BUPATI ROTE NDAO
PROVINSI NUSA TENGGARA TIMUR

PERATURAN BUPATI ROTE NDAO
NOMOR 75 TAHUN 2023

TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH KABUPATEN ROTE NDAO

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI ROTE NDAO,

Menimbang:

a. bahwa dalam rangka melindungi kerahasiaan, keutuhan dan ketersediaan aset informasi di lingkungan Pemerintah Kabupaten Rote Ndao dari berbagai ancaman keamanan informasi baik dari dalam maupun luar maka perlu melakukan pengelolaan keamanan informasi;

b. bahwa sesuai ketentuan Pasal 24 ayat (2) Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik mengamanatkan bahwa Penyelenggaraan Sistem Elektronik wajib menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Sistem Manajemen Keamanan Informasi di lingkungan Pemerintah Kabupaten Rote Ndao;

Mengingat:

1. Pasal 18 ayat 6 Undang-Undang Dasar Tahun 1945;

2. Undang-Undang Nomor 9 Tahun 2002 tentang Pembentukan Kabupaten Rote Ndao di Provinsi Nusa Tenggara Timur (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 22, Tambahan Lembaran Negara Republik Indonesia Nomor 4184);

3. 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);

4. Peraturan..

4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
5. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 1054);
6. 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);
7. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik;
8. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik;

Menetapkan : PERATURAN BUPATI TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KABUPATEN ROTE NDAO.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:
1. Daerah adalah Kabupaten Rote Ndao.
2. Kepala Daerah adalah Bupati Rote Ndao.
3. Perangkat daerah adalah unsur pembantu Bupati dan DPRD dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
4. Dinas adalah dinas komunikasi, informatika, statistik dan persandian Kabupaten Rote Ndao yang menyelenggarakan urusan di bidang keamanan informasi yang menjadi kewenangan daerah otonom.
5. Pegawai Aparatur Sipil Negara yang selanjutnya disebut pegawai ASN 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 peraturan perundang-undangan.
6. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.
7. Sistem adalah suatu kesatuan yang terdiri komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran informasi, materi atau energi untuk mencapai suatu tujuan.

8.Informasi..

8. Informasi adalah keterangan, pernyataan, gagasan yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.
9. Teknologi informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
10. Teknologi informasi dan komunikasi yang selanjutnya disingkat tik adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
11. Perangkat lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian sistem elektronik.
12. Keamanan informasi adalah suatu kondisi dimana terjaganya aspek kerahasiaan, keutuhan dan ketersediaan dari informasi.
13. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko.
14. Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
15. Penyelenggara sistem elektronik adalah setiap orang, penyelenggara negara, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan sistem elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna sistem elektronik untuk keperluan dirinya dan/atau keperluan pihak lain.
16. Pelayanan publik adalah kegiatan atau rangkaian kegiatan dalam rangka pemenuhan kebutuhan pelayanan sesuai dengan peraturan perundang-undangan bagi setiap warga negara dan penduduk atas barang, jasa, dan/atau pelayanan administratif yang disediakan oleh penyelenggara pelayanan publik.
17. Penyelenggaraan sistem elektronik adalah pemanfaatan sistem elektronik oleh penyelenggara negara, orang, badan usaha, dan/atau masyarakat.
18. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja dari layanan sistem elektronik.
19. Aset informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
20. Aset pengolahan adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi.
21. Penyimpanan informasi adalah suatu proses menyimpan informasi dengan menggunakan media baik elektronik maupun non-elektronik.
22. Pusat data atau data center adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti sistem komunikasi data dan penyimpanan data.

23.Standar..

23. Standar Nasional Indonesia yang selanjutnya disebut SNI adalah dokumen berisi ketentuan teknik, persyaratan, dan karakteristik suatu kegiatan atau hasil kegiatan, yang disusun dan disepakati oleh pihak-pihak yang berkepentingan untuk membentuk keteraturan yang optimal ditinjau dari konteks keperluan tertentu, dan ditetapkan oleh badan standardisasi nasional sebagai standar yang berlaku di seluruh wilayah indonesia.
24. Sertifikat sistem manajemen keamanan informasi adalah bukti tertulis yang diberikan oleh lembaga sertifikasi kepada penyelenggara sistem elektronik yang telah memenuhi persyaratan.
25. Kriptografi adalah sebuah ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga.
26. Penilaian mandiri adalah mekanisme evaluasi yang dilakukan secara mandiri oleh penyelenggara sistem elektronik berdasarkan kriteria tertentu.
27. Indeks keamanan informasi yang selanjutnya disebut Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di organisasi.
28. Sertifikasi adalah suatu penetapan yang diberikan oleh suatu organisasi profesional terhadap seseorang untuk menunjukkan bahwa orang tersebut mampu untuk melakukan suatu pekerjaan atau tugas spesifik.
29. SNI ISO/IEC 27001 adalah sebuah dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Managemen System* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah organisasi dalam rangka mengimplementasikan konsep keamanan informasi.

BAB II
MAKSUD DAN TUJUAN

Pasal 2

(1) Maksud ditetapkannya Peraturan Bupati ini adalah sebagai pedoman pengelolaan SMKI secara terpadu untuk memastikan terjaganya kerahasiaan, keaslian, keutuhan dan ketersediaan suatu informasi.
(2) Tujuan ditetapkannya Peraturan Bupati ini adalah:
    a. menjamin terciptanya integritas, sinkronisasi dan sinergi dalam sistem manajemen keamanan informasi untuk seluruh perangkat daerah di lingkungan Pemerintah Kabupaten Rote Ndao; dan
    b. mengoptimalkan pengelolaan sistem manajemen keamanan informasi meliputi infrastruktur komputer, jaringan, sistem informasi/aplikasi dan sumber daya manusia.

BAB III
ASET INFORMASI DAN PENGOLAHAN INFORMASI

Pasal 3

Aset informasi merupakan aset dalam bentuk:
a. fisik meliputi informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti di atas kertas, papan tulis, spanduk atau di dalam buku dan dokumen; dan

b.elektronik..

b. elektronik meliputi informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti *database* dan *file* di dalam komputer, informasi yang ditampilkan pada *website* dan layar komputer serta informasi yang dikirimkan melalui jaringan telekomunikasi.

Pasal 4

Aset pengolahan informasi berupa:
a. peralatan mekanik yang digerakkan dengan tangan secara manual; dan
b. peralatan elektronik yang bekerja secara elektronik penuh.

BAB IV
PENYIMPANAN INFORMASI

Pasal 5

Penyimpanan Informasi menggunakan media:
a. elektronik, meliputi server, hard disk, flash disk, kartu memori dan lain-lain; dan
b. non-elektronik, meliputi lemari, rak, laci, *filling cabinet* dan lain-lain.

BAB V
KATEGORISASI SISTEM ELEKTRONIK

Pasal 6

(1) Kategorisasi sistem elektronik berdasarkan asas risiko terdiri atas:
   a. sistem elektronik strategis;
   b. sistem elektronik tinggi; dan
   c. sistem elektronik rendah.
(2) Sistem elektronik strategis sebagaimana dimaksud pada ayat (1) huruf a, merupakan sistem elektronik yang berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara atau pertahanan dan keamanan negara.
(3) Sistem elektronik tinggi sebagaimana dimaksud pada ayat (1) huruf b, merupakan sistem elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu.
(4) Sistem elektronik rendah sebagaimana dimaksud pada ayat (1) huruf c, merupakan sistem elektronik lainnya yang tidak termasuk pada ayat (2) dan ayat (3).

BAB VI
PENYELENGGARAAN SMKI

Bagian Kesatu
Standar Penyelenggaraan SMKI

Pasal 7

(1) Penyelenggara sistem elektronik yang menyelenggarakan sistem elektronik strategis wajib menerapkan:
   a. SNI ISO/IEC 27001 atau *update*terbaru;
   b. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh BSSN; dan
   c. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh Kementerian atau Lembaga.

(2) Penyelenggara..

(2) Penyelenggara sistem elektronik yang menyelenggarakan sistem elektronik tinggi wajib menerapkan:
   a. SNI ISO/IEC 27001 atau *update* terbaru dan standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh BSSN; dan
   b. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh Kementerian atau Lembaga.

(3) Penyelenggara sistem elektronik.
Penyelenggara yang menyelenggarakan sistem elektronik rendah wajib menerapkan:
   a. SNI ISO/IEC 27001 atau update terbaru; dan
   b. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh BSSN.

Bagian Kedua
Persiapan Penerapan SMKI dan Penilaian Mandiri

Pasal8

Penerapan SNI ISO/IEC 27001 oleh penyelenggara sistem elektronik dengan melakukan penilaian mandiri berdasarkan kategorisasi sistem elektronik menggunakan Indeks KAMI sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Ketiga
Penerapan SMKI Sesuai Kategorisasi Sistem Elektronik

Pasal 9

(1) Dinas dalam melakukan pengamanan informasi wajib memiliki koordinator keamanan teknologi informasi.

(2) Koordinator keamanan teknologi informasi sebagaimana dimaksud pada ayat (I) bertanggungjawab terhadap teknologi informasi yang digunakan untuk mendukung proses tata kelola pemerintahan dan pencapaian tujuan organisasi.

(3) Koordinator keamanan teknologi informasi sebagaimana dimaksud pada ayat (2) memiliki wewenang:
   a. menyusun prosedur pelaksanaan keamanan informasi yang diterapkan secara efektif baik bagi perangkat daerah maupun pengguna; dan
   b. melakukan evaluasi kinerja pelaksanaan teknologi informasi.

(4) Koordinator keamanan informasi sebagaimana dimaksud pada ayat (3) dijabat oleh pejabat struktural yang membidangi persandian.

Pasal 10

(1) Dinas penyelenggara teknologi informasi wajib melakukan proses manajemen risiko dalam menerapkan 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..

(3) Manajemen risiko sebagaimana dimaksud pada ayat (2) mencakup :

a. pengembangan sistem;

b. operasional teknologi informasi;

c. jaringan komunikasi;

d. penggunaan perangkat komputer;

e. pengendalian terhadap informasi; dan/atau

f. pihak ketiga sebagai penyedia jasa teknologi informasi.

(4) Penerapan manajemen risiko harus dilakukan secara terintegrasi pada setiap penggunaan operasional teknologi informasi terkait sistem yang digunakan.

Pasal 11

(1) Dinas menyediakan sumber daya yang dibutuhkan untuk membentuk, mengimplementasikan, memelihara dan meningkatkan penerapan SMKI secara berkesinambungan.

(2) Uraian secara rinci SMKI sebagaimana dimaksud pada ayat (1) tercantum dalam lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 12

(1) Dinas wajib menyusun standar dan prosedur pengendalian kegiatan teknologi informasi yang memenuhi syarat keamanan informasi dan untuk mengimplementasikan tindakan dalam mengelola risiko.

(2) Syarat 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 sistem informasi;

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.

Pasal 13

(1) Dinas bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman.

(2) Pelaksanaan..

(2) Pelaksanaan pemrosesan transaksi pada operasional teknologi informasi harus memenuhi prinsip kehati-hatian.

(3) Dinas penyelenggara teknologi informasi wajib mengidentifikasi dan memantau aktivitas operasional teknologi informasi untuk memastikan efektifitas, efesiensi dan keamanan dari aktivitas tersebut antara lain dengan:

a. menerapkan perimeter fisik dan lingkungan di area kerja dan pusat data;

b. mengendalikan hak akses secara memadai sesuai kewenangan yang ditetapkan;

c. menerapkan pengendalian terhadap informasi yang diproses;

d. memastikan ketersediaan dan kecukupan kapasitas layanan jaringan komunikasi baik yang dikelola secara internal maupun oleh pihak lain penyedia jasa;

e. melakukan pemantauan kegiatan operasional teknologi informasi termasuk audit trail; dan

f. melakukan pemantauan terhadap aplikasi yang digunakan oleh perangkat daerah maupun pengguna.

Pasal 14

(1) Dinas wajib memastikan ketersediaan data dan sistem dalam rangka menjaga kelangsungan teknologi informasi melalui penyelenggaraan fasilitas pusat data baik dikelola oleh internal maupun oleh pihak penyedia jasa.

(2) Setiap aktivitas pada fasilitas di pusat data wajib dipantau guna menghindari kesalahan proses pada sistem dan memperhatikan aspek perlindungan terhadap data yang diproses dan lingkungan fisik.

Pasal 15

(1) Dinas harus menerapkan prinsip pengendalian terhadap aktivitas teknologi informasi melalui proses evaluasi dan monitoring secara berkala.

(2) Dinas 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) Dinas berdasarkan hasil audit, umpan balik, maupun evaluasi terhadap pengendalian keamanan informasi yang dilakukan, wajib meningkatkan efektivitas sistem 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) wajib dilaporkan kepada kepala dinas dan didokumentasikan.

Pasal 16

(1) Apabila terjadi kebocoran informasi pada perangkat daerah yang berdampak sangat luas, maka Bupati menunjuk auditor lembaga sertifikasi untuk melakukan investigasi.

(2) Dinas..

(2) Dinas wajib memberikan akses kepada auditor lembaga sertifikasi untuk melakukan pemeriksaan.

Bagian Keempat
Lembaga Sertifikasi

Pasal 17

(1) Lembaga sertifikasi yang dapat melakukan investigasi sebagaimana dimaksud pada Pasal 16 ayat (1) adalah lembaga sertifikasi yang diakui oleh BSSN.
(2) Ketentuan mengenai pengakuan Lembaga sertifikasi sebagaimana dimaksud dalam ayat (1) sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 18

(1) Lembaga Sertifikasi menugaskan tim Auditor SMKI untuk melakukan audit SMKI terhadap perangkat daerah penyelenggara sistem elektronik.
(2) Tim Auditor SMKI sebagaimana dimaksud pada ayat (1) melaporkan hasil audit pada lembaga sertifikasi yang menugaskan.
(3) Lembaga Sertifikasi mengkaji hasil audit yang dilaporkan oleh tim auditor SMKI.
(4) Lembaga Sertifikasi menerbitkan sertifikat SMKI bagi perangkat daerah penyelenggara sistem elektronik yang telah memenuhi standar.

Pasal 19

Lembaga Sertifikasi wajib melaksanakan audit pengawasan paling sedikit 1 (satu) kali dalam setahun dan audit khusus apabila terjadi insiden terhadap setiap sistem elektronik yang telah tersertifikasi.

Pasal 20

(1) Apabila audit pengawasan tidak memenuhi standar, maka diberikan waktu paling lama 90 (sembilan puluh) hari kalender untuk memenuhi standar tersebut.
(2) Apabila setelah 90 (sembilan puluh) hari kalender belum terpenuhi, maka Lembaga Sertifikasi dapat mencabut sertifikat SMKI.
(3) Pencabutan sebagaimana dimaksud pada ayat (2) wajib dilaporkan oleh Lembaga Sertifikasi kepada BSSN paling lambat 2 (dua) hari kerja sejak dilakukan pencabutan.

BAB VII
PEMBIAYAAN

Pasal 21

Pembiayaan atas pelaksanaan Peraturan Bupati ini dibebankan pada: ۴
anggaran pendapatan dan belanja negara;
a. anggaran pendapatan dan belanja daerah; dan/atau
b. sumber pembiayaan lain sesuai dengan ketentuan peraturan perundang-undangan.

BAB VIII..

BAB VIII
KETENTUAN PENUTUP

Pasal 22

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Rote Ndao.

Ditetapkan di Baa
Pada tanggal 26 september 2023

BUPATI ROTE NDAO,

PAULINA HANING - BULLU

Diundangkan di Ba'a
Pada tanggal 26 September 2023

SEKRETARIS DAERAH KABUPATEN ROTE NDAO,

JONAS MATEOS SELLY

BERITA DAERAH KABUPATEN ROTE NDAO TAHUN 2023 NOMOR 075

LAMPIRAN PERATURAN BUPATI ROTE NDAO
NOMOR 75 TAHUN 2023
TENTANG
SISTEM MANAJEMEN KEAMANAN INFRMASI DI LINGKUNGAN PEMERINTAH KABUPATEN ROTE NDAO

BAB I
PENDAHULUAN

Kebijakan umum keamanan informasi memuat kebijakan keamanan informasi yang menjadi acuan dalam kebijakan spesifik, pedoman, prosedur, manajemen risiko maupun proses keamanan informasi lainnya. Kebijakan spesifik digunakan oleh bagian teknis dalam menyelesaikan tanggung jawab keamanan informasi. Pedoman dan prosedur digunakan untuk mengimplementasikan kebijakan yang telah ditetapkan dan sifatnya anjuran. Hal tersebut berbeda dengan kebijakan yang sifatnya keharusan. Kebijakan umum keamanan informasi memiliki kesamaan tingkat dengan kebijakan di daerah lainnya dan dipatuhi oleh semua pengguna. Berbeda dengan kebijakan spesifik yang hanya berlaku untuk perangkat daerah tertentu sesuai dengan bidangnya. Begitupula dengan pedoman dan prosedur yang dilaksanakan oleh dinas.

BAB II
KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Keamanan Informasi.
   1. Ruang lingkup keamanan informasi terdiri atas:
      a) keamanan informasi meliputi keamanan database, kontrak, dokumentasi sistem, manual pengguna, prosedur pendukung, strategi untuk mengatasi keadaan dimana kondisi harus dapat terus berjalan pasca terjadinya bencana (*business continuity plan*);
      b) keamanan aset perangkat lunak meliputi keamanan perangkat lunak aplikasi, perangkat lunak sistem dan utilitas;
      c) keamanan aset fisik meliputi keamanan perangkat komputer dan perangkat jaringan;
      d) keamanan layanan meliputi keamanan layanan komputasi dan komunikasi, utilitas umum (listrik, pemanas dan *air-conditioning*);
      e) keamanan sumber daya manusia beserta kualifikasi, keterampilan dan pengalaman; dan
      f) keamanan aset yang tidak berwujud seperti reputasi, image organisasi.
   2. Keamanan informasi merupakan tanggungjawab dari semua pihak yang terkait pada daerah yang terdiri dari:
      a) Bupati;
      b) Wakil Bupati;
      c) Sekretaris Daerah;
      d) Para Asisten;

e) Kepala..

e) Kepala Perangkat Daerah;
f) Anggota DPRD;
g) Instansi Vertikal; dan
h) Seluruh Aparatur Sipil Negara.

3. Keamanan informasi di lingkungan pemerintah daerah dilakukan dengan cara:
   a) memberikan langkah-langkah perlindungan, mempertahankan informasi dan sistem informasi dengan memastikan ketersediaan, integritas, otentikasi, kerahasiaan dan nirpenyangkalan bagi stakeholder utama daerah;
   b) meningkatkan jaminan atas aset informasi terhadap risiko keamanan melalui proteksi yang cukup dan berkelanjutan. Risiko tersebut memiliki dampak langsung maupun tidak langsung bagi negara;
   c) meningkatkan kepatuhan terhadap undang-undang dan peraturan terkait keamanan informasi yang ada di indonesia;
   d) meningkatkan kepercayaan publik dan stakeholder terhadap daerah; dan
   e) meningkatkan respon terhadap pelanggaran atau insiden keamanan informasi.
4. Tujuan keamanan informasi.
   Tujuan keamanan informasi di lingkungan pemerintah daerah adalah untuk:
   a) memastikan kerahasiaan terhadap aset informasi di lingkungan Pemerintah daerah;
   b) memastikan ketersediaan dan integritas informasi bagi stakeholder;
   c) memastikan kepatuhan terhadap hukum, undang-undang dan peraturan yang berlaku; dan
   d) memastikan kapabilitas organisasi untuk melanjutkan operasi atau layanannya ketika terjadi insiden keamanan.
5. Prinsip keamanan informasi.
   Prinsip keamanan informasi di lingkungan pemerintah daeah meliputi:
   a) prinsip kerahasiaan yaitu kemampuan akses atau modifikasi informasi diberikan hanya kepada pihak yang berwenang untuk tujuan yangjelas;
   b) prinsip ketersediaan yaitu informasi dan aset teknologi informasi yang dimiliki oleh daerah tersedia untuk mendukung organisasi dalam rentang waktu yang disepakati bersama sesuai tujuan organisasi;
   c) prinsip integritas yaitu informasi yang digunakan pengguna bisa dipercaya kebenarannya, merefleksikan realitas sebenarnya, terutama informasi strategis;
   d) prinsip akuntabilitas yaitu tanggung jawab dan akuntabilitas pemilik, penyedia dan pengguna sistem informasi dan pihak lain yang terkait dengan keamanan informasi harus dideskripsikan dengan jelas;

e) prinsip..

e) prinsip kesadaran yaitu pemilik, penyedia, pengguna sistem informasi dan pihak lain yang terkait memiliki pemahaman dan informasi yang cukup mengenai kebijakan, pedoman, prosedur, ukuran dan praktek keamanan informasi;
f) prinsip integrasi yaitu kebijakan, pedoman, prosedur, ukuran dan praktek untuk keamanan informasi harus dikoordinasikan dan diintegrasikan antara satu dengan yang lainnya; dan
g) prinsip perbaikan berkelanjutan yaitu keamanan informasi harus diperbaiki terus menerus mengikuti perkembangan risiko dan kebutuhan organisasi.

6. Pemantauan, pengukuran, analisis dan evaluasi kinerja keamanan informasi.
   a. Dinas dalam melakukan pemantauan, pengukuran, analisis dan evaluasi kinerja keamanan informasi wajib menentukan:
      1) apa yang perlu dipantau dan diukur termasuk proses dan pengendalian keamanan informasi;
      2) metode untuk pemantauan, pengukuran, analisis dan evaluasi jika dapat diterapkan untuk memastikan hasil yang valid;
      3) kapan pemantauan dan pengukuran harus dilakukan;
      4) siapa yang wajib memantau dan mengukur;
      5) kapan hasil dari pemantauan dan pengukuran harus dianalisis dan dievaluasi; dan
      6) siapa yang wajib menganalisis dan mengevaluasi hasil tersebut.
   b. Dinas wajib menyimpan informasi terdokumentasi yang memadai sebagai bukti hasil pemantauan dan pengukuran.
7. Audit internal.
   a. Dinas wajib melakukan audit internal pada selang waktu terencana untuk memberikan informasi apakah keamanan informasi diimplementasikan dan dipelihara secara efektif serta sesuai dengan:
      1) persyaratan yang ditetapkan Bupati untuk keamanan informasinya;
      2) persyaratan standar ISO/IEC 27001; dan
      3) indeks KAMI.
   b. Dinas wajib:
      1) merencanakan, menetapkan, menerapkan dan memelihara program audit, termasuk frekuensi, metode, tanggung jawab, persyaratan perencanaan dan pelaporan. Program audit harus mempertimbangkan pentingnya proses yang bersangkutan dan hasil audit sebelumnya;
      2) menentukan kriteria audit dan ruang lingkup untuk setiap audit;
      3) melakukan audit yang menjamin objektivitas dan ketidak berpihakan proses audit;
      4) memastikan bahwa hasil audit tersebut dilaporkan kepada manajemen yang relevan dan bertanggungjawab; dan
      5) menyimpan informasi terdokumentasi sebagai alat bukti dari program audit dan hasil audit.

c. Peninjauan..

c. Peninjauan manajemen.
Bupati harus mereviu kebijakan SMKI minimal satu kali dalam satu tahun untuk memastikan kesesuaian, kecukupan dan efektivitas. Peninjauan manajemen harus mencakup pertimbangan:
1. status tindakan dari reviu manajemen sebelumnya;
2. perubahan isu eksternal dan internal yang relevan dengan keamanan informasi;
3. umpan balik dari kinerja keamanan informasi, termasuk kecenderungan dalam hal:
   a) ketidaksesuaian dan tindakan korektif;
   b) hasil pemantauan dan pengukuran;
   c) hasil audit;
   d) pemenuhan terhadap sasaran keamanan informasi;
   e) umpan balik dari pihak yang berkepentingan;
   f) hasil penilaian risiko dan status rencana penanganan risiko;dan
   g) peluang untuk perbaikan berkelanjutan. Keluaran dari peninjauan manajemen harus mencakup keputusan yang berkaitan dengan peluang perbaikan berkelanjutan dan setiap kebutuhan untuk perubahan SMKI.
4. Dinas harus menyimpan informasi terdokumentasi sebagai bukti hasil peninjauan manajemen.

8. Perbaikan ketidaksesuaian dan tindakan korektif.
Apabila terjadi ketidaksesuaian maka dinas harus:
   a) bereaksi terhadap ketidaksesuaian dan jika dapat, diterapkan untuk mengambil tindakan untuk mengendalikan dan mengoreksinya dan menangani konsekuensinya;
   b) mengevaluasi kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian, agar hal itu tidak terulang atau terjadi di tempat lain. Tindakan yang dilakukan adalah dengan cara:
      1) meninjau ketidaksesuaian;
      2) menentukan penyebab ketidaksesuaian; dan
      3) menentukan apakah ada ketidaksesuaian serupa atau berpotensi terjadi kembali.
   c) melaksanakan tindakan apapun yang diperlukan;
   d) mereviu efektivitas tindakan korektif apapun yang diambil; dan
   e) membuat perubahan pada keamanan informasi, jika diperlukan tindakan korektif harus sesuai dengan efek dari ketidaksesuaian yang ditemui.
9. Dinas harus menyimpan informasi terdokumentasi sebagai bukti dari:
   a) sifat ketidaksesuaian dan tindakan berikutnya yang diambil; dan
   b) hasil dari setiap tindakan korektif.

BAB III
KEBIJAKAN KEAMANAN INFORMASI

A. Dokumen Kebijakan Keamanan Informasi.

Dokumen kebijakan keamanan informasi harus mendapatkan persetujuan dari Bupati. Dokumen tersebut harus dipublikasikan dan dikomunikasikan kepada seluruh pegawai dan pihak eksternal terkait. Dokumen kebijakan keamanan informasi tersebut termasuk prinsip, kebijakan, prosedur dan standar teknis keamanan.

B. Review..

B. Review Kebijakan Keamanan Informasi.

Kebijakan keamanan informasi harus direview secara kontinu dan sistematis. Review tersebut akan digunakan untuk perbaikan kebijakan keamanan informasi. Review ters ebut dilakukan oleh (*Chief Information Security Officer*/CISO) dan disampaikan ke Komite Keamanan Informasi (KKI) untuk mendapatkan persetujuan revisi bila diperlukan. Proses review tersebut harus mendapatkan dukungan dari Daerah.

BAB IV
TANGGUNG JAWAB KEAMANAN INFORMASI

Tanggung jawab keamanan informasi memuat organisasi berserta tanggung jawab masing-masing bagian dalam organisasi tersebut. Bagian ini terbagi menjadi:

1. Pengorganisasian keamanan informasi (*Chief Information Security Officer*/CISO);
2. Tanggungjawab penanggungjawab utama keamanan informasi;
3. Tanggung jawab komite keamanan informasi; Tanggung jawab kepala perangkat daerah atau pejabat eselon II;
4. Tanggungjawab pelaksana keamanan informasi; dan
5. Proses reviu independen.

A. Pengorganisasian Keamanan Informasi Organisasi (*Chief Information Security Officer*/CISO).

Keamanan informasi di lingkungan pemerintah daerah terdiri dari:

1. Penanggung jawab eksekutif (*Goverment Chief Information Officer*/GCIO) yang dipimpin oleh Sekretaris Daerah bertanggung jawab menentukan prinsip, aksioma dan kebijakan keamanan informasi, menjamin ketersediaan, keakuratan, ketepatan dan keamanan informasi yang dibutuhkan oleh organisasi untuk mencapai tujuan organisasi serta mendapatkan laporan dari GCISO, komite risiko dan komite audit untuk memastikan prinsip, aksioma, kebijakan dan pelaksanaan keamanan informasi diterapkan.
2. Penanggung jawab utama keamanan informasi (*Goverment Chief Information Security Officer*/GCISO) yang dijabat oleh Kepala Dinas Komunikasi, Informatika, Statistik dan Persandian Kabupaten Rote Ndao yang bertanggung jawab atas aspek keamanan informasi di daerah.
3. Komite Keamanan Informasi (KKI) yang dipimpin oleh GCISO dan anggotanya yang meliputi semua Kepala Perangkat Daerah. KKI merupakan komite yang dibentuk untuk membahas dan memutuskan sejumlah aspek yang terkait dengan keamanan dalam pengembangan, implementasi, pengoperasian, monitoring, pemeliharaan dan peningkatan tata kelola keamanan informasi daerah.
4. Manajer keamanan informasi yang dijabat oleh kepala bidang persandian yang bertanggung jawab atas aspek pengelolaan keamanan informasi, keamanan fasilitas fisik dan non fisik dalam organisasi.

5. Bagian..

5. Bagian operasi dan administrasi keamanan informasi yang tugaskan kepada staf bidang persandian yang bertanggung jawab untuk mengelola pelaksanaan keamanan informasi sesuai dengan arahan yang telah ditetapkan.
6. Pemilik aset informasi yang ditugaskan kepada seluruh Asisten, Kepala Perangkat Daerah, kelurahan termasuk BUMD yang bertanggung jawab dalam mengimplementasikan tata kelola keamanan informasi pada informasi yang dimilikinya.
7. Bagian manajemen fasilitas yang ditugaskan kepada perangkat daerah yang bertanggung jawab dalam mengelola fasilitas fisik (perangkat keras infrastruktur) agar sesuai dengan kebijakan keamanan informasi.
8. Bagian penjaga keamanan fasilitas yang ditugaskan kepada perangkat daerah masing-masing yang bertanggung jawab dalam menjaga keamanan fasilitas fisik organisasi.
9. Bagian kepatuhan keamanan informasi yang ditugaskan kepada pejabat eselon III pada perangkat daerah masing-masing yang bertanggung jawab dalam memastikan teknologi yang diterapkan telah sesuai dengan kebijakan, standar teknis, prosedur dan arsitektur organisasi.
10. Pelaksana keamanan informasi yang ditugaskan kepada pejabat dan pegawai serta pihak eksternal yang mengakses aset informasi atau memberikan layanan aset informasi kepada daerah, merupakan pelaksanan keamanan informasi, sehingga bertanggung jawab untuk mengimplementasikan tata kelola keamanan informasi sesuai dengan tugas dan fungsi masing-masing.
11. Peninjauan independen yang ditugaskan kepada tim auditor dari BSSN untuk bertanggung jawab dalam melakukan peninjauan independen atas tata kelola keamanan informasi. Mencakup peninjauan implementasi kebijakan, pedoman dan prosedur keamanan informasi untuk menjamin efektivitas Pegawai ASN.

B. Kepemimpinan dan Komitmen Penanggung Jawab Eksekutif.
Penanggung Jawab Eksekutif (*Goverment Chief Information Officer*/GCIO) dan Penanggung Jawab Utama Keamanan Informasi (*Goverment Chief Information Security Officer*/GCISO) harus menunjukkan kepemimpinan dan komitmen terkait keamanan informasi dengan cara:
1. memastikan kebijakan dan sasaran keamanan informasi ditetapkan dan selaras dengan arah strategis daerah;
2. memastikan persyaratan keamanan informasi terintegrasi ke dalam proses organisasi;
3. memastikan tersedianya sumber daya yang dibutuhkan untuk pelaksanaan keamanan informasi;
4. mengomunikasikan pentingnya manajemen keamanan informasi yang efektif dan sesuai dengan persyaratan keamanan informasi;
5. memastikan bahwa pelaksanaan keamanan informasi mencapai manfaat yang diharapkan;
6. memberikan arahan dan dukungan kepada personel agar berkontribusi untuk efektivitas pelaksanaan keamanan informasi;

7. mempromosikan..

7. mempromosikan perbaikan berkelanjutan; dan
8. mendukung peran manajemen yang relevan lainnya untuk menunjukkan kepemimpinannya ketika diterapkan pada wilayah tanggung jawabnya.

C. Tanggung Jawab Penanggung Jawab Eksekutif (*Goverment Chief Information Officer*/GCIO)

Penanggung Jawab Eksekutif bertanggung jawab memberikan arahan strategis keamanan informasi. Penanggung Jawab Eksekutif mempunyai peran sebagai berikut:

1. memberikan dukungan terhadap keamanan informasi;
2. mereview dan menyetujui prinsip dan aksioma keamanan informasi;
3. menyetujui anggaran keamanan informasi; dan
4. menerima dan menindaklanjuti laporan manajemen terkait keamanan informasi.

D. Tanggung Jawab Komite Keamanan Informasi (KKI)

KKI merupakan komite yang dibentuk untuk membahas dan memutuskan sejumlah aspek yang terkait dengan pengembangan, implementasi, pengoperasian, monitoring, pemeliharaan dan peningkatan tata kelola keamanan informasi. Mekanisme koordinasi dalam KKI dilakukan melalui pertemuan tatap muka secara berkala atau melalui media komunikasi lain seperti email atau sosial media internal daerah. Komite Keamanan Informasi mempunyai peran sebagai berikut:

1. melakukan revisi kebijakan keamanan informasi yang disampaikan oleh GCISO dan disahkan oleh Bupati;
2. membahas dan memutuskan pelaksanaan reviu independen atas kebijakan keamanan informasi;
3. menyepakati klasifikasi aset informasi daerah yang selanjutnya disahkan oleh Bupati; dan
4. menyepakati sanksi yang akan dikenakan apabila terjadi pelanggaran.

E. Tanggung Jawab Penanggung Jawab Utama Keamanan Informasi (Goverment Chief Information Security Officer/ GCISO).

GCISO bertanggung jawab membantu GCIO dalam memimpin pengelolaan keamanan informasi di lingkungan pemerintah daerah. GCISO mempunyai peran sebagai berikut:

1. melakukan perencanaan, pengembangan, implementasi, pengoperasian, monitoring, pemeliharaan dan peningkatan tata kelola keamanan informasi;
2. melakukan peninjauan manajemen atas kebijakan keamanan informasi secara berkala;
3. menyampaikan usulan revisi kebijakan keamanan informasi, untuk selanjutnya dibahas oleh KKI sebelum mendapat persetujuan dan pengesahan Bupati;
4. memberikan masukan atas sanksi yang akan diberikan kepada setiap pelanggaran keamanan informasi;
5. melakukan publikasi dan sosialisasi kendali risiko keamanan informasi kepada perangkat daerah, kelurahan dan pihak eksternal pemerintah daerah; dan
6. memberikan masukan dan melakukan koordinasi dengan GCIO dalam pengelolaan akses aset informasi daerah.

F. Tanggung Jawab..

F. Tanggung Jawab Manajer Keamanan Informasi.

Manajer keamanan informasi bertanggung jawab untuk mengelola keamanan informasi dan keamanan non fisik dalam organisasi. Manajer keamanan informasi mempunyai peran sebagai berikut:

a. mendefinisikan standar teknis dan non teknis, prosedur dan panduan keamanan informasi;
b. membantu inspektorat dan komite keamanan informasi dalam mendefinisikan dan mengimplementasikan kendali, proses dan perangkat-perangkat pendukung supaya mematuhi kebijakan serta mengelola resiko keamanan informasi;
c. mereviu dan memonitor kepatuhan terhadap kebijakan dan berkontribusi pada proses audit internal dan penilaian mandiri/ *Control Self Assesment* (CSA);
d. mengumpulkan, menganalisa dan memberikan saran terkait metrik keamanan informasi dan insiden;
e. mendukung Inspektorat dalam melakukan penyelidikan dan remediasi insiden keamanan informasi atau pelanggaran kebijakan lainnya;
f. mengorganisasi kampanye kesadaran keamanan untuk pegawai ASN dalam meningkatkan budaya keamanan dan mengembangkan pemahaman yang luas akan persyaratan ISO/IEC 27001;
g. mengordinasi implementasi kebijakan keamanan informasi selain keamanan fasilitas fisik;
h. memastikan keberadaan dan implementasi kendali teknis, fisik dan prosedural. Salah satunya dengan memastikan kendali diterapkan dengan tepat oleh seluruh pegawai ASN. Manajer keamanan informasi memastikan:
    1) pegawai ASN diinformasikan kewajiban-kewajibannya untuk melaksanakan kebijakan keamanan informasi;
    2) pegawai ASN mematuhi kebijakan keamanan informasi dan mendukung secara aktif kendali keamanan informasi tersebut; dan
    3) pegawai ASN dimonitor untuk menilai tingkat kapatuhan terhadap kebijakan keamanan informasi dan menilai penerapan kendali-kendali keamanan informasi tersebut.
i. memberikan arahan, dukungan dan alokasi sumber daya dalam rangka memastikan perlindungan secara tepat aset-aset informasi;
j. menginformasikan manajemen keamanan informasi dan/atau Inspektorat jika ada pelanggaran kebijakan (pelanggaran yang sudah terjadi atau pelanggaran yang baru dicurigai dan berpengaruh terhadap aset pihak terkait); dan
k. melakukan evaluasi kepatuhan terhadap kebijakan melalui proses *Control Self-Assessment* (CSA) dan audit internal secara periodik.

G. Tanggung Jawab Manajer Keamanan.

Manajer keamanan bertanggung jawab untuk mengelola keamanan fasilitas fisik dan non fisik dalam organisasi. Manajer Keamanan mempunyai peran sebagai berikut:

1. melakukan implementasi dan manajemen akses kontrol fisik dan non fisik pada masing-masing fasilitas organisasi;
2. melakukan implementasi dan penjagaan kendali lingkungan yang tepat untuk memastikan terdapat lingkungan yang sesuai dengan kebijakan keamanan informasi;

3. mengelola..

3. mengelola dan memelihara fasilitas fisik sesuai dengan kebijakan keamanan informasi;
4. memberikan otorisasi akses ke area aman organisasi;
5. memastikan fasilitas fisik dan perlengkapan yang ada di dalamnya terlindung dari gangguan catu daya dan gangguan fisik lainnya;
6. mengelola fasilitas fisik dan non fisik agar sesuai dengan kebijakan keamanan informasi; dan
7. memastikan semua peralatan dan perlengkapan fisik pendukung dilakukan pengesetan sesuai keamanan informasi.

H. Tanggung Jawab Bagian Operasi dan Administrasi Keamanan Informasi.
Bagian operasi dan administrasi bertanggung jawab mengelola pelaksanaan keamanan informasi sesuai dengan arahan yang telah ditetapkan. Bagian operasi dan administrasi keamanan informasi mempunyai peran sebagai berikut:
1. mengidentifikasi infrastruktur yang memiliki risiko tinggi, menilai kerentanannnya dan melakukan tindakan yang tepat dalam mengendalikan risiko pada tingkat operasional;
2. manajemen kejadian keamanan informasi yang dihasilkan oleh semua perangkat operasional teknologi informasi; dan
3. manajemen insiden keamanan informasi yang akan menyebabkan kerusakan atau mengancam keamanan informasi.

I. Tanggung Jawab Pemilik Aset Informasi.
Pemilik Aset Informasi bertanggung jawab untuk mengimplementasikan tata kelola keamanan informasi pada informasi yang dimilikinya. Pemilik aset informasi mempunyai peran sebagai berikut:
a. melakukan proses klasifikasi dan perlindungan aset informasi secara tepat;
b. menentukan dan memberikan pendanaan pada kendali protektif yang sesuai;
c. memberikan hak akses pada aset informasi yang sesuai dengan klasifikasi dan kebutuhan organisasi;
d. melakukan atau memberikan kuasa kepada pihak ketiga terkait proses penilaian resiko keamanan informasi untuk memastikan kebutuhan keamanan informasi didefinisikan dan didokumentasi secara tepat;
e. memastikan proses peninjauan akses sistem/data diselesaikan tepat waktu; dan
f. memantau kepatuhan kebijakan keamanan informasi yang akan berpengaruh terhadap aset informasi daerah.

J. TanggungJawab Bagian Manajemen Fasilitas
Bagian manajemen fasilitas bertanggung jawab dalam mengelola fasilitas fisik agar sesuai dengan kebijakan keamanan informasi. Bagian manajemen fasilitas mempunyai peran sebagai berikut:
1. melakukan perencanaan pengembangan fasilitas yang memperhatikan aspek kenyamanan dan memastikan pelaksanaannya sesuai dengan perencanaan tersebut;
2. menyediakan fasilitas fisik dalam pelaksanaan kebijakan keamanan informasi;

3. menyediakan..

3. menyediakan fasilitas keamanan yang mendukung tugas operasional petugas keamanan; dan
4. melakukan pemeliharaan terhadap fasilitas listrik, saluran air, *air-conditioning*, kabel telekomunikasi agar terhindar dari kondisi yang dapat membahayakan orang, data dan informasi yang ada di dalam gedung dan fasilitas itu sendiri.

K. Tanggung Jawab Bagian Penjaga Keamanan.

Bagian penjaga keamanan bertanggung jawab dalam menjaga keamanan fasilitas fisik organisasi. Bagian penjaga keamanan mempunyai peran sebagai berikut:

1. memberikan perlindungan bagi gedung, fasilitas, pegawai, tamu, pihak-pihak yang berkepentingan, kegiatan kriminal dan penyusupan;
2. melakukan kegiatan pencegahan dengan cara melakukan pengawasan keamanan untuk mencegah terjadinya kejadian-kejadian yang dapat membahayakan semua orang dalam area yang dapat menyebabkan kerusakan gedung dan fasilitas terkait;
3. merespon dengan segera setiap ada alarm tanda bahaya diaktifkan;
4. melaporkan segala aktivitas pengamanan kepada atasan dan melaporkan segala aktivitas basil pengamatan yang mencurigakan tetapi di luar kewenangannya kepada aset;
5. melakukan pemeriksaan kepada setiap orang dan barang yang masuk ke area perkantoran; dan
6. melakukan pencatatan semua orang yang masuk dan keluar area.

L. Tanggung Jawab Bagian Kepatuhan Keamanan Informasi.

Bagian kepatuhan keamanan informasi bertanggung jawab memastikan teknologi yang diterapkan telah sesuai dengan kebijakan, standar teknis, prosedur dan arsitektur organisasi. Bagian kepatuhan keamanan informasi mempunyai peran sebagai berikut:

1. memantau penerapan teknologi agar bisa dipastikan selaras dengan kebijakan organisasi;
2. melakukan peninjauan dan menilai keamanan informasi secara periodik;
3. mengidentifikasi dan merekomendasikan tindakan terhadap pelanggaran agar tetap sesuai dengan kebijakan organisasi; dan
4. merekomendasikan suatu cara paling efisien dan efektif untuk manajemen keamanan informasi dan implementasinya dalam organisasi.

M. Tanggung Jawab Pelaksana Keamanan Informasi.

Pelaksana keamanan informasi bertanggung jawab untuk mengimplementasikan tata kelola keamanan informasi. Pelaksana keamanan informasi mempunyai peran sebagai berikut:

1. melindungi kerahasiaan, integritas dan ketersediaan aset informasi yang menjadi wewenang dan tanggung jawabnya masing-masing dengan memperhatikan klasifikasi informasi dan mematuhi kebijakan, pedoman dan prosedur keamanan informasi;
2. mengimplementasikan keamanan informasi sesuai dengan bagian masing-masing; dan
3. melaporkan setiap insiden atau pelanggaran keamanan informasi kepada GCISO.

N. Reviu..

N. Reviu Independen.

Reviu independen terhadap tata kelola keamanan informasi dilakukan secara berkala atau sewaktu-waktu jika diperlukan. Peninjauan tersebut mencakup peninjauan implementasi kebijakan, pedoman dan prosedur keamanan informasi. Peninjauan independen dapat dilakukan oleh tim auditor BSSN atau pihak independen lain yang ditunjuk sesuai kebijakan keamanan informasi.

BAB V
MANAJEMEN RISIKO KEAMANAN INFORMASI

A. Ruang Lingkup dan Tujuan.

1. Ruang lingkup manajemen risiko meliputi:
   a) identifikasi risiko;
   b) analisa dan evaluasi risiko;
   c) identifikasi dan evaluasi aset penanganan risiko;
   d) persetujuan pimpinan atas manajemen risiko; dan
   e) pernyataan pelaksanaan manajemen risiko.
2. Manajemen risiko bertujuan untuk:
   a) mendukung tata kelola keamanan informasi;
   b) kepatuhan terhadap ISO/IEC 27001;
   c) persiapan *business continuity plan*;
   d) persiapan *incident response plan*; dan
   e) penyusunan persyaratan keamanan informasi.

B. Kebijakan Manajemen Risiko Keamanan Informasi.

Manajemen risiko terdiri dari beberapa tahapan yaitu pembentukan konteks, identifikasi risiko, analisa dan evaluasi risiko, identifikasi evaluasi aset penanganan risiko, persetujuan pimpinan dan pernyataan penerapan manajemen keamanan informasi. Kebijakan pada masing-masing tahapan tersebut adalah:

1. Pembentukan konteks yaitu:
   a) menentukan lingkup dan batasan manajemen risiko sesuai dengan operasi, struktur, lokasi, aset dan teknologi yang ada di daerah; dan
   b) merupakan kriteria yang akan digunakan untuk mengevaluasi risiko keamanan informasi di daerah.
2. Identifikasi risiko yaitu:
   a) identifikasi aset informasi sesuai dengan lingkup manajemen risiko dan pemilik dari aset tersebut;
   b) identifikasi ancaman atas aset informasi tersebut;
   c) identifikasi kerentanan sebagai hasil ancaman tersebut; dan
   d) identifikasi dampak dari hilangnya kerahasiaan, integritas dan ketersediaan serta indepedensi yang mungkin terjadi atas aset informasi tersebut.
3. Analisis dan evaluasi risiko yaitu:
   a) perkiraan dampak yang diterima oleh daerah jika terjadi suatu kegagalan keamanan informasi, termasuk juga konsekuensi atas hilangnya kerahasiaan, integritas dan ketersediaan informasi;
   b) perkiraan kemungkinan munculnya kegagalan keamanan akibat adanya ancaman, kerentanan dan dampak yang berkaitan dengan aset informasi tersebut dan pengendalian yang dilakukan saat ini;

c) perkiraan..

c) perkiraan tingkatan untuk setiap risiko; dan
d) menentukan apakah risiko dapat diterima atau memerlukan tindakan lebih lanjut menggunakan kriteria risiko yang wajar yang telah ditetapkan.

4. Identifikasi dan evaluasi alternatif penanganan risiko yaitu:
   a) melakukan pengendalian yang memadai atas risiko tersebut;
   b) menerima risiko tersebut sesuai dengan kebijakan daerah;
   c) menghindari risiko tersebut; dan
   d) memilih tujuan dan rancangan pengendalian sebagai bentuk penanganan risiko, yang didasarkan kepada standar diantaranya sesuai SNI ISO/IEC 27001:2009, ISO/IEC 27005:2008, PP60/2008 SPIP dan standar lain sesuai perkembangan.
5. Persetujuan pimpinan yaitu:
   a) persetujuan dari pimpinan daerah atas hasil analisa risiko keamanan informasi dan rencana mitigasi risiko; dan
   b) otorisasi pimpinan daerah untuk menerapkan dan melaksanakan manajemen risiko keamanan informasi.
6. Pernyataan penerapan manajemen keamanan informasi meliputi:
   a) tujuan pengendalian dan rancangan pengendalian yang dipilih serta alasan pemilihan pengendalian tersebut;
   b) tujuan pengendalian dan rancangan pengendalian yang dilaksanakan saat ini; dan
   c) pengecualian untuk setiap tujuan pengendalian dan rancangan pengendalian dari standar yang akan disertifikasi serta alasan pengecualiannya.

BAB VI
KLASIFIKASI INFORMASI

A. Ruang Lingkup dan Tujuan.
   1. Ruang lingkup informasi yang dimaksud yaitu keseluruhan informasi yang dimiliki oleh pemerintah daerah.
   2. Tujuan klasifikasi informasi yaitu untuk memastikan informasi yang dimiliki daerah mendapatkan tingkat pengamanan yang sesuai.

B. Kebijakan Klasifikasi Informasi.
   Kebijakan klasifikasi informasi dibagi dalam dua bentuk yaitu:
   1. bentuk non-elektronik yaitu kode klasifikasi diberikan pada lembar disposisi atau lembar kendali dokumen atau pada dokumen itu sendiri pada sisi kanan atas.
   2. bentuk elektronik yaitu kode klasifikasi diberikan pada bagian awal dari nama file atau pada bagian tertentu dari properties file tersebut. Untuk email kode klasifikasi diberikan pada subjek email.

   Dua bentuk informasi tersebut diklasifikasikan berdasarkan tiga kriteria keamanan yaitu kerahasiaan, integritas dan ketersediaan.

   Berikut klasifikasi pada masing masing kriteria adalah:

   a. Kerahasiaan
      1) informasi publik (disimbolkan dengan angka "0");
      2) informasi terbatas (disimbolkan dengan angka "1");
      3) informasi rahasia (disimbolkan dengan angka "2"); dan
      4) informasi sangat rahasia (disimbolkan dengan angka ""S").

b. Integritas..

b. Integritas.

Integritas diklasifikasikan menjadi dua yaitu:

1) informasi tidak harus selalu lengkap dan akurat (disimbolkan dengan angka "0"); dan
2) informasi harus selalu lengkap dan akurat (disimbolkan dengan angka "1").

c. Ketersediaan.

Ketersediaan diklasifikasikan menjadi dua yaitu:

1) informasi dengan mudah dapat disediakan Kembali (disimbolkan dengan angka "0"); dan
2) informasi sulit untuk disediakan kembali (disimbolkan dengan angka" 1").

BAB VII
PENGELOLAAN HAK AKSES

A. Ruang Lingkup dan Tujuan.

1. Ruang lingkup pengelolaan hak akses yaitu akses fisik maupun lojik terhadap informasi elektronik maupun non-elektronik oleh pihak internal maupun eksternal.
2. Tujuan pengelolaan hak akses yaitu untuk mengendalikan akses terhadap informasi yang dimiliki daerah sehingga informasi hanya bisa diakses oleh pihak yang berwenang saja.

B. Kebijakan Pengelolaan Hak Akses.

Pengelolaan hak akses dibagi tiga yaitu pemberian hak akses atas informasi, pemberian hak akses kepada pihak eksternal, pengendalian akses jaringan dan sistem operasi. Berikut kebijakan pada masing-masing bagian tersebut, yaitu:

1. Pemberian Hak Akses Atas Informasi.

Pemberian hak akses atas informasi dilakukan dengan tata cara umum sebagai berikut:

a) pihak-pihak yang membutuhkan akses terhadap suatu informasi mengajukan permohonan hak akses kepada pemilik informasi secara tertulis;
b) pemilik informasi harus memastikan bahwa pihak-pihak pengguna yang membutuhkan akses terhadap informasi telah menandatangani perjanjian kerahasiaan sesuai dengan ketentuan yang ada;
c) untuk informasi yang berbentuk non-elektronik, persetujuan diberikan oleh pemilik informasi untuk disampaikan kepada pengguna sebagai pemberitahuan; dan
d) untuk informasi yang berbentuk non-elektronik, persetujuan diberikan oleh pemilik informasi untuk disampaikan kepada pengguna sebagai pemberitahuan serta di tindaklanjuti pemberian hak akses kepada pengguna terhadap informasi yang diminta secara elektronik.

Pengelola informasi menindaklanjuti pemberian hak akses informasi dengan ketentuan sebagai berikut:

a) memberikan..

a) memberikan atau membuka akses apabila seluruh pedoman sudah dipenuhi, serta berhak untuk membatasi hak akses dari setiap pengguna sesuai dengan kebutuhan yang telah ditentukan dan sesuai dengan perizinan yang diberikan oleh pemilik informasi;
b) menjaga catatan pengelolaan hak akses serta memastikan bahwa pihak-pihak yang memiliki hak akses istimewa telah dikendalikan dengan memadai;
c) memverifikasi pemberian password baru, password pengganti dan password sementara, memastikan bahwa pengguna hak akses telah menerima password yang diberikan dan password dari vendor selama proses pemasangan sistem dan/atau piranti lunak harus segera diganti; dan
d) melakukan peninjauan secara periodik terhadap hak akses informasi, termasuk pemeriksaan tingkatan akses yang diberikan dan penghapusan atau pemblokiran terhadap kelebihan penerbitan hak akses dan harus segera merubah atau memblokir hak akses apabila pengguna pindahjabatan ataupun pindah kerja/keluar dari daerah.

Setelah hak akses diberikan, setiap pemilik hak akses informasi elektronik (*user ID dan password*) wajib:

a) mengganti password segera setelah menerima hak atas akses informasi dengan segera mengubah *password* sementara ketika pertama log-in;
b) menjaga kerahasiaan *password* dengan tidak menuliskan *password* pada kertas, komputer, dan/atau media lain yang tidak dilindungi dan mudah dibaca oleh pihak yang tidak berkepentingan;
c) mengubah *password* dengan segera apabila terdapat indikasi mencurigakan atau masalah pada sistem;
d) menggunakan password dengan kriteria: mudah dihafal, tidak mudah ditebak orang lain, menggunakan kombinasi angka, huruf kecil, tanda baca dan huruf besar;
e) mengganti *password* secara berkala, untuk *password* akun tertentu (akun khusus atau akun yang kritikal) harus lebih sering diganti dan tidak menggunakan kembali *password* yang pernah digunakan; dan
f) menggunakan *password* dinas yang berbeda dengan *password* untuk kebutuhan pribadi (contohnya membedakan email/surat elektronik pribadi dengan email/surat elektronik kantor).

2. Pemberian hak akses kepada pihak eksternal.

Pemilik informasi sebagai pihak yang memberikan izin atas permintaan akses informasi kepada pihak eksternal harus memperhatikan hal-hal sebagai berikut:

a) permohonan tertulis pihak eksternal atas setiap jenis informasi yang akan diakses dan fasilitas pegawai ASN;
b) akses fisik, akses lojik oleh pengguna dan sambungan jaringan antara daerah dengan pihak eksternal, baik akses *on-site* dan *off-site* maupun *remote-site*;
c) klasifikasi keamanan informasi dengan mempertimbangkan nilai, sensitifitas informasi dan tingkat risiko di daerah;

d) pihak..

d) pihak-pihak eksternal lain yang terlibat dalam penanganan aset informasi di daerah dan pengendalian yang diperlukan untuk melindungi informasi yang tidak boleh diakses oleh pihak eksternal;
e) perbedaan pemahaman dan pengendalian yang dilakukan pihak eksternal dalam hal penyimpanan, pemrosesan, komunikasi, pertukaran dan perubahan informasi; dan
f) dampak hak akses tidak tersedia bagi pihak eksternal saat dibutuhkan atau dampak kesalahan informasi yang diterima oleh pihak eksternal.

3. Pengendalian Akses Jaringan dan Sistem Operasi.

Pengendalian akses jaringan dan sistem operasi bertujuan untuk:

a) mengendalikan akses ke jaringan data dan layanan yang ada pada jaringan data. Pengendalian tersebut dengan menetapkan kriteria yang harus dipenuhi, pihak yang diperbolehkan mengakses jaringan data, serta jaringan/layanan jaringan yang bisa diakses;
b) memperoleh kepastian mengenai sumber sambungan jaringan dengan mengotentifikasi pengguna sambungan jaringan tersebut. Pengendalian otentifikasi tambahan dapat diimplementasikan untuk pengendalian akses melalui jaringan lain;
c) menggunakan peralatan akses jaringan khusus yang hanya dapat digunakan bersama dengan teknik tertentu. Peralatan tersebut harus dapat mengidentifikasi jaringan yang mendapatkan izin untuk diakses dan harus selalu memastikan keamanan peralatan tersebut;
d) menetapkan domain jaringan berdasarkan pada penilaian risiko dan tingkat kebutuhan keamanan untuk setiap domain;
e) memastikan bahwa penggunaan jaringan selalu dipantau, dibatasi atau dilarang untuk tujuan tertentu. Tujuan tertentu yang dimaksud antara lain email pribadi, pemindahan data yang tidak ada kaitannya dengan kegiatan di daerah, akses interaktif dan aplikasi interaktif yang dapat memindahkan data ketempat lain;
f) memastikan bahwa penggunaan jaringan bersama, khususnya yang keluar dari pemerintah daerah telah memiliki pengendalian tambahan terutama jika terdapat jaringan yang dapat digunakan bersama dengan pihak ketiga (pengguna diluar pemerintah daerah);
g) berkaitan dengan pengelolaan komputer pengguna harus dipastikan bahwa:
    1) disetiap komputer pengguna telah menampilkan peringatan bahwa komputer hanya dapat diakses oleh pihak yang mempunyai otorisasi;
    2) komputer pengguna tidak memperlihatkan karakter untuk *password* yang sedang dimasukkan pada saat *log-on*;
    3) komputer pengguna tidak menampilkan sistem atau aplikasi sampai proses *log-on* benar-benar selesai; dan
    4) layar komputer harus bersih pada saat istirahat (*time-out*). Aplikasi harus ditutup setelah jangka waktu tertentu apabila tidak digunakan.
h) berkaitan dengan pengelolaan akun dan *password*, harus dipastikan bahwa:

1. seluruh..

1. seluruh pegawai ASN/pengguna selalu menggunakan user id dan password untuk menjaga akuntabilitas informasi. Pengendalian "*unique identifier*" (user id) berlaku pada seluruh jenis pengguna sistem informasi di daerah;
2. user id selalu digunakan sehingga aktivitas pengguna dan fungsi dapat dilacak, dibatasi dan dikendalikan;
3. kepentingan pribadi atau diluar kegiatan pemerintah daerah tidak diperbolehkan menggunakan akun yang sama dengan akun untuk kegiatan Pemerintah daerah;
4. pada keadaan tertentu penggunaan id bersama untuk grup atau pekerjaan tertentu diperbolehkan setelah mendapatkan persetujuan manajer keamanan informasi;
5. terdapat rekaman pengguna, penggunaan *password* serta catatan penggunaan *password* yang sama dan atau berulang;
6. penyimpanan *password* para pengguna di tempat atau sistem terpisah dari data sistem aplikasi, serta terlindung pada saat pembuatan, penyimpanan dan pengirimannya;
7. setiap pengguna diwajibkan untuk menggunakan pedoman identifikasi, otentifikasi dan otorisasi dalam menggunakan utilitas sistem operasi. Penggunaan utilitas sistem operasi dibatasi dan harus terdapat rekaman/log dari seluruh penggunaannya;
8. seluruh akun yang sudah tidak digunakan harus dihapus/dibuang/dinon-aktifkan;
9. terdapat batas minimum dan maksimum waktu penggunaan akses pada sistem informasi di daerah;
10. penggunaan sambungan jaringan hanya pada jam kerja dan jika tidak ada surat perintah untuk lembur atau perpanjangan waktu kerja, maka sambungan ke jaringan harus segera diputus.

i) memastikan penggunaan fasilitas *mobile* komputer dan alat komunikasi untuk kepentingan pribadi tidak diizinkan;

j) menentukan peralatan komunikasi yang tepat dan dapat digunakan di daerah, termasuk metode pengamanan akses jarak jauh, serta piranti lunak dan piranti keras pendukungnya; dan

k) seluruh pegawai ASN/pengguna disarankan untuk tidak meninggalkan seluruh piranti mobile komputer dan alat komunikasi tanpa mendapat penjagaan dan perhatian seperti di mobil, kamar hotel dan tempat rapat.

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, serta penggunaan teknologi kriptografi dalam pengolahan dan penyimpanan informasi di lingkungan pemerintah daerah.

B. Kebijakan Kriptografi

Kebijakan kriptografi meliputi:

1. Kontrol..

1. Kontrol kriptografi digunakan untuk menjamin kerahasiaan dan integritas dari informasi sensitif di lingkungan perangkat daerah;
2. Kontrol kriptografi mencakup namun tidak terbatas pada:
   a) enkripsi informasi dan jaringan komunikasi;
   b) pemeriksaan integritas informasi;
   c) otentikasi identitas; dan
   d) tanda tangan elektronik.
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; dan
7. Pengelolaan dari kunci kriptografi didasarkan pada prinsip pengawasan ganda untuk mengurangi risiko penyalahgunaan.

BAB IX
PENGENDALIAN FISIK DAN LINGKUNGAN

A. Ruang Lingkup dan Tujuan
   1. Ruang lingkup fisik dan lingkungan meliputi wilayah kerja dan peralatan kerja.
      a. Pengamanan wilayah kerja termasuk batasan keamanan fisik, pengendalian akes fisik, keamanan kantor, ruangan dan fasilitas, perlindungan terhadap ancaman dari lingkungan eksternal, area akses publik, pengantaran dan penerimaan, aktivitas pekerjaan di area rahasia; dan
      b. Pengamanan peralatan kerja termasuk penempatan peralatan dan perlindungannya, fasilitas pendukung, keamanan instalasi kabel, pemeliharaan peralatan, keamanan peralatan yang berada di luar lingkungan pemerintah daerah, keamanan penghapusan dan penggunaan ulang peralatan atau media informasi dan pemindahan aset informasi.
   2. Tujuan pengendalian fisik dan lingkungan adalah untuk:
      a) menghindari terjadinya akses fisik secara ilegal, penghancuran atau campur tangan dari pihak lain terhadap aset informasi di lingkungan pemerintah daerah; dan
      b) menghindari terjadinya kehilangan, kerusakan, pencurian, persekongkolan terhadap aset dan informasi, serta gangguan lainnya akibat aktivitas yang dilakukan oleh pemerintah daerah.

B. Kebijakan Pengendalian dan Keamanan Wilayah Kerja.
   1. Kebijakan pengendalian wilayah kaerja meliputi:
      a. Pengendalian akses fisik
         Pengendalian akses fisik dilakukan dengan cara:

1) mencatat..

1) mencatat setiap tamu yang datang;
2) mengawasi setiap tamu yang datang;
3) memberikan hak akses hanya sebatas keperluan tamu tersebut;
4) menginformasikan syarat-syarat keamanan dan pedoman yang harus diikuti selama berada di lingkungan pemerintah daerah;
5) memberikan kartu identitas selama berada di daerah untuk seluruh pegawai ASN, kontraktor dan pengguna eksternal; dan
6) reviu terhadap izin pemberian hak akses ke wilayah kerja yang di dalamnya terdapat informasi dan fasilitas pengolahnya atau jika diperlukan, merekomendasikan untuk menghapus hak akses tersebut.

2. Keamanan Wilayah Kerja.
   a. Kemanan wilayah kerja yang meliputi: kantor, ruangan dan fasilitas kantor dilakukan dengan cara:
      1) menempatkan dan menyimpan secara aman fasilitas utama pengolah informasi dan fasilitas lainnya;
      2) menempatkan gedung/wilayah kerja yang sensitif dilokasi yang tidak mudah terlihat dan hanya memberikan izin masuk secara terbatas untuk tujuan-tujuan tertentu; dan
      3) antisipasi atas kemungkinan terjadinya akses secara umum terhadap buku petunjuk dan buku telpon internal yang berisi informasi yang sensitif beserta fasilitas pegawai ASN.
   b. Perlindungan terhadap ancaman dari lingkungan eksterna dilakukan dengan cara:
      1) meletakan dan menyimpan benda-benda yang berbahaya pada jarak yang cukup aman dari wilayah kerja yang di dalamnya terdapat aset informasi dan fasilitas pengolahnya;
      2) menyediakan dan menempatkan peralatan pemadam kebakaran di setiap lokasi/wilayah kerja yang memerlukan penjagaan khusus; dan
      3) menyimpan media back-up pada jarak yang cukup aman untuk menghindari kerusakan akibat bencana alam atau bencana sosial.
   c. Area akses publik, pengantaran dan penerimaan.
      Keamanan area akses publik, pengantaran dan penerimaan dilakukan dengan cara:
      1) membatasi hak akses untuk wilayah pengantaran dan penerimaan barang dari luar pemerintah daerah;
      2) merancang wilayah pengantaran dan penerimaan barang sehingga persediaan/peralatan dapat ditempatkan atau dipindahkan ke bagian lain tanpa melibatkan kurir eksternal pemerintah daerah;
      3) melakukan pemeriksaan terhadap barang-barang yang akan dimasukkan ke lingkungan pemerintah daerah di tempat pengantaran dan penerimaan barang sebelum barang-barang tersebut dialokasikan ke unit-unit pemerintah daerah; dan
      4) mendaftarkan barang-barang yang masuk ke pemerintah daerah.
   d. Aktivitas pekerjaan di area rahasia.
      Keamanan aktivitas pekerjaan di area rahasia dilakukan dengan:
      a) memastikan bahwa setiap orang yang bekerja di wilayah yang di dalamnya terdapat informasi yang sensitif dan fasilitas pegawai ASN harus mengerti dan tahu bahwa tempat di mana ia beraktivitas adalah wilayah yang harus dijaga keamanannya;

b) harus..

b) harus melakukan antisipasi untuk pekerjaan yang tidak terpantau;
c) mengamankan wilayah-wilayah kerja yang belum digunakan dengan cara dikunci secara fisik dan harus diperiksa secara rutin; dan
d) melarang masuknya alat dengan kemampuan merekam ke dalam wilayah-wilayah kerja tertentu, kecuali telah ada izin sebelumnya.

C. Kebijakan Pengamanan Peralatan Kerja.

1. Penempatan peralatan dan perlindungannya dilakukan dengan:
   a) menempatkan semua peralatan sesuai dengan tempatnya;
   b) melindungi peralatan yang digunakan untuk mengolah informasi yang bersifat sensitif, menempatkan fasilitas pengolah informasi yang menangani data yang sensitif sedemikian rupa sehingga pada saat aplikasi digunakan, informasi yang ada di layar tidak dapat dilihat oleh orang yang tidak berkepentingan;
   c) menempatkan jenis peralatan yang membutuhkan perlindungan secara khusus di tempat yang khusus juga;
   d) melakukan pengendalian untuk meminimalisir risiko ancaman fisik yang potensial seperti: pencurian, kebakaran, ledakan bom, asap, banjir, efek zat kimia dan gangguan komunikasi;
   e) menyediakan penangkal petir untuk setiap gedung di lingkungan pemerintah daerah dan menyesuaikannya untuk seluruh jalur komunikasi dan tenaga listrik yang digunakan;
   f) melakukan pengawasan untuk mendeteksi kondisi lingkungan, seperti suhu dan kelembaban, yang bisa mempengaruhi berfungsinya fasilitas pengolah informasi; dan
   g) membuat peraturan untuk aktivitas makan, minum dan merokok di wilayah yang dekat dengan fasilitas pengolah informasi.

   Keamanan fasilitas pendukung dilakukan dengan:
   a) memastikan jumlah seluruh fasilitas pendukung (seperti air, listrik, pemanas dan ventilasi) telah mencukupi untuk kebutuhan di seluruh lingkungan pemerintah daerah;
   b) memastikan jumlah bahan bakar telah tersedia dan mencukupi untuk generator jika terjadi pemadaman listrik;
   c) menyiapkan penerangan darurat untuk mengantisipasi terjadinya pemadaman listrik;
   d) memeriksa secara rutin semua peralatan UPS dan generator untuk memastikan kecukupan kapasitas yang diperlukan oleh pemerintah daerah;
   e) meletakan tombol listrik darurat di dekat pintu keluar darurat di ruang peralatan untuk mengantisipasi keadaan darurat;
   f) memastikan bahwa persediaan air telah cukup dan stabil untuk memfasilitasi pendingin ruangan, kelembaban dan sistem pemadam kebakaran;
   g) memeriksa ulang dan jika diperlukan, memasang kembali sistem alarm untuk mendeteksi kegagalan fungsi pada fasilitas pendukung; dan

h) memastikan..

h) memastikan peralatan telekomunikasi harus disambungkan dengan penyedia jasa fasilitas setidaknya dengan dua sambungan/jalur yang berbeda untuk mengantisipasi jika terjadi kerusakan pada salah satu sambungan/jalur.

3. Keamanan instalasi kabel dilakukan dengan:
   a) menempatkan sambungan listrik dan telefon yang berhubungan dengan fasilitas pemrosesan informasi di bawah tanah atau tempat lain yang aman sebagai alternatif perlindungan;
   b) melindungi jaringan kabel dari pemotongan ilegal dan kerusakan;
   c) melakukan pengidentifikasian kabel dan penandaan peralatan secara jelas untuk meminimalisir kesalahan penanganan;
   d) melakukan pencatatan untuk daftar pemotongan kabel dengan tujuan mengurangi kemungkinan terjadinya kesalahan;
   e) melakukan instalasi untuk saluran lapis baja dan mangan atau kotak yang terkunci pada titik pemeriksaan dan pemberhentian;
   f) menggunakan media alternatif dan atau media pengiriman yang menyediakan keamanan yang memadai;
   g) menggunakan instalasi kabel dengan fiber optik;
   h) menggunakan pelindung elektromagnetik untuk melindungi kabel;
   i) melakukan teknik penghapusan dan pemeriksaan fisik untuk media ilegal yang di sambung ke kabel; dan
   j) melakukan pengendalian akses fisik untuk panel sambungan dan ruang kabel.
4. Keamanan pemeliharaan peralatan dilakukan dengan:
   a) melakukan perawatan secara rutin untuk semua peralatan milik pemerintah daerah sesuai dengan pentunjuk pemeliharaan dengan memperhatikan spesifikasi peralatan tersebut;
   b) membuat catatan mengenai dugaan kesalahan, pencegahan dan pemeliharaan terhadap peralatan pemerintah daerah; dan
   c) melakukan pengendalian terhadap perawatan yang telah dilaksanakan.
5. Keamanan peralatan yang berada di luar lingkungan pemerintah daerah dilakukan dengan:
   a) melakukan pelarangan untuk membawa keluar dari lingkungan pemerintah daerah setiap bentuk peralatan atau media yang berisi informasi atau fasilitas pengolah informasi tanpa pengawasan yang memadai kecuali peralatan mobile dengan prosedur khusus; dan
   b) melakukan peninjauan secara rutin terhadap petunjuk pemeliharaan untuk setiap peralatan sesuai dengan spesifikasinya.
6. Keamanan penghapusan dan penggunaan ulang peralatan atau media informasi dilakukan dengan:
   a) menghancurkan dan menghapuskan setiap benda atau media informasi yang sensitif jika ia tidak akan digunakan lagi;
   b) menggunakan/memilih metode penghapusan yang khusus agar informasi yang terdapat di dalamnya tidak dapat dilacak kembali; dan
   c) melakukan penilaian risiko untuk media yang rusak tetapi berisi informasi sensitif untuk menentukan apakah media tersebut akan dihancurkan seluruhnya atau diperbaiki kembali.

7. Keamanan..

7. Keamanan pemindahan aset informasi dilakukan dengan:
   a) memastikan bahwa seluruh aset informasi seperti peralatan, dokumen, software tidak dipindahkan tanpa izin;
   b) menentukan siapa saja pihak-pihak yang berhak melakukan pemindahan aset informasi dan memberikan izin atas pemindahan aset informasi tersebut; dan
   c) menetapkan batas waktu peminjaman atau pemindahan peralatan dan melakukan pengecekan atas pengembalian peralatan tersebut serta melakukan pencatatan waktu peminjaman atau pemindahan dan pengembalian peralatan tersebut.

BAB X
PENGENDALIAN ASPEK SUMBER DAYA MANUSIA

A. Ruang Lingkup dan Tujuan.
   1. Ruang lingkup pengendalian aspek sumber daya manusia meliputi: proses pemeriksaan dan verifikasi latar belakang calon pegawai, sosialisasi peran dan tanggung jawab dalam keamanan informasi termasuk perjanjian kerahasiaan, pendidikan dan pelatihan peningkatan keamanan informasi, dan perubahan dan/atau penghapusan hak akses informasi serta pengembalian aset informasi jika ada pemberhentian, perubahan, atau berakhirnya perjanjian kerja.
   2. Tujuan pengendalian aspek sumber daya manusia adalah untuk:
      1) memastikan bahwa seluruh pegawai ASN memahami peran dan tanggung jawab mereka terhadap keamanan informasi untuk mengurangi risiko terjadinya pencurian, kecurangan dan penyalahgunaan aset informasi dan fasilitas pengolahnya;
      2) memastikan bahwa seluruh pegawai ASN waspada terhadap ancaman keamanan informasi sehingga mereka sadar akan peran dan tanggungjawab mereka untuk mengurangi risiko terjadinya insiden karena faktor kelalaian manusia; dan
      3) memastikan bahwa proses pemberhentian atau perubahan Pegawai ASN dilakukan dengan cara yang benar.

B. Kebijakan Pengendalian Aspek Sumber Daya Manusia.
   Pengendalian aspek sumber daya manusia meliputi:
   1) proses pemeriksaan dan verifikasi latar belakang;
   2) sosialisasi peran dan tanggang jawab dalam keamanan informasi;
   3) perjanjian kerahasiaan;
   4) pendidikan dan pelatihan peningkatan keamanan informasi;
   5) pengembalian aset informasi; dan
   6) perubahan dan/atau penghapusan hak akses informasi.

   a. Proses pemeriksaan dan verifikasi latar belakang yaitu:
      1) melakukan proses verifikasi dan pemeriksaan mengenai latar belakang untuk semua calon pegawai ASN untuk memastikan bahwa latar belakang mereka telah memenuhi persyaratan sesuai peraturan perundang-undangan dan etika, serta sesuai dengan persyaratan yang ditetapkan oleh pemerintah daerah;

2). Proses..

2) Proses pemeriksaan dan verifikasi latar belakang harus meliputi informasi-informasi berikut:
   a) keterangan mengenai karakter yang dimiliki baik secara individu maupun organisasi;
   b) keterangan mengenai daftar riwayat hidup yang lengkap;
   c) konfirmasi mengenai kualifikasi pendidikan dan akademis;
   d) keterangan mengenai kompetensi;
   e) keterangan mengenai catatan kriminal (jika ada); dan
   f) kegiatan dalam dunia maya termasuk kegiatan membobol sistem keamanan komputer untuk tujuan kejahatan/ *cracking*.

b. Sosialisasi peran dan tanggung jawab dalam keamanan informasi, antara lain:
   1) memberikan arahan yang memadai kepada pegawai ASN, mengenai peran dan tanggung jawab mereka terhadap keamanan informasi sebelum hak akses diberikan kepada mereka; dan
   2) memotivasi pegawai ASN agar memiliki kesadaran akan peran dan tanggung jawab mereka terhadap keamanan informasi sehingga dapat memenuhi semua kebijakan keamanan informasi di lingkungan pemerintah daerah.

c. Perjanjian kerahasiaan yaitu:
   1) memastikan bahwa seluruh pegawai ASN menyetujui peran dan tanggung jawab keamanan informasi yang diberikan kepada mereka dengan menandatangani surat perjanjian yang menyatakan kesanggupan menjaga kerahasiaan dan larangan penyingkapan untuk jenis aset informasi yang bersifat sensitif bagi pemerintah daerah;
   2) seluruh pegawai ASN setiap tahun harus menandatangani perjanjian kerahasiaan sebagai bagian dari perjanjian kerja pegawai;
   3) memastikan bahwa seluruh rekanan penyedia barang dan jasa di daerah telah menyetujui peran dan tanggung jawab keamanan informasi yang diberikan kepada mereka dengan menandatangani surat perjanjian yang menyatakan kesanggupan menjaga kerahasiaan dan larangan penyingkapan untuk jenis aset informasi yang bersifat sensitif bagi pemerintah daerah;
   4) memastikan bahwa seluruh komisi dan instansi yang menjadi rekan kerja pemerintah daerah telah menyetujui peran dan tanggung jawab keamanan informasi yang diberikan kepada mereka dengan menandatangani surat perjanjian yang menyatakan kesanggupan menjaga kerahasiaan dan larangan penyingkapan untuk jenis aset informasi yang bersifat sensitif bagi pemerintah daerah dan yang dilarang menurut peraturan perundang-undangan yang berlaku;
   5) Hal-hal yang harus diperhatikan dalam perjanjian kerahasiaan antara lain adalah sebagai berikut:
      a) setiap butir perjanjian yang disetujui tidak mengandung kesalahpahaman dan pemerintah daerah mendapat jaminannya dan sesuai dengan kebijakan keamanan informasi yang berlaku;

b) pedoman..

b) pedoman perlindungan informasi dan mekanisme serta pengendalian atas perlindungan fisik yang dibutuhkan termasuk pengendalian untuk memastikan perlindungan dari penyalahgunaan aplikasi;
c) pengendalian untuk memastikan pengembalian atau penghancuran aset informasi yang penting dan rahasia pada saat berakhirnya perjanjian;
d) kerahasiaan, keintegritasan dan ketersediaan terhadap hak kekayaan intelektual, hak cipta dan pembatasan untuk penggandaan serta penyingkapan informasi;
e) struktur pelaporan yang jelas dan format pelaporan yang telah disetujui mengenai keamanan informasi, termasuk pengaturan untuk masalah-masalah perubahan yangjelas dan spesifik;
f) perbedaan alasan, persyaratan dan keuntungan yang didapat dan dibutuhkan oleh pihak-pihak yang memiliki hak akses atas informasi;
g) persyaratan untuk mengurus daftar personil yang diizinkan menggunakan jasa layanan yang tersedia, termasuk juga hak khusus mereka dalam hal penggunaan dan pernyataan bahwa seluruh akses yang tidak memiliki persetujuan adalah dilarang;
h) pengaturan mengenai pelaporan, pengumuman dan penyelidikan atas kasus keamanan informasi dan pelanggaran keamanan, termasukjuga pelanggaran atas persyaratan;
i) hak untuk mengawasi, mencabut dan semua aktivitas yang bersinggungan dengan aset informasi daerah termasuk proses untuk mencabut hak akses atau memotong sambungan antara dua sistem;
j) hak untuk mengaudit semua bentuk tanggung jawab yang telah ditetapkan dalam perjanjian, di mana audit dilakukan oleh pihak ketiga, dan mengakumulasikan hak dasar bagi para auditor; dan
k) keterlibatan pihak ketiga dengan sub kontraktor dan implementasi dari pengendalian keamanan terhadap sub kontraktor termasuk rencana antisipasi untuk kemungkinan terjadinya/timbulnya keinginan dari pihak ketiga untuk mengakhiri perjanjian sebelum waktunya, apabila dokumentasi terakhir/terbaru mengenai daftar aset, lisensi, perjanjian atau hak yang berhubungan dengan pihak ketiga, termasuk negosiasi ulang untuk suatu perjanjian jika persyaratan keamanan di lingkungan pemerintah daerah berubah.

d. Pendidikan dan pelatihan peningkatan keamanan informasi yaitu:
1) merancang dan memberikan pendidikan dan pelatihan di seluruh lingkungan pemerintah daerah secara rutin dengan tujuan membangun kesadaran akan keamanan informasi;
2) mengenali masalah-masalah keamanan informasi dan kasus-kasus yang mungkin terjadi; dan
3) mengantisipasi adanya perubahan dalam kebijakan atau pedoman yang berlaku.

e. Pengembalian aset informasi yaitu:

1). memastikan..

1) memastikan bahwa setiap perjanjian kerja untuk pegawail ASN yang dibuat telah mencakup ketentuan mengenai tanggung jawab dan tugas yang terkait dengan keamanan informasi yang harus diselesaikan sesaat setelah pemberhentian/ perubahan dilakukan;
2) jika seorang pegawai ASN yang akan memasuki tahap pemberhentian/perubahan penugasan memiliki informasi atau pengetahuan yang cukup banyak dan penting bagi keperluan dan tujuan pemerintah daerah, harus dipastikan bahwa informasi dan pengetahuan itu telah didokumentasikan dan disampaikan kepada pemerintah daerah secara lengkap dan jelas;
3) pada proses pemberhentian, perubahan atau berakhirnya masa perjanjian, harus dipastikan bahwa setiap pegawai ASN telah mengembalikan seluruh aset informasi yang selama ini menjadi kewenangannya kepada pemerintah daerah dengan memindahkan setiap aset informasi dari media pribadi ke media milik pemerintah daerah atau dengan menghapuskannya dari media pribadi tersebut.

f. Perubahan dan/atau penghapusan hak akses yaitu:
1) memastikan bahwa semua hak akses yang dimiliki oleh pegawai ASN telah dihapuskan sesaat setelah pemberhentian, perubahan atau berakhirnya perjanjian kerja;
2) hak akses yang harus dihapuskan meliputi: akses fisik, akses logis, kunci, kartu identitas, fasilitas pengolah informasi dan lain-lain;
3) penghapusan hak akses sesaat sebelum memasuki pemberhentian atau perubahan penugasan dilakukan dengan memperhatikan hal-hal berikut:
   a. inisiatif dan alasan dilakukannya pemberhentian atau perubahan;
   b. tanggungjawab terakhir atau terkini dari pegawai ASN; dan
   c. nilai dari aset informasi terkini yang dapat diakses oleh pegawai ASN.
4) melakukan antisipasi bagi pegawai ASN, kontraktor dan pihak pengguna yang merasa tidak puas dengan pemberhentian tersebut dan mungkin melakukan pencurian aset informasi yang penting dan sensitif; dan
5) melakukan tindakan pengarahan kepada kelompok yang masih memiliki hak akses terhadap aset informasi untuk tidak lagi berbagi informasi kepada pegawai yang sudah tidak memiliki hak akses karena adanya pemberhentian atau perubahan penugasan untuk hak akses secara kelompok.

BAB XI
PENGAMANAN PENGEMBANGAN DAN PEMELIHARAAN SISTEM INFORMASI

A. Ruang Lingkup dan Tujuan
1. Ruang lingkup pengamanan pengembangan dan pemeliharaan sistem operasi yaitu pertimbangan keamanan dalam pengembangan dan pemeliharaan, pengendalian aplikasi, penggunaan enkripsi, pengamanan kode sumber, file sistem dan data pengujian, manajemen perubahan, pengendalian kebocoran informasi dan kelemahan teknikal.
2. Tujuan pengamanan pengembangan dan pemeliharaaan sistem informasi yaitu untuk memastikan keamanan menjadi bagian integral dari sistem informasi.

B. Kebijakan..

B. Kebijakan Pengamanan Pengembangan dan Pemeliharaan Sistem Informasi

Pengamanan pengembangan dan pemeliharaan sistem informasi terdiri dari beberapa kebijakan yaitu pertimbangan keamanan dalam pengembangan dan pemeliharaan, pengendalian aplikasi, penggunaan enkripsi, pengamanan kode sumber, file sistem dan data pengujian, manajemen perubahan, pengendalian kebocoran informasi dan kelemahan teknikal.

1. Pertimbangan Keamanan dalam Pengembangan dan Pemeliharaan.

Dalam pengembangan dan pemeliharaan, pertimbangan yang harus diperhatikan, antara lain:

a) nilai aset informasi dan kemungkinan gangguan terhadap aktivitas pemerintah daerah karena kegagalan sistem informasi;
b) integrasi sistem dengan sistem yang dimiliki pemerintah daerah;
c) kriteria keamanan dalam kontrak dengan vendor;
d) penilaian risiko terhadap produk yang tidak memenuhi persyaratan keamanan yang diperlukan dan menentukan kendali alternatif untuk meminimalkan risiko;
e) reviu keamanan pada fitur-fitur tambahan apabila dapat meningkatkan risiko keamanan informasi maka fitur tersebut sebaiknya tidak digunakan; dan
f) evaluasi keamanan oleh pihak ketiga apabila diperlukan.

2. Pengendalian Aplikasi.

Aplikasi yang ada di pemerintah daerah harus memiliki pengendalian memadai, minimal mampu melakukan validasi data masukan, validasi pemrosesan dan validasi data keluaran. Validasi tersebut dilakukan dengan menerapkan hal-hal berikut yaitu:

a) pemeriksaan data masukan, data referensi (nama, alamat, nomor referensi) dan parameter lainnya, termasuk dokumen sumber data masukan dari perubahan yang tidak diotorisasi;
b) pemeriksaan secara berkala terhadap isi atribut data dan kumpulan data untuk menegaskan validasi dan integritas data;
c) pedoman khusus dalam menghadapi kesalahan validasi (apabila terjadi kesalahan) serta pengujian kewajaran data masukan;
d) penetapan tanggung-jawab untuk setiap pegawai/personil yang terlibat dalam proses pemasukan data;
e) pencatatan/perekaman seluruh kegiatan proses pemasukan data;
f) penggunaan pengujian dan validasi secara otomatis yang digunakan untuk mengurangi risiko kesalahan dalam memasukkan data dan mencegah peretasan, kelebihan kapasitas dan eksploitasi yang disebabkan oleh pemrosesan data yang tidak valid;
g) perancangan dan implementasi aplikasi diharuskan dapat meminimalisasi risiko kesalahan dalam pemrosesan informasi;
h) program aplikasi yang digunakan beroperasi dengan benar pada waktu yang telah ditentukan dan jika terjadi kesalahan maka pemrosesan berikutnya segera dihentikan; dan
i) validasi hasil keluaran yang meliputi pengujian kewajaran data keluaran, tanggung-jawab untuk setiap pegawai/personil yang terlibat dalam pemrosesan data keluaran dan catatan atas aktivitas proses validasi data keluaran.

3. Penggunaan.

3. Penggunaan Enkripsi.

Pada pengembangan aplikasi, informasi yang ada di aplikasi pemerintah daerah harus disandi sesuai dengan tingkatan klasifikasi keamanan informasi dan kunci enkripsi telah dikelola dengan baik sesuai dengan peraturan perundang-undangan, dengan melaksanakan hal-hal sebagai berikut:

a) menerapkan enkripsi pada informasi yang sensitif/kritikal baik selama penyimpanan maupun pemindahan untuk memastikan kerahasiaan;
b) menggunakan tanda tangan digital atau kode otentifikasi pada pesan yang sensitif/kritikal baik selama penyimpanan maupun pemindahan untuk memastikan integritas/otentifikasi; dan
c) menggunakan teknik kriptografi untuk membuktikan terjadi atau tidaknya suatu kejadian atau tindakan untuk memastikan non repudiasi.

4. Pengamanan kode sumber, file sistem, dan data pengujian pengamanan dengan memastikan bahwa:

a) kode sumber aplikasi, file-file sistem dan data pengujian aplikasi telah dikendalikan dengan baik;
b) instalasi atas aplikasi hanya dilakukan oleh pihak yang berhak, sesuai pedoman; dan
c) perubahan atas berbagai paket aplikasi harus diminimalisir dan dikendalikan dengan baik, antara lain dengan melaksanakan hal berikut:
   1) penggunaan sistem operasi dengan kode yang sah;
   2) pemutakhiran piranti lunak, aplikasi dan program dilakukan oleh pegawai yang terlatih dan telah mendapat otorisasi;
   3) analisa risiko terkait apabila menggunakan piranti lunak yang tidak mendapat dukungan/bantuan pelayanan dari vendor;
   4) memastikan vendor yang menyuplai piranti lunak dapat membantu apabila dibutuhkan dan aktivitas pemeliharaan oleh vendor tersebut harus senantiasa dipantau;
   5) pengujian piranti lunak atau aplikasi harus dilakukan dan strategi pengembalian data harus dapat dilakukan sebelum mengubah sistem yang telah diimplementasikan;
   6) pedoman yang digunakan dalam sistem aplikasi pada lingkungan operasional juga diterapkan pada lingkungan pengujian sistem aplikasi dan harus dilakukan pemisahaan otorisasi setiap informasi operasi yang diduplikat ke sistem pengujian aplikasi serta informasi mengenai data pengujian harus segera dihapuskan setelah pengujian selesai dilakukan;
   7) penjagaan data kode sumber secara ketat dan kode sumber tersebut tidak boleh berada dalam lingkungan operasional;
   8) pembatasan akses pegawai pendukung/tambahan/sementara pada bagian sistem informasi terhadap kumpulan data kode sumber;
   9) pemeliharaan, penduplikasian, pemutakhiran kumpulan kode sumber dan dokumen terkait, yang hanya bisa dilakukan setelah mendapatkan otorisasi dari petugas yang berwenang; dan
   10) pemeliharaan rekaman hasil pemeriksaan/audit yang berhubungan dengan akses kumpulan program sumber.

5. Manajemen..

5. Manajemen Perubahan.

Keamanan dalam manajemen perubahan dilakukan dengan beberapa hal berikut:

a) persetujuan resmi harus dilakukan sebelum pelaksanaan perubahan dan penjagaan dokumen persetujuan perubahan dari pihak yang terkait;
b) pemberitahuan harus dilakukan ketika akan ada perubahan sehingga dapat direviu dan diuji sebelumnya dan perubahan tersebut dimasukkan dalam rencana keberlangsungan pemerintah daerah;
c) pemilihan waktu yang tepat dalam perubahan sehingga tidak menggangu operasi;
d) perubahan dokumentasi pendukung ketika diperlukan dan apabila dilakukan perubahan dokumentasi pendukung, dokumentasi sebelumnya harus segera ditarik atau dimusnahkan;
e) perjanjian lisensi piranti lunak, perjanjian penjaminan dengan pihak lain dalam hal terjadi kegagalan/kebangkrutan pihak luar, penjaminan kualitas dan keamanan piranti lunak;

6. Pengendalian Kebocoran Informasi dan Kelemahan Teknikal.

Pengendalian kebocoran informasi dan kelemahan teknikal dilakukan dengan beberapa hal berikut:

a) penetapan kelompok atau perorangan yang bertanggung-jawab untuk memantau kelemahan-kelemahan yang ada pada seluruh sistem informasi pemerintah daerah termasuk mengamati media dan komunikasi yang berada diluar area pemerintah daerah untuk menghindari informasi yang terselubung, memantau secara berkala terhadap pegawai ASN maupun aktivitas sistem, memantau penggunaan sumber daya yang ada pada sistem komputer, melakukan pencegahan penggunaan jaringan akses yang tidak terotorisasi untuk melacak saluran terselubung / tersembunyi;
b) Pengelolaan informasi spesifik yang sangat dibutuhkan dalam membantu mengatasi penyerangan, termasuk daftar vendor piranti lunak, nomor versi piranti lunak, daftar instalasi piranti lunak ke sistem yang ada dan orang yang bertanggung-jawab terhadap piranti lunak tersebut; dan
c) Penetapan peranan dan tanggung jawab monitoring serangan, penilaian risiko terhadap serangan, penutupan celah dan pembaharuan piranti lunak yang ada.

BAB XII
PENGAMANAN OPERASIONAL SISTEM INFORMASI

A. Ruang Lingkup dan Tujuan

1. Ruang lingkup pengamanan operasional sistem informasi adalah dokumentasi pedoman operasi, proses pemisahan tugas, pengawasan penggunaan sistem informasi, manajemen back-up, pengelolaan keamanan jaringan, pengelolaan layanan jasa pihak ketiga, perencanaan dan perizinan sistem, perlindungan untuk kode-kode berbahaya, penanganan media, proses pertukaran informasi, pengelolaan pesan elektronik, transaksi elektronik dan informasi yang tersedia untuk umum.

2. Tujuan..

2. Tujuan pengamanan operasional sistem informasi adalah memberikan panduan pelaksanaan pengendalian keamanan informasi dalam kegiatan operasional sistem informasi dan komunikasi.

B. Kebijakan Pengamanan Operasional Sistem Informasi

Pengamanan operasional sistem informasi dibagi tiga belas yaitu pendokumentasian pedoman operasi, pemisahan tugas, pengawasan penggunaan sistem informasi, manajemen *back-up*, pengelolaan keamanan jaringan, pengelolaan layanan jasa pihak ketiga, perencanaan dan perizinan sistem, perlindungan untuk kode-kode berbahaya, penanganan media, pertukaran informasi, pesan elektronik dan transaksi elektronik, informasi yang tersedia untuk umum. Berikut kebijakan pada masing-masing bagian tersebut.

1. Pendokumentasian pedoman operasi yaitu:
   a) memastikan bahwa seluruh pedoman untuk berbagai aktivitas yang berhubungan dengan pengolahan informasi dan fasilitas komunikasi telah terdokumentasi dengan baik dan diberlakukan dengan resmi;
   b) melakukan koordinasi dengan tim bantuan/help desk jika terjadi kondisi yang tidak diharapkan atau mengalami kesulitan teknis;
   c) menyusun perintah kerja untuk hal-hal berikut:
      1) pengolahan dan penanganan informasi di pusat pengolahan data;
      2) proses cadangan/ *back-up* di pusat pengolahan data;
      3) persyaratan penjadwalan pekerjaan, langkah awal kerja, dan jangka waktu penyelesaian pekerjaan di pusat pengolahan data; dan
      4) penanganan kesalahan atau kondisi lain yang tidak diharapkan yang mungkin muncul saat pelaksanaan tugas, termasuk pembatasan untuk penggunaan fasilitas sistem di pusat pengolahan data.
   d) melakukan penyimpanan untuk dokumentasi sistem secara aman, memperhatikan daftar akses untuk dokumentasi sistem dan persetujuan pemilik aplikasi, dan melindungi sistem pendokumentasian yang diselenggarakan atau disediakan oleh jaringan publik secara memadai.
2. Pemisahan tugas.

   Untuk mengurangi risiko terjadinya penyalahgunaan sistem informasi, baik yang disengaja maupun tidak disengaja, harus dilakukan proses pemisahan tugas. Pemisahan tugas tersebut antara lain pemisahan antara pelaksana dan pemberi izin. Jika pemisahan tugas terjadi kesulitan, maka bentuk pengendalian yang lain seperti pengawasan, *log* dan supervisi dari atasan. Proses pemisahan tugas meliputi:
   a) memastikan setiap pengguna informasi hanya dapat melakukan akses dan modifikasi terhadap informasi setelah memperoleh otorisasi formal dan diawasi oleh pihak yang menjadi pemilik informasi;
   b) memastikan telah terdapat pemisahan antara wilayah pengembangan, pengujian dan operasional sistem informasi di pemerintah daerah, dengan melaksanakan hal-hal sebagai berikut:

1) memastikan..

1) memastikan bahwa lingkungan pengembangan aplikasi dan lingkungan operasional aplikasi berada pada sistem atau komputer yang berbeda dan pada domain atau direktori yang berbeda. Lingkungan pengujian sistem dengan lingkungan operasional sistem sedapat mungkin serupa/tidak berbeda;
2) menetapkan pedoman tata cara pemindahan aplikasi dari lingkungan pengembangan ke lingkungan operasional;
3) membatasi akses terhadap bahasa pemrograman/*compiler*, *editor*, atau alat pengembangan lainnya melalui lingkungan sistem operasional jika tidak terlalu dibutuhkan;
4) melakukan proses pembedaaan profil pengguna pada saat pengujian sistem dan pada saat pelaksanaan sistem informasi di Pemerintah Kabupaten Rote Ndao;
5) menyediakan menu yang memberikan petunjuk penggunaan yang memadai untuk mengurangi risiko kesalahan pada seluruh aplikasi yang ada di Pemerintah Kabupaten Rote Ndao; dan
6) memastikan bahwa tidak terjadi penyalinan data yang sensitif pada lingkungan pengujian sistem.

3. Pengawasan penggunaan sistem informasi yakni:
   a. menentukan tingkat pengawasan yang diperlukan untuk setiap fasilitas pengolahan informasi yang digunakan oleh setiap individu dan memastikan bahwa setiap aktivitas pengawasan yang dilakukan telah sesuai dengan persyaratan hukum yang berlaku;
   b. membuat audit *log* yang meliputi hal-hal berikut:
      1) rekaman user ID, identitas terminal dan lokasi jika memungkinkan, serta alamat dan protokol jaringan;
      2) rekaman tanggal dan waktu *log-on* atau *log-off*, baik yang sukses maupun ditolak;
      3) rekaman daftar percobaan akses ke data atau perangkat sistem informasi yang sukses atau ditolak;
      4) rekaman perubahan pada konfigurasi sistem;
      5) catatan penggunaan secara istimewa/khusus termasuk penggunaan sistem utilitas dan aplikasi;
      6) catatan pengaktifan dan pe-non-aktifan sistem perlindungan; dan
      7) informasi tentang gagal atau suksesnya suatu peristiwa/kondisi yang dilakukan oleh administrator dan operator system informasi.
   c. Proses pengelolaan catatan yang merekam segala aktifitas suatu aplikasi yang dijalankan/*log* harus melakukan dan mempertimbangkan hal-hal berikut:
      1) menghindari perubahan pada tipe pesan yang dicatat;
      2) menghindari pengeditan atau penghapusan pada berbagai *log*;
      3) menghindari kelebihan kapasitas penyimpanan untuk *log file* yang dapat menyebabkan kegagalan pada pencatatan peristiwa atau kelebihan penulisan pada catatan peristiwa; dan
      4) keperluan pengumpulan bukti.

4. Manajemen back-up.

   Untuk memelihara integritas dan ketersediaan informasi dapat membuat cadangan/*back-up* penyedia informasi dan fasilitas pemrosesan informasi. Manajemen *back-up* meliputi hal-hal sebagai berikut:

a) manajemen..

a) manajemen *back-up* untuk sistem yang kritis bagi tujuan pemerintah daerah harus meliputi seluruh sistem informasi, aplikasi dan data yang penting sehingga bisa mendapatkan hasil pemulihan yang lengkap jika terjadi bencana;
b) memastikan bahwa cakupan dan frekuensi *back-up* yang dilakukan telah mewakili persyaratan operasional, persyaratan keamanan informasi terkait dan tingkat risiko tinggi untuk keberlangsungan operasional pemerintah daerah;
c) menyediakan fasilitas back-up yang memadai untuk menjamin bahwa seluruh informasi dan aplikasi dapat kembali lagi jika terjadi bencana atau kegagalan fungsi. Rekaman back-up harus lengkap dan akurat untuk setiap salinan *back-up*;
d) menyimpan hasil *back-up* di lokasi yang jauh, sesuai dengan jarak yang cukup aman untuk menghindari kerusakan jika terjadi bencana di lingkungan pemerintah daerah. Selain itu pemerintah daerah harus memberikan perlindungan fisik dan menyediakan lingkungan yang memadai untuk *back-up* informasi sesuai dengan standar;
e) melakukan pemeriksaan terhadap media *back-up* untuk menjamin bahwa media *back-up* bisa dimanfaatkan dalam keadaan darurat. Ketika kerahasiaan menjadi sangat penting, perlu membuat perlindungan *back-up* dengan menggunakan metode enkripsi; dan
f) melakukan pemeriksaan dan pengujian secara rutin terhadap pedoman penyimpanan untuk menjamin bahwa pedoman tersebut efektif dan bisa dilengkapi sesuai dengan waktu yang dinyatakan dalam pedoman operasional pemulihan.

5. Pengelolaan keamanan informasi yakni:
a) menjamin adanya perlindungan atas jaringan komunikasi informasi dan perlindungan atas infrastruktur pendukungnya serta tersedianya fasilitas jaringan komunikasi cadangan;
b) memisahkan antara pelaksana operasional jaringan dengan pelaksana operasional komputer;
c) melakukan pengendalian khusus untuk menjamin keamanan atas kerahasiaan dan integritas data yang melalui wilayah jaringan publik atau jaringan nirkabel, dan untuk melindungi sistem dan aplikasi yang *online*;
d) melakukan pengendalian khusus untuk memelihara ketersediaan layanan jaringan dan sambungan komputer;
e) memastikan bahwa penyedia jasa layanan jaringan memiliki kemampuan untuk mengatur layanan sesuai yang telah disepakati secara aman dan dilakukan pengawasan secara rutin;
f) memastikan bahwa penyedia jasa layanan jaringan telah melaksanakan aturan keamanan jaringan dengan memperhatikan keistimewaan keamanan dan tingkat pelayanan yang diberikan, dan sesuai dengan persyaratan Pemerintah Kabupaten Rote Ndao; dan
g) memperhatikan persyaratan keamanan dalam pengelolaan penyedia jasa jaringan sebagai berikut:
   1) tersedianya teknologi yang digunakan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi, dan pengendalian sambungan jaringan;

2) tersedianya..

2) tersedianya batasan teknis yang diperlukan untuk sambungan yang aman dengan layanan jasa jaringan yang sesuai dengan peraturan keamanan dan sambungan jaringan; dan
3) tersedianya pedoman yang digunakan untuk penggunaan layanan jasa jaringan dalam membatasi akses ke jaringan atau aplikasi.

6. Pengelolaan layanan jasa pihak ketiga yakni:
   a) menjamin pelaksanaan layanan dari pihak ketiga yang terkait dengan operasional sistem informasi dan komunikasi telah mempertimbangkan aspek keamanan informasi serta telah diawasi secara memadai dan berbagai perubahan telah memperoleh persetujuan yang memadai;
   b) memastikan bahwa perjanjian yang dilakukan dengan pihak ketiga yang memberikan layanan jasa harus meliputi persetujuan untuk melaksanakan keamanan, mendefinisikan bentuk jasa yang diberikan, dan aspek-aspek manajemen jasa yang diberikan;
   c) untuk kondisi *outsourcing*, harus dipastikan rencana transisi informasi dan fasilitas pengolahnya untuk menjamin bahwa keamanan telah dilaksanakan dan dipelihara selama masa transisi;
   d) melakukan pengawasan terhadap kinerja layanan jasa yang diberikan oleh pihak ketiga untuk memastikan kesesuaiannya dengan perjanjian yang disepakati;
   e) melakukan reviu atas laporan layanan jasa yang dihasilkan oleh pihak ketiga dan mengatur rapat lanjutan untuk menindaklanjuti laporan tersebut sesuai dengan persyaratan dalam perjanjian;
   f) menyediakan informasi mengenai insiden keamanan informasi dan melakukan reviu atas informasi tersebut sesuai dengan persyaratan yang ada dalam perjanjian ataupun pedoman;
   g) melakukan reviu terhadap jejak audit pihak ketiga dan catatan insiden keamanan, permasalahan operasional, kegagalan, jejak kesalahan, dan gangguan yang berkaitan dengan layanan jasa pihak ketiga, dan menyelesaikan serta mengatur masalah-masalah yang telah teridentifikasi dari hasil tinjauan tersebut; dan
   h) menetapkan pedoman perubahan pada layanan jasa pihak ketiga, yang meliputi:
      1) peningkatan terhadap layanan jasa yang selama ini diberikan dan pengembangan terhadap setiap aplikasi dan sistem yang baru serta modifikasi dan pembaharuan terhadap kebijakan dan pedoman yang berlaku di Pemerintah Kabupaten Rote Ndao;
      2) perubahan dan peningkatan pada jaringan, penggunaan teknologi baru, dan pengadopsian produk baru atau versi terbaru dari produk yang sudah digunakan;
      3) lingkungan dan alat pengembangan yang baru, perubahan pada lokasi fisik dari fasilitas layanan jasa, dan perubahan pada vendor; dan
      4) pengendalian baru untuk mengatasi insiden keamanan informasi dan untuk memperbaiki keamanan informasi.

7. Perencanaan dan perizinan sistem yakni:
   a) memastikan bahwa persyaratan dan kriteria untuk perizinan terhadap sistem baru telah ditetapkan, disetujui, didokumentasikan, dan diujikan;

b) menentukan..

b) menentukan persyaratan kinerja dan kapasitas untuk setiap komputer yang digunakan di lingkungan Pemerintah Kabupaten Rote Ndao;
c) melakukan penyesuaian dan pengawasan terhadap sistem untuk memastikan ketersediaan dan keefektifitasan sistem tersebut;
d) melakukan pendeteksian terhadap kendali untuk mengetahui masalah-masalah yang sedang terjadi;
e) melakukan pengawasan terhadap sumber daya sistem yang paling utama, dengan memperhatikan sumber daya yang memiliki durasi/ *lead time* paling lama dan biaya paling tinggi;
f) membuat mekanisme seperti dokumentasi untuk mengantisipasi ketergantungan terhadap personil kunci yang mungkin membawa ancaman bagi keamanan sistem atau layanan jasa;
g) menyediakan solusi perbaikan untuk setiap kesalahan yang terjadi pada pelaksanaan pedoman untuk melakukan restart dan rencana cadangan/ *contingency*;
h) memiliki jaminan bahwa instalasi sistem yang baru tidak akan mempengaruhi sistem yang telah ada. Jaminan ini dapat dilihat dari adanya bukti bahwa pengaruh yang ada pada sistem baru telah dipertimbangkan dan telah diamankan oleh provider; dan
i) menyediakan pedoman pengoperasian atau penggunaan sistem yang baru bagi seluruh pegawai Pemerintah Kabupaten Rote Ndao dalam rangka mengefektifkan pedoman teknis dan menghindari terjadinya *human error*.

8. Perlindungan untuk *malicious* dan *mobile code*/kode-kode berbahaya yakni:
a) melakukan perlindungan terhadap *malicious code*/kode berbahaya yang didasarkan pada pendeteksian awal, perbaikan *software*, kesadaran keamanan, dan pengendalian manajemen perubahan dan sistem akses yang memadai;
b) melarang penggunaan *software* tidak direkomendasikan di lingkungan Pemerintah Kabupaten Rote Ndao dan melaksanakan pedoman untuk perlindungan terhadap ancaman ketika menerima *file* dan *software* dari jaringan ekstemal atau dari perantara jaringan yang lain;
c) melaksanakan *reviu* secara rutin terhadap software dan isi data dari sistem yang mendukung proses bisnis di Pemerintah Kabupaten Rote Ndao;
d) melakukan penyelidikan terhadap adanya file yang tidak direkomendasikan dan perubahan ilegal terhadap file atau informasi;
e) melakukan instalasi dan pembaharuan secara rutin terhadap pendeteksian *malicious code*/kode berbahaya dan perbaikan perangkat lunak untuk pemindaian komputer atau media lain sebagai bentuk kendali pencegahan. Hal ini harus meliputi:
1) pemeriksaan untuk setiap berkas elektronik, media optik, dan berkas yang diterima jaringan, terhadap *malicious code*/ kode berbahaya sebelum penggunaan;

2) pemeriksaan..

2) pemeriksaan email yang memiliki ikatan dan berkas yang didownload terhadap *malicious code*/kode berbahaya sebelum penggunaan. Pelaksanaannya harus dilakukan di tempat yang berbeda, seperti server, komputer, dan saat memasuki jaringan Pemerintah Kabupaten Rote Ndao; dan

3) pemeriksaan situs terhadap *malicious code*/kode berbahaya.

f) menetapkan pedoman pengelolaan dan tanggung jawab untuk mencegah *malicious code* terhadap sistem yang berjalan, pelatihan yang diperlukan, pelaporan dan perbaikan dari serangan *malicious code*;

g) menyiapkan strategi menghadapi masalah/ *Business Continuity Plan* (BCP) yang memadai untuk *recovery* dari serangan *malicious code*, termasuk semua data penting dan software back-up serta aturan pemulihan;

h) melakukan pengesahan *mobile code* hanya di lingkungan yang terbatas dan melakukan pemblokiran untuk setiap penggunaan *mobile code* ilegal;

i) melakukan pengendalian sumber daya yang tersedia untuk akses *mobile code* dan pengendalian kriptografi untuk otentifikasi *mobile code* yang unik serta mengaktifkan pengukuran teknis yang tersedia di sistem untuk memastikan *mobile code* telah diatur; dan

j) mendeteksi dan mencegah terjadinya *malicious code* yang mungkin dikirim pada saat terjadi komunikasi elektronik.

9. Penanganan Media yakni:

a) memastikan bahwa setiap media yang akan dipindah-tangankan dari Pemerintah Kabupaten Rote Ndao tidak boleh memiliki sistem pemulihan isi media tersebut. Jika diperlukan, dilakukan otorisasi bagi media yang akan dipindahkan dari Pemerintah Kabupaten Rote Ndao dan rekaman pemindahannya harus disimpan untuk memelihara bukti audit;

b) bagi informasi yang disimpan di media jika umur media tersebut lebih pendek dari umur kebutuhan informasi yang ada di dalamnya maka untuk menghindari kehilangan informasi akibat penurunan nilai media, harus dilakukan proses penyimpanan yang aman;

c) melakukan pendaftaran untuk media yang bisa dipindah-tangankan untuk membatasi kemungkinan kehilangan data. Pemindahan media sedapat mungkin hanya boleh dilakukan jika terdapat alasan yang kuat untuk melakukannya;

d) melakukan penyimpanan atau penghapusan media secara aman untuk media yang berisi informasi sensitif;

e) melaksanakan pedoman untuk mengidentifikasikan setiap jenis media yang membutuhkan penghapusan secara aman;

f) melakukan pencatatan untuk penghapusan media yang bersifat sensitif untuk memelihara bukti audit;

g) melakukan pemilihan secara selektif untuk penyedia jasa pengumpulan dan penghapusan kertas, peralatan, dan media, Pemilihan tersebut dengan mempertimbangkan pengendalian dan pengalaman yang cukup dari penyedia jasa tersebut;

h) melakukan..

h) melakukan penanganan dan penamaan seluruh media yang bisa mengindikasikan level klasifikasi. Selain itu juga dilakukan proses penyimpanan untuk media yang sesuai dengan spesifikasi masing-masing;

i) memastikan bahwa data yang diinput telah lengkap, proses yang dijalankan lengkap, dan pengesahan output telah dilaksanakan. Selain itu juga dipastikan perlindungan untuk data mentah yang memiliki nilai sensitifitas;

j) memilih dan menggunakan penyedia jasa kurir atau jasa transportasi yang terpercaya, menetapkan daftar penyedia jasa kurir yang boleh digunakan, dan mengembangkan pedoman pemeriksaan untuk setiap penyedia jasa kurir atau jasa transport yang telah dipilih;

k) melakukan proses pengepakan yang memadai untuk setiap media yang akan dikirim untuk melindungi isi dari kerusakan (suhu yang terlalu panas atau lembab, atau pengaruh elektromagnetik) selama dalam perjalanan; dan

l) melindungi informasi yang sensitif dengan pengendalian tertentu untuk menghindari terjadinya modifikasi dan penyingkapan yang ilegal, misalnya penggunaan kontainer yang terkunci, pengiriman langsung, perusakan bukti pengepakan, dan pemisahan pengiriman dengan rute yang berbeda.

10. Pertukaran informasi yakni:

a) melaksanakan pedoman untuk melindungi pertukaran informasi dari penghapusan, penyalinan, modifikasi, kesalahan alamat, dan penghancuran;

b) melindungi pertukaran informasi yang sensitif dalam bentuk ikatan / *attachment*,

c) membuat panduan untuk penggunaan informasi dan fasilitas pengolahnya bagi seluruh pengguna, termasuk juga panduan penggunaan alat komunikasi nirkabel yang memiliki risiko tinggi;

d) memastikan tidak ada kolusi antara pegawai Pemerintah Kabupaten Rote Ndao, kontraktor, dan pengguna lainnya mengenai tanggung jawab mereka terhadap keamanan informasi;

e) melaksanakan panduan untuk menyimpan atau menghapus semua bentuk korespondensi bisnis, termasuk pesan, yang berhubungan dengan hukum dan perundang-undangan lokal dan nasional;

f) dilarang meninggalkan informasi yang bersifat sensitif dan kritis di mesin printer atau mesin penjawab telepon untuk menghindari akses oleh pihak yang tidak berwenang;

g) melakukan pengendalian dan pembatasan akses untuk fasilitas komunikasi yang bisa diteruskan, misalnya email yang diteruskan ke alamat eksternal;

h) melakukan tindakan pencegahan dalam berkomunikasi, misalnya jangan memberitahu informasi sensitif ketika berbicara via telepon untuk menghindari bocornya informasi kepada orang disekitar atau orang yang menyadap;

i) tidak boleh mendaftarkan akun email yang berisi informasi pribadi ke perangkat lunak lain yang tidak berkepentingan dengan daerah;

j) dalam..

j) dalam rangka mengantisipasi terjadinya kesalahan, mesin faksimili dan foto copy yang digunakan harus memiliki media yang jika terjadi kesalahan maka pengiriman akan tetap dicetak;
k) mengumumkan pihak yang telah melakukan pengiriman dan penerimaan informasi dari dalam atau ke luar daerah; dan
l) menetapkan standar untuk teknik pengepakan dalam proses pengiriman informasi, menetapkan standar untuk identifikasi jasa kurir, serta memastikan tersedianya salinan perjanjian dan memastikan dapat dilakukannya pencarian jejak dan pengakuan dari pertukaran informasi yang terjadi.

11. Pesan elektronik dan transaksi elektronik yakni:
    a) melindungi informasi dalam bentuk pesan elektronik yang ada di daerah dari akses ilegal, modifikasi, atau layanan ilegal;
    b) memastikan tujuan dan transportasi yang benar untuk setiap pesan yang dikirim ataupun diterima daerah;
    c) memastikan reliabilitas dan ketersediaan secara umum untuk setiap pesan;
    d) memastikan keamanan pesan elektronik dengan menggunakan tanda tangan elektronik oleh setiap pihak yang terlibat dalam transaksi;
    e) memastikan komunikasi antara kedua belah pihak telah disandi dan protokol yang digunakan untuk berkomunikasi telah dilindungi; dan
    f) memastikan bahwa daerah telah mendapatkan jaminan keamanan yang terintegrasi ketika menggunakan jasa dari pihak-pihak berwenang.
12. Informasi yang tersedia untuk umum yakni:
    a) membentuk mekanisme perlindungan untuk perangkat lunak dan informasi yang dapat diakses oleh umum. Hal itu ditujukan untuk menjaga integritas perangkat lunak dan informasi tersebut;
    b) memeriksa akses sistem informasi bagi publik, untuk menghindari kelemahan dan kegagalan sebelum informasi disediakan. Pemilik informasi memberi persetujuan secara formal sebelum informasi disediakan untuk publik; dan
    c) melarang setiap pihak eksternal untuk melakukan akses ke dalam jaringan dan sistem informasi Pemerintah Kabupaten Rote Ndao jika tidak memiliki otorisasi.
13. Monitoring yakni:
    a) menjalankan monitoring sistem dan kejadian keamanan informasi. Hasil pemantauan tersebut harus terekam secara otomatis. Log operator termasuk administrator harus selalu dibuat dan log dari pengujian/*fault* harus dijalankan;
    b) membuat dan menyimpan *log* atau *audit-log* yang paling sedikit memuat:
        1) user ID;
        2) tanggal, bulan, tahun, waktu dari event utama, misalnya *log-on* dan *log-off*,
        3) identitas terminal, misalnya MAC atau IP dan letak;
        4) rekaman usaha akses sistem yang berhasil atau gagal;
        5) rekaman usaha akses data atau sumber daya yang berhasil dan gagal;

6) perubahan..

6) perubahan konfigurasi sistem;
7) pemakaian akses khusus seperti adminstrator atau *super user* atau *power-user*,
8) pemakaian aplikasi sistem dan utilitas sistem;
9) file yang diakses dan hak akses yang dipaksa;
10) alamat dan protokol jaringan;
11) alarm yang dibangkitkan sistem pengendalian akses; dan
12) aktivasi dan deaktivasi sistem proteksi, misalnya anti-virus atau *firewall* dan IDS/IPS;.

c) memonitor pemakaian/akses sistem yang meliputi:
1. akses terotorisasi, termasuk rinciannya yang meliputi:
a. nama use ID;
b. waktu dan tanggal kejadian penting;
c. jenis kejadian;
d. file-file yang diakses; dan
e. aplikasi dan/atau utilitas yang dipergunakan.
2. Semua operasi admin seperti:
a) pemakaian akun dengan kelebihan/*privilege* di atas user biasa, seperti supervisor, *root*, administrator,
b) *system start-up and stop*, dan
c) pemasangan atau pelepasan alat input/output (I/O *device*) (*attachment/detachment*).
3. Usaha akses yang gagal atau tidak terotorisasi seperti:
a) aksi user yang gagal atau ditolak;
b) aksi gagal atau ditolak yang melibatkan data atau sumber daya lain;
c) pelanggaran dan peringatan kebijakan akses jaringan dan *firewall*; dan
d) alarm dari IDS (*intrusion detection systems*)/ sistem yang memonitor trafik jaringan untuk mendeteksi aktivitas-aktivitas mencurigakan.
4. Peringatan sistem atau sistem gagal seperti:
a) peringatan atau pesan konsol/ *console alerts or messages*;
b) pengecualian log sistem/ *system log exceptions*;
c) alarm manajemen jaringan/ *network management alarms*;
d) alarm yang dinaikkan oleh sistem kontrol akses/ *alarms raised by the access control system*; dan
e) perubahan atau usaha perubahan setting dan/atau kendali keamanan sistem.

d) menentukan frekuensi reviu monitoring berdasarkan hasil analisa risiko;
e) memastikan fasilitas *logging* dan informasi *log* tidak dapat dirubah dan diakses oleh pihak yang tidak berhak; dan
f) memastikan bahwa seluruh kegiatan adminstrator sistem dan operator sistem secara otomatis merekam *log*-nya; danmenjalankan sistem pencatatan *fault* yang meliputi pencatatan otomatis, analisa dan tindak lanjut.

BAB XIII
MANAJEMEN INSIDEN KEAMANAN INFORMASI

A. Ruang Lingkup dan Tujuan

1. Ruang Lingkup

Ruang lingkup manajemen insiden keamanan informasi meliputi: pengelolaan pelaporan insiden dan penetapan penanggung jawab pelaporan insiden, penetapan pedoman pelaporan insiden, pengelolaan tindakan umpan balik dari proses pelaporan insiden dan pengelolaan tindakan pemulihan perbaikan sistem.

2 Tujuan manajemen insiden keamanan informasi adalah memberikan panduan pelaksanaan pengelolaan insiden keamanan informasi kebijakan pengamanan operasional sistem informasi.

a. Kebijakan Manajemen Insiden Keamanan Informasi

Insiden yang berkaitan dengan keamanan informasi adalah:

1) gangguan/kehilangan akses layanan, peralatan atau fasilitas sistem informasi;
2) sistem tidak berjalan, gagal fungsi/ *malfunction/ overload*;
3) perangkat keras dan perangkat lunak tidak berjalan;
4) kegagalan sistem informasi termasuk layanan sistem informasi;
5) Kode berbahaya/*malicious code* dan layanan penolakan/*denial service*;
6) Kesalahan akibat dari ketidak-lengkapan/ketidak-akuratan data;
7) Kesalahan manusia/ *human error*;
8) Tidak patuhan dengan kebijakan atau pedoman;
9) Pelanggaran terhadap pengaturan keamanan fisik sistem informasi
10) Perubahan sistem yang tidak terpantau;
11) Pelanggaran atas penggunaan akses;
12) Pelanggaran kerahasiaan dan integritas seluruh hal yang terkait dengan informasi; dan
13) Penyalahgunaan sistem informasi Pemerintah Kabupaten Rote Ndao.

Kebijakan manajemen insiden keamanan informasi meliputi:

a) melaporkan insiden-insiden yang berhubungan dengan keamanan informasi melalui pedoman yang telah ditetapkan sebelumnya baik yang berkaitan dengan teknologi informasi maupun yang berkaitan dengan fasilitas dan infrastruktur sesegera mungkin;
b) menetapkan pegawai yang bertanggung jawab terhadap pelaporan insiden yang berhubungan dengan keamanan informasi. Pegawai tersebut harus dapat dihubungi setiap saat, diketahui oleh seluruh pegawai dan organisasi Pemerintah Kabupaten Rote Ndao, dan mampu mengambil tindakan yang tepat, cepat, dan akurat.
c) menetapkan pedoman pelaporan yang meliputi:
   1. analisis dan identifikasi penyebab insiden;
   2. Penahanan/isolasi;
   3. Perencanaan dan penerapan tindakan;
   4. Pemulihan; dan
   5. Pelaporan tindakan yang telah diambil.

Hal-hal yang harus diperhatikan dalam proses penetapan pedoman laporan insiden keamanan informasi adalah:

1. setiap..

1. setiap tindakan/umpan balik yang dilakukan harus direkam untuk mengetahui bahwa tindakan dilakukan dengan tepat dan cermat;
2. rekaman tersebut harus disimpan dengan baik untuk pertimbangan lebih lanjut apabila terjadi kejadian yang sama maupun lainnya dimasa yang akan datang;
3. tindakan pemulihan/perbaikan sistem harus dipantau secara resmi dan seluruh tindakan yang diambil harus didokumentasikan secara rinci;
4. seluruh laporan atas tindakan pemulihan/perbaikan sistem harus dilaporkan dan direviu;
5. tidak dibenarkan mengambil tindakan penanggulangan sendiri tanpa sepengetahuan pihak yang berkompeten di Pemerintah Kabupaten Rote Ndao. Segera memberitahukan pihak yang berwenang menanggulangi kejadian terkait keamanan informasi Pemerintah Kabupaten Rote Ndao;
6. seluruh pihak yang terkait dipastikan telah mengetahui tanggung jawabnya untuk melaporkan setiap kejadian yang dapat berdampak kepada sistem informasi Pemerintah Kabupaten Rote Ndao;
7. Setiap pihak yang berhubungan dengan sistem informasi Pemerintah Kabupaten Rote Ndao harus menerapkan sikap kehati-hatian terhadap segala aspek yang harus dirahasiakan.

BAB XIV
MANAJEMEN KONTINUITAS OPERASI

A. Ruang Lingkup dan Tujuan.
   1. Ruang lingkup operasi dalam manajemen kontinuitas adalah operasi proses bisnis yang dianggap kritis oleh pemerintah daerah.
   2. Tujuan manajemen kontinuitas operasi yaitu menangani terhentinya aktivitas bisnis dan menjaga proses bisnis kritis dari kegagalan sistem informasi atau bencana untuk memastikan berjalan kembali proses bisnis tepat pada waktunya.

B. Kebijakan Manajemen Kontinuitas Operasi.
   Dalam manajemen kontinuitas operasi harus dilakukan beberapa hal berikut:
   1. Penilaian risiko dalam kontinuitas operasi dengan melakukan beberapa halyakni:
      a) menentukan kemungkinan ancaman dan dampak secara keseluruhan apabila terjadi gangguan baik dari aspek waktu, skala kerusakan dan periode pemulihan; dan
      b) mempertimbangkan untuk mengambil asuransi yang tepat apabila dianggap perlu, sebagai bagian dari manajemen risiko operasional.
   2. Penyusunan rencana kontinuitas operasi, perbaikan operasi ketika terjadi bencana dengan memperhatikan hal sebagai berikut:
      a) identifikasi seluruh kehilangan layanan dan informasi yang dapat diterima; dan
      b) persiapan pedoman untuk memulihkan atau memperbaiki operasi daerah dan ketersediaan informasi pada saat dibutuhkan.
   3. Penyusunan organisasi pelaksana kontinuitas operasi;

4. Pengujian..

4. Pengujian dan pemutakhiran rencana kontinuitas dengan melakukan:
   a) simulasi;
   b) pengujian pemulihan teknis; dan
   c) pengujian pemulihan di tempat pengganti.
5. Sosialisasi dan pelatihan kepada seluruh pegawai ASN; dan
6. Perlindungan terhadap pegawai ASN, fasilitas kritikal dam kekayaan intelektual.

BAB XV
KEPATUHAN KEAMANAN INFORMASI

A. Ruang Lingkup dan Tujuan
   1. Ruang lingkup kepatuhan keamanan informasi meliputi kepatuhan terhadap undang-undang, peraturan, kontrak dengan pihak luar dan kebijakan keamanan informasi.
   2. Tujuan kepatuhan keamanan informasi yaitu untuk menghindari pelanggaran terhadap undang-undang, peraturan, kontrak, dan kebijakan keamanan informasi yang telah ditetapkan pemerintah daerah.

B. Kebijakan Kepatuhan Keamanan Informasi
   Kebijakan kepatuhan keamanan informasi terdiri dari ketaatan kepada persyaratan hukum, perlindungan atas rekaman pemerintah daerah, pencegahan atas penyalahgunaan fasilitas pemrosesan informasi, ketaatan kepada kebijakan, pedoman dan prosedur keamanan informasi. Kebijakan pada masing-masing bagian tersebut adalah:
   1. Ketaatan hukum dilakukan dengan:
      a) menggunakan produk dan piranti lunak yang legal;
      b) memperoleh piranti lunak dari sumber yang diketahui dan mempunyai reputasi yang baik sehingga tidak terjadi pelanggaran hak cipta;
      c) memelihara kesadaran atas perlindungan hak kekayaan intelektual dan memberikan peringatan kepada pegawai yang melanggar hak kekayaan intelektual;
      d) memelihara bukti dan keterangan mengenai izin kepemilikan, *master disk* dan buku petunjuk;
      e) memastikan piranti lunak dan produk yang dipasang di sistem pemerintah daerah telah mempunyai izin;
      f) membuat tata cara pemindahan piranti lunak kepada pihak lain;
      g) mempersiapkan dan menggunakan peralatan audit yang tepat;
      h) mematuhi syarat dan kondisi dari piranti lunak dan informasi yang diperoleh dari jaringan publik;
      i) tidak menduplikasi, mengubah ke format yang lain atau menyadap rekaman komersial seperti film atau audio tanpa mendapatkan izin dari pemilik hak cipta;
      j) tidak melakukan duplikasi sebagian atau keseluruhan dari buku, artikel, laporan atau dokumen lainnya, tanpa mendapatkan izin dari pemilik hak cipta; dan
      k) memeriksa kepatuhan rencana keberlangsungan terhadap persyaratan hukum yang berlaku.

2. Perlindungan..

2. Perlindungan atas rekaman pemerintah daerah dengan cara:
   a) menyusun panduan penyimpanan, penempatan, penanganan dan pemindahan rekaman;
   b) memastikan bahwa penyimpanan rekaman dikategorikan secara rinci termasukjangka waktu dan media penyimpanan;
   c) menetapkan pedoman penggunaan media penyimpanan elektronik yang menjamin akses data (baik media maupun format) dalam periode tertentu untuk menghindari kehilangan yang diakibatkan perubahan teknologi;
   d) menetapkan pedoman penyimpanan dan penanganan media rekaman yang sesuai dengan rekomendasi pabrik. Apabila akan menyimpan rekaman dalam jangka waktu yang lama perlu mempertimbangkan penggunaan media-media khusus;
   e) memperhatikan degradasi kemampuan media penyimpanan rekaman;
   f) menghancurkan rekaman yang sudah tidak dibutuhkan lagi oleh pemerintah daerah setelah periode penyimpanan berakhir;
   g) menerapkan pengendalian yang tepat untuk melindungi rekaman dari kehilangan, kerusakan dan pemalsuan;
   h) memastikan bahwa setiap kunci kriptografi dan program yang berhubungan dengan kriptografi disimpan pada jangka waktu tertentu, sesuai dengan dokumen yang disandi sehingga dokumen tersebut dapat dibuka kembali;
   i) mengkomunikasikan kebijakan perlindungan dan kerahasiaan data pribadi kepada seluruh pegawai dan pihak yang terkait; dan
   j) menerapkan pengendalian yang tepat untuk memastikan seluruh kebijakan, perundang-undangan dan peraturan yang terkait dengan perlindungan data pribadi.
3. Pencegahan atas penyalahgunaan fasilitas pemrosesan informasi dengan cara:
   a) memastikan seluruh pegawai ASN memahami bahwa setiap penggunaan fasilitas pemrosesan informasi harus melalui persetujuan pihak yang menjadi pemilik aset informasi tersebut;
   b) memastikan tidak ada penggunaan fasilitas di luar kepentingan kegiatan pemerintah daerah atau untuk tujuan yang tidak mempunyai otorisasi;
   c) memberikan tindakan tegas bagi pegawai ASN yang menggunakan fasilitas atau otorisasi selain untuk kepentingan kegiatan pemerintah daerah;
   d) memastikan seluruh pegawai memahami dan menyadari secara tepat mengenai batasan penggunaan akses yang diizinkan, salah satunya dengan pernyataan tertulis dari pegawai ASN;
   e) menampilkan pesan peringatan apabila pengguna melakukan akses yang tidak diizinkan; dan
   f) apabila pemerintah daerah membutuhkan pemantauan informasi lintas negara, maka pemerintah daerah wajib memperhatikan aspek hukum negara tersebut dan dapat membuat perjanjian yang diperlukan untuk kepentingan tersebut.
4. Ketaatan kepada kebijakan, standar, pedoman dan prosedur keamanan informasi dilakukan dengan beberapa hal berikut:

a. mereviu..

a. mereviu secara berkala kepatuhan terhadap pedoman pemrosesan informasi kepada seluruh pihak yang bertanggung jawab. Apabila ada ketidakpatuhan maka dilakukan hal berikut:
   1) menentukan dan menemukan penyebab ketidakpatuhan;
   2) menentukan dan menerapkan tindakan perbaikan yang tepat; dan
   3) mengevaluasi tindakan yang perlu diambil untuk memastikan tidak terjadi kembali ketidakpatuhan tersebut.
b. menjaga rekaman hasil reviu ketidakpatuhan dan tindakan yang diambil;
c. memastikan bahwa pemeriksaan kepatuhan keamanan informasi dilakukan oleh pegawai yang berpengalaman, kompeten dan berwenang serta disupervisi oleh pihak yang berkompeten dan berwenang;
d. memastikan akses data pada pemeriksaan hanya akses membaca/*read only* dan hanya diperbolehkan untuk mendapatkan salinan yang terpisah dari sistem file dan salinan tersebut segera dihapus setelah selesai pemeriksaan;
e. memastikan bahwa apabila terdapat kewajiban untuk menyimpan file yang diperiksa untuk kebutuhan dokumentasi pemeriksaan, maka harus dilakukan dengan perlindungan yang tepat;
f. memastikan seluruh akses yang dilakukan oleh pemeriksa dipantau dan direkam untuk kebutuhan referensi apabila diuji kembali dengan menggunakan referensi stempel waktu untuk data dan sistem yang kritikal;
g. memastikan peralatan audit seperti piranti lunak atau arsip data harus dipisahkan dari peralatan pengembangan dan operasional dan tidak disimpan pada ruang penyimpanan dan area pengguna, kecuali memiliki tingkat perlindungan tambahan;
h. *reviu* konfigurasi jaringan, sistem operasi, aplikasi, desktop, dan komponen sistem lain terhadap standar; dan
i. jika pihak ketiga turut terlibat dalam pemeriksaan dan terdapat risiko penyalahgunaan peralatan audit atau informasi, maka pengendalian terhadap risiko dan dampaknya harus segera dilakukan misalnya segera mengubah *password* yang diberikan kepada pihak ketiga tersebut.

BUPATI ROTE NDAO,

PAULINA LANING - BULLU