Kerja.
 - b. insiden keamanan informasi diklasifikasikan berdasarkan tingkat kepentingannya menjadi berikut:
 - 1) *emergency*, apabila insiden tersebut dapat atau telah menghentikan proses operasional PD dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan PD/Unit Kerja;
 - 2) normal, apabila insiden tersebut tidak menghentikan proses operasional PD/Unit Kerja dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan PD/Unit Kerja.
8. Setiap insiden keamanan informasi harus ditangani dengan baik untuk mencegah meluasnya insiden, untuk memulihkan layanan atau informasi yang mungkin hilang dan untuk meminimalisasi dampak dari insiden.
9. Setiap tindakan yang diidentifikasi untuk menangani kejadian, kelemahan dan insiden keamanan informasi harus dikonsultasikan dengan koordinator NTTProv-CSIRT dan/atau personil yang kompeten dan relevan dengan kejadian, kelemahan dan insiden keamanan informasi.
10. Setiap tindakan penanganan kejadian, kelemahan dan insiden keamanan informasi harus didokumentasikan dengan baik.

KELANGSUNGAN USAHA (*BUSINESS CONTINUITY*)

A. Tujuan

Tujuan dari kebijakan mengenai kelangsungan usaha (*business continuity*) adalah untuk memastikan ketersediaan layanan TIK beserta fasilitas pengolahan informasi dalam kondisi darurat dan memulihkan layanan seperti sediakala dalam kondisi kembali normal.

B. Kebijakan

1. PD/Unit Kerja harus menetapkan, mendokumentasikan, mengimplementasikan dan memelihara proses, prosedur dan kontrol yang diperlukan untuk menjamin keberlanjutan keamanan informasi sesuai prasyarat yang telah ditetapkan pada saat dan setelah terjadinya gangguan besar atau bencana.
2. PD/Unit Kerja harus memverifikasi kontrol keberlanjutan keamanan informasi yang telah ditetapkan dan diimplementasikan secara berkala untuk menjamin kesesuaian dan efektivitasnya pada saat dan setelah terjadinya gangguan besar atau bencana.
3. PD/Unit Kerja harus menetapkan prasyarat untuk keberlanjutan keamanan informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis organisasi untuk menjamin keberlanjutan dari keamanan informasi di PD/Unit Kerja, pada saat dan setelah terjadinya gangguan besar atau bencana.
4. Prasyarat keamanan informasi dapat diintegrasikan pada siklus proses *business continuity management* (BCM) yang mencakup:
 - a. memahami kebutuhan organisasi;
 - b. menentukan strategi BCM;
 - c. mengembangkan dan mengimplementasikan rencana penanggulangan/keberlanjutan bisnis;
 - d. pengujian, pemeliharaan dan peninjauan rencana penanggulangan / keberlanjutan bisnis;
5. Aspek redundansi harus ditetapkan untuk fasilitas pengolahan informasi dan sarana pendukungnya untuk memastikan ketersediaan dari proses bisnis dan operasional PD/Unit Kerja serta pemberian layanan PD/Unit Kerja kepada pelanggan.
6. Apabila prasyarat redundan tidak dapat dipenuhi, maka proses alternatif perlu ditetapkan untuk menjamin ketersediaan dari proses bisnis dan operasional PD/Unit Kerja serta *delivery* dari layanan PD/Unit Kerja kepada pelanggan.

7. Fasilitas pengolahan informasi beserta sarana pendukungnya yang telah memenuhi aspek redundansi harus diuji secara berkala untuk menjamin kesesuaian dari fungsinya.
8. Guna menjamin ketersediaan layanan serta keamanan informasi dalam kondisi darurat (misalnya: bencana alam) pada lokasi utama, perlu adanya redundansi terhadap fasilitas pengolahan informasi yang disebut sebagai fasilitas *backup site*.
9. *Backup site* yang dimaksud dapat berupa lokasi kerja pengganti atau *disaster recovery center* (DRC) bagi alternatif area *data center*.
10. Ketentuan dalam pengelolaan terkait *Backup Site* meliputi:
 - a. lokasi *backup site* secara geografis memiliki probabilitas kejadian bencana alam yang minimal;
 - b. *backup site* ditujukan sebagai media penyimpanan *backup* alternatif, serta sebagai fasilitas pengolahan informasi alternatif;
 - c. terpenuhinya pemulihan layanan operasional sepenuhnya pada fasilitas *backup site* sesuai kerangka parameter *recovery time objective* (RTO);
 - d. pengelola *backup site* beserta Pemilik Aset Informasi melakukan uji keberlangsungan secara berkala dibawah koordinasi penanggung jawab kelangsungan bisnis, minimal 1 kali dalam setahun, untuk menguji kesiapan seluruh pihak dalam hal:
 - 1) memindahkan operasional ke fasilitas *backup site*;
 - 2) memulihkan operasional aplikasi beserta data sesuai parameter *recovery point objective* (RPO) yang telah ditetapkan.

BAB XVI

KEPATUHAN

A. Tujuan

Tujuan dari kebijakan kepatuhan adalah untuk menghindari pelanggaran kewajiban hukum, undang-undang, peraturan atau kontrak yang terkait keamanan informasi dan persyaratan keamanan dan untuk memastikan keamanan informasi diimplementasikan dan dioperasikan sesuai dengan prosedur dan kebijakan organisasi.

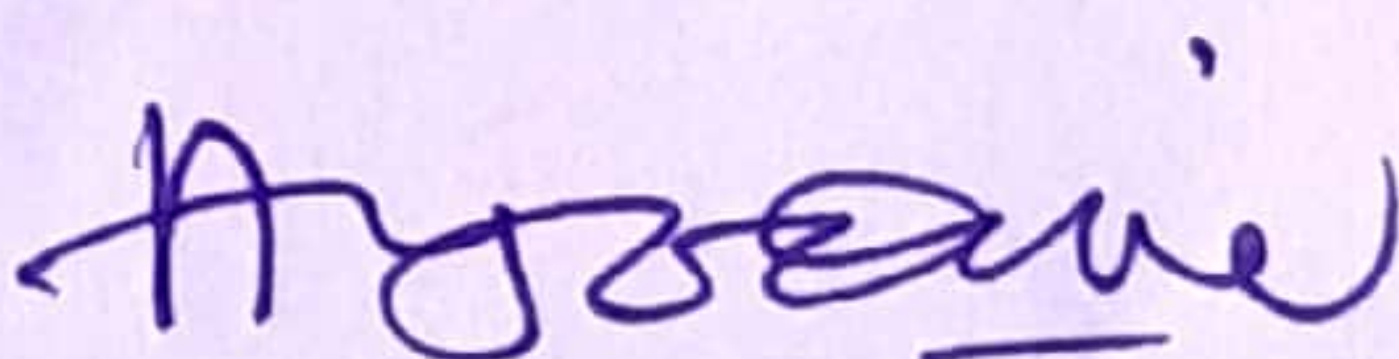
B. Kebijakan

1. Pemerintah Daerah Provinsi Nusa Tenggara Timur berkomitmen untuk menjaga kepatuhan terhadap setiap prasyarat keamanan informasi yang relevan. Prasyarat keamanan informasi yang dimaksud mencakup prasyarat hukum, regulasi dan kontraktual;
2. Seluruh prasyarat hukum, regulasi dan kontraktual yang terkait dengan keamanan informasi dan berlaku bagi PD/Unit Kerja harus diidentifikasi, didokumentasikan dan dipelihara;
3. PD/Unit Kerja harus mematuhi hak atas kekayaan intelektual yang terkait dengan material yang digunakan oleh PD/Unit Kerja seperti:
 - a. penggunaan perangkat lunak dan material yang bersifat *proprietary* harus mematuhi undang-undang terkait hak atas kekayaan intelektual (haki) yang berlaku;
 - b. bukti dari lisensi atau izin resmi harus didapatkan dan disimpan untuk seluruh materi berlisensi / *copyright* yang di-install;
 - c. lisensi yang bersifat berlangganan/harus diperbaharui dalam jangka waktu tertentu, harus dikelola untuk memastikan penggunaannya secara legal dan berkesinambungan;
 - d. penggunaan lisensi dari materi berlisensi/*copyright* harus dikendalikan dengan baik;
4. Dokumen-dokumen penting PD/Unit Kerja harus dilindungi dari kehilangan, pemalsuan, kerusakan, atau penyalahgunaan sesuai dengan peraturan perundangan, regulasi, dan persyaratan kontrak dan bisnis;
5. PD/Unit Kerja harus memastikan privasi dan perlindungan terhadap informasi terkait dengan pribadi (*personally identifiable information*) sesuai dengan prasyarat hukum, perundangan, regulasi dan kontraktual;



6. Pimpinan PD/Unit Kerja harus secara rutin memantau dan meninjau kepatuhan dari personil, proses kerja dan pemrosesan informasi dalam area tanggung jawabnya terhadap kebijakan dan standard keamanan informasi PD/Unit Kerja serta prasyarat keamanan informasi yang berlaku;
7. Pada saat terjadi ketidaksesuaian, pimpinan PD/Unit Kerja bertanggung jawab untuk menangani ketidaksesuaian yang terjadi sesuai dengan kebijakan terkait penanganan ketidaksesuaian dan peningkatan SMKI;
8. Sistem informasi PD/Unit Kerja harus ditinjau untuk menganalisis kepatuhan teknis dengan kebijakan dan standard keamanan yang berlaku serta dengan prasyarat keamanan informasi yang relevan dan berlaku, paling tidak satu kali dalam satu tahun;
9. Apabila diperlukan, peninjauan tersebut dapat melibatkan personil yang memiliki kualifikasi di bidang keamanan informasi untuk mendapatkan pemahaman yang mendalam mengenai risiko keamanan informasi yang mungkin muncul dari pengecualian tersebut.

PJ. GUBERNUR NUSA TENGGARA TIMUR, P


AYODHIA G. L. KALAKE