GUBERNUR SUMATERA BARAT

PERATURAN GUBERNUR SUMATERA BARAT

NOMOR 2 TAHUN 2024

TENTANG

PERATURAN PELAKSANAAN PERATURAN DAERAH NOMOR 10 TAHUN 2019 TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR SUMATERA BARAT,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 14 ayat (6), Pasal 18 ayat (5), Pasal 20 ayat (3),Pasal 28 Ayat (3), Pasal 42 ayat (2), Pasal 43 ayat (3), Pasal 44 ayat (2), Peraturan Daerah Provinsi Sumatera Barat Nomor 10 Tahun 2019 tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi perlu menetapkan Peraturan Gubernur tentang Peraturan Pelaksanaan Peraturan Daerah Nomor 10 Tahun 2019 tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi;

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843), sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
3. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua atas Undang-Undang Nomor 12 Tahun 2011 Tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 143, Tambahan Lembaran Negara Republik

Indonesia Nomor 6801);

4. 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);
5. Undang-Undang Nomor 17 Tahun 2022 tentang Provinsi Sumatera Barat (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 160, Tambahan Lembaran Negara Republik Indonesia Nomor 8606);
6. 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);
7. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
8. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Tahun 2019 Nomor 120 tentang Perubahan atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (berita Negara Republik Indonesia Tahun 2019 Nomor 157);
9. Peraturan Kepala 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);
10. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (berita Negara Republik Indonesia Tahun 2021 Nomor 541);
11. Peraturan Daerah Provinsi Sumatera Barat Nomor 10 Tahun 2019 tentang Penyelenggaraan Persandian untuk Pengamanan Informasi (Lembaran Daerah Provinsi Sumatera Barat Tahun 2019 Nomor 10);

MEMUTUSKAN :

Menetapkan : PERATURAN GUBERNUR TENTANG PERATURAN PELAKSANAAN PERATURAN DAERAH NOMOR 10 TAHUN 2019 TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Daerah adalah Provinsi Sumatera Barat.
2. Gubernur adalah Gubernur Sumatera Barat.
3. Pemerintah Daerah adalah Gubernur dan perangkat daerah sebagai unsure penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
4. Kabupaten/Kota adalah Pemerintah Kabupaten/Kota di Provinsi Sumatera Barat.
5. Perangkat Daerah adalah unsur pembantu Gubernur dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
6. Dinas adalah Dinas yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika, persandian dan statistik.
7. Persandian adalah kegiatan dibidang pengamanan data/informasi yang dilaksanakan dengan menerapkan konsep, teori, seni dan ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terkait pada etika profesi sandi.
8. Penyelenggaraan Persandian adalah pelaksanaan urusan Pemerintahan bidang Persandian oleh Pemerintah Daerah sesuai ketentuan peraturan perundang-undangan.
9. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi Informasi dan komunikasi secara elektronik atau pun non elektronik.
10. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan

Informasi.

11. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
12. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
13. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang mempunyai tugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber.
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. Jaring Komunikasi Sandi adalah keterhubungan antar pengguna persandian melalui jaringan telekomunikasi.
16. Forum Komunikasi Sandi Daerah yang selanjutnya disebut FORKOMSANDA adalah wadah untuk berkomunikasi, berkoordinasi, dan bertukar informasi terkait penyelenggaraan persandian di tingkat Daerah.

Pasal 2

Peraturan Gubernur ini dimaksudkan untuk memberikan pedoman bagi Perangkat Daerah dalam melaksanakan kebijakan, program, dan kegiatan penyelenggaraan persandian untuk pengamanan informasi.

Pasal 3

Peraturan Gubernur ini bertujuan untuk :

a. menciptakan hubungan komunikasi yang baik dan aman pada seluruh Perangkat Daerah;
b. membantu Perangkat Daerah dalam Pengamanan Informasi milik Pemerintah Daerah untuk menjamin keutuhan, keotentikan dan kenirsangkalan informasi;
c. meningkatkan kinerja Perangkat Daerah dalam pelaksanaan pada sistem pemerintahan berbasis elektronik (SPBE);
d. menjamin integritas informasi untuk memastikan bahwa informasi tidak diubah/dimodifikasi selama

penyimpanan atau pada saat dikirimkan;

e. menjamin keautentikan pemilik informasi untuk memastikan bahwa informasi dikirimkan dan diterima oleh pihak yang benar (keaslian pengirim/penerima informasi);
f. menjamin nir-penyangkalan untuk memastikan bahwa pemilik informasi tidak dapat menyangkal bahwa informasi tersebut adalah miliknya atau telah disahkan olehnya;
g. menjaga kerahasiaan untuk memastikan bahwa informasi hanya dapat diakses oleh pihak yang sah;
h. meningkatkan kepercayaan dan penerimaan terhadap implementasi sistem elektronik; dan
i. meningkatkan efisiensi dan efektivitas penyelanggaraan pemerintahan dan layanan publik.

Pasal 4

Ruang lingkup dari Peraturan Gubernur ini meliputi:

a. tata cara penyusunan rencana pengamanan informasi;
b. tata cara permohonan fasilitasi penyediaan sarana dan prasarana keamanan teknologi informasi dan komunikasi khusus kepada BSSN;
c. pengelolaan sumberdaya manusia;
d. tim pengelola keamanan informasi;
e. koordinasi;
f. Forum Komunikasi Sandi Daerah; dan
g. pembinaan dan pengawasan.

BAB II

TATA CARA PENYUSUNAN RENCANA PENGAMANAN INFORMASI

Bagian Kesatu

Umum

Pasal 5

(1) Penyusunan rencana Pengamanan Informasi dilakukan dengan :
    a. menyusun rencana strategis Pengamanan Informasi;
    b. menetapkan arsitektur Keamanan Informasi; dan
    c. menetapkan aturan mengenai tata kelola Keamanan Informasi.
(2) Penyusunan rencana Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dapat diseminarkan.

Bagian Kedua

Rencana Strategis Pengamanan Informasi

Pasal 6

(1) Perencanaan persandian untuk pengamanan informasi di lingkungan Pemerintah Daerah dituangkan dalam rencana strategis Pengamanan Informasi.

(2) Rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) disusun untuk jangka waktu 5 (lima) tahun.

(3) Rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) disusun oleh Dinas dan dikoordinasikan dengan Perangkat Daerah yang membidangi perencanaan pembangunan Daerah.

Pasal 7

(1) Rencana strategis Pengamana Informasi sebagaimana dimaksud dalam Pasal 6 ayat (1), paling sedikit memuat:

a. visi dan misi Pengamanan Informasi;
b. sasaran dan target pengembangan Pengamanan Informasi;
c. kebijakan dan strategi pengembangan Pengamanan Informasi;
d. arsitektur keamanan informasi;
e. proses kerja Pengamanan Informasi;
f. data dan layanan informasi Pengamanan Informasi;
g. rencana Integritas data dan layanan Pengamanan Informasi;
h. rencana pengembangan Pengamanan Informasi;
i. strategi implementasi pengembangan Pengamanan Informasi; dan
j. roadmap implementasi Pengamanan Informasi Pemerintah Daerah.

(2) Rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Gubernur.

Pasal 8

Rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 6 dan Pasal 7 diintegrasikan kedalam rencana pembangunan jangka menengah daerah.

Pasal 9

(1) Dalam penyusunan rencana strategis sebagaimana dimaksud dalam Pasal 6, Gubernur dapat melakukan koordinasi dan konsultasi kepada BSSN.
(2) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (1), secara teknis Gubernur dapat menunjuk Dinas.

Bagian Ketiga

Arsitektur Keamanan Informasi

Pasal 10

(1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf b memuat :
    a. infrastruktur teknologi informasi;
    b. desain keamanan perangkat teknologi informasi dan keamanan jaringan; dan
    c. aplikasi keamanan perangkat teknologi informasi dan keamanan jaringan.
(2) Dalam melakukan penyusunan arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) Gubernur dapat melakukan koordinasi dan konsultasi kepada BSSN.
(3) Koordinasi dan konsultasi sebagaimana dimaksud pada ayat (2) secara teknis dilakukan oleh Dinas.
(4) Evaluasi arsitektur Keamanan Informasi oleh Gubernur sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas setiap tahun atau sewaktu-waktu sesuai dengan kebutuhan.
(5) Evaluasi sebagaimana dimaksud pada ayat (4) dilakukan terhadap pelaksanaan dan kesesuaian Arsitektur Keamanan Informasi terhadap perkembangan teknologi dan kebutuhan Daerah.

Pasal 11

(1) Infrastruktur teknologi informasi sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf a merupakan sumberdaya teknologi informasi yang menyediakan *platform* untuk aplikasi sistem informasi Pemerintah Daerah yang lebih rinci.
(2) Infrastruktur teknologi informasi sebagaimana

dimaksud ayat (1) meliputi:

a. perangkat keras;

b. perangkat lunak;

c. jaringan; dan

d. layanan.

(3) Infrastruktur teknologi Informasi sebagaimana dimaksud pada ayat (2) terdiri dari komponen yang harus dipenuhi yakni :

a. *hardware* komputer, seperti *personal computer, desktop*, *notebook*, komputer *server* dan *smartphone*;

b. perangkat lunak dan data dapat dikumpulkan, diolah, dan disajikan;

c. manajemen dan penyimpanan data;

d. jaringan dan telekomunikasi;

e. layanan dan konsultasi integrasi sistem; dan

f. sistem operasi.

Pasal 12

(1) Desain keamanan perangkat teknologi Informasi dan keamanan jaringan sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf b merujuk pada penerapan aspek keamanan.

(2) Aspek keamanan sebagaimana dimaksud pada ayat (1) meliputi:

a. Perancangan;

b. Pengembangan; dan

c. pengoperasian perangkat teknologi Informasi (TI).

(3) Desain keamanan perangkat teknologi Informasi dan keamanan jaringan sebagaimana dimaksud pada ayat (1) bertujuan untuk:

a. melindungi informasi sensitif;

b. mencegah ancaman dan serangan siber;

c. menjaga integritas;

d. kerahasiaan; dan

e. menjamin ketersediaan data.

Pasal 13

(1) Prinsip dan aspek desain keamanan perangkat teknologi Informasi sebagaimana dimaksud dalam Pasal (12) ayat (1) yakni :

a. prinsip akses terendah (*least privilage*);

b. mekanisme sederhana (*economy of mechanism*);

c. penyelesaian menyeluruh (*complete mediation*);
d. rancangan terbuka (*open design*);
e. pemisahan hak akses istimewa (*separation of priviledge*);
f. mekanisme pemisahan hak akses (*least common mechanism*);
g. penggunaan yang mudah (*psychological acceptability*);
h. pertahanan yang mendalam (*defense in depth*);
i. titik pengawasan (*choke point*);
j. aman disaat kendala (*fail safe stance*);
k. terlibat secara keseluruhan (*universal participation*);
l. keberagaman pertahanan (*diversity of defense*);dan
m. kesederhanaan (*simplicity*).

(2) Prinsip dan aspek desain keamanan perangkat teknologi Informasi sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

Pasal 14

(1) Aplikasi keamanan perangkat teknologi Informasi dan keamanan jaringan sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf c meliputi :
   a. aplikasi keamanan perangkat teknologi Informasi;dan
   b. aplikasi keamanan jaringan;

(2) Aplikasi keamanan perangkat teknologi informasi sebagaimana dimaksud pada ayat (1) huruf a diterapkan untuk melindungi aplikasi perangkat lunak yang digunakan dalam lingkungan teknologi Informasi.

(3) Aplikasi keamanan jaringan sebagaimana dimaksud pada ayat (1) huruf b diterapkan untuk melindungi jaringan komputer dari ancaman dan serangan yang dapat mengakibatkan kebocoran data, gangguan layanan, dan kerugian lainnya.

Bagian Keempat

Tata Kelola Keamanan Informasi

Pasal 15

(1) Tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf c, paling sedikit terdiri atas:
   a. keamanan sumberdaya teknologi Informasi;
   b. keamanan akses kontrol;

c. keamanan data dan informasi;
d. keamanan sumberdaya manusia;
e. keamanan jaringan;
f. keamanan surat elektronik;
g. keamanan pusat data; dan
h. keamanan komunikasi.

(2) Dalam melakukan penyusunan aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) Gubernur dapat melakukan koordinasi dan konsultasi kepada BSSN.

(3) Dalam hal melaksanakan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (2), secara teknis Gubernur dapat menunjuk Dinas.

(4) Tata kelola keamanan informasi sebagaimana dimaksud pada ayat (2) digunakan untuk mengimplementasikan sistem manajemen Keamanan Informasi (SMKI) di lingkungan Pemerintah Daerah.

(5) Tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

Pasal 16

(1) Dalam menyusun rencana Pengamanan Informasi sebagaimana dimaksud dalam Pasal 5, Gubernur dapat membentuk tim.

(2) Tim sebagaimana dimaksud pada ayat (1), terdiri dari:
a. aparatur sipil negara pada Perangkat Daerah terkait;
b. akademisi; dan
c. praktisi.

(3) Tim sebagaimana dimaksud pada ayat (1) mempunyai tugas :
a. melakukan identifikasi dan kajian terhadap kebutuhan Pengamanan Informasi Pemerintah Daerah;
b. melakukan analisis resiko terhadap potensi ancaman dan serangan siber terhadap data dan Informasi Pemerintah Daerah;
c. melaksanakan dan memfasilitasi penyusunan rencana pengamanan Informasi Pemerintah Daerah yang terdiri dari rencana strategis Pengamanan Informasi, arsitektur Keamanan Informasi dan tata kelola Keamanan Informasi.
d. memberikan rekomendasi dan masukan terkait

kebutuhan, resiko dan rencana pengamanan data dan Informasi Pemerintah Daerah;

e. melakukan koordinasi dan konsultasi.

(4) Tim sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Gubernur.

BAB III

TATA CARA PERMOHONAN FASILITASI PENYEDIAAN SARANA DAN PRASARANA KEAMANAN TEKNOLOGI INFORMASI DAN KOMUNIKASI KHUSUS KEPADA BSSN

Pasal 17

(1) Dalam rangka pemenuhan kebutuhan fasilitas Pengamanan Informasi dan komunikasi khusus, Gubernur mengajukan permohonan ke BSSN melalui Dinas.

(2) Pengajuan permohonan sebagaimana dimaksud pada ayat (1) berdasarkan perencanaan kebutuhan Pengamanan Informasi.

(3) Pengajuan permohonan sebagaimana dimaksud pada ayat (1) meliputi :

a. sarana dan prasarana;

b. pendampingan personil untuk berbagi pengetahuan sarana dan prasarana keamanan teknologi Informasi dan komunikasi.

(4) Perencanaan kebutuhan Pengamanan Informasi sebagaimana dimaksud pada ayat (2) dilakukan oleh Dinas.

(5) Perencanaan kebutuhan Pengamanan Informasi sebagaimana dimaksud pada ayat (4) dikomunikasikan dengan BSSN.

(6) Pengajuan permohonan sebagaimana dimaksud pada ayat (1) disampaikan secara tertulis.

BAB IV

PENGELOLAAN SUMBERDAYA MANUSIA

Bagian Kesatu

Umum

Pasal 18

(1) Dinas mengelola sumberdaya manusia untuk menjamin Keamanan Informasi dalam menjaga keberlangsungan dan peningkatan mutu pelayanan Informasi.

(2) Pengelolaan sumberdaya manusia sebagaimana

dimaksud pada ayat (1) mencakup aparatur sipil negara pengelola Keamanan Informasi pada Perangkat Daerah.

Pasal 19

(1) Dalam pengelolaan sumberdaya manusia sebagaimana dimaksud dalam Pasal 18, Dinas berkoordinasi dengan Perangkat Daerah yang membidangi urusan kepegawaian dan Perangkat Daerah yang membidangi urusan pengembangan sumberdaya manusia.
(2) Pengelolaan sumberdaya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses sebagai berikut:
    a. Pengembangan kompetensi;
    b. Pembinaan karir;
    c. pendayagunaan; dan
    d. pemberian tunjangan pengamanan persandian.

Bagian Kedua

Pengembangan Kompetensi

Pasal 20

Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 19 ayat (2) huruf a dilaksanakan melalui:

1. pendidikan;
2. pelatihan;
3. bimbingan teknis dan kursus;
4. workshop dan seminar.

Pasal 21

(1) Pendidikan sebagaimana dimaksud pada pasal 20 ayat (1) bertujuan untuk meningkatkan pengetahuan dan keterampilan dalam pengelolaan teknologi Informasi melalui pendidikan kejenjang yang lebih tinggi dari jenjang pendidikan sebelumnya.
(2) Pendidikan dilakukan pada perguruan tinggi didalam maupun di luar negeri baik perguruan tinggi negeri maupun perguruan tinggi swasta dengan memperhatikan kesesuaian jurusan atau bidang studi dengan kebutuhan pengembangan teknologi Informasi Pemerintah Daerah.
(3) Kesesuaian jurusan atau bidang studi pada perguruan tinggi tujuan sebagaimana dimaksud pada ayat (1),

ditentukan oleh Perangkat Daerah yang membidangi pengelolaan pendidikan pegawai.

(4) Sumber daya Aparatur yang telah mengikuti pendidikan di bidang teknologi Informasi dikembalikan ke Perangkat Daerah semula.

Pasal 22

(1) Pelatihan sebagaimana dimaksud dalam Pasal 20 ayat (2) merupakan kegiatan untuk meningkatkan kompetensi dalam mengelola teknologi Informasi Pemerintah Daerah dalam kurun waktu minimal 3 (tiga) hari antara 24 (dua puluh empat) jam pelajaran sampai dengan 150 (seratus lima puluh) jam pelajaran.

(2) Pelatihan sebagaimana dimaksud pada ayat (1) dapat diselenggarakan oleh Perangkat Daerah yang membidangi pengembangan sumberdaya manusia, perguruan tinggi, lembaga negara atau kementerian serta pihak swasta.

(3) Pelatihan bidang teknologi Informasi sebagaimana dimaksud pada ayat (1) meliputi:
   a. pengelolaan perangkat keras (*hardware*);
   b. pengelolaan perangkat lunak (*software*);
   c. manajemen teknologi Informasi;
   d. sistem Informasi; dan
   e. keamanan Informasi.

Pasal 23

(1) Bimbingan teknis dan kursus sebagaimana dimaksud pada pasal 20 ayat (3) merupakan suatu kegiatan pengembangan profesionalisme bidang teknologi Informasi pada Pemerintah Daerah yang diselenggarakan instansi pemerintah maupun instansi swasta baik didalam negeri maupun di luar negeri.

(2) Dinas dapat merencanakan dan mengirim peserta untuk mengikuti bimbingan teknis dan kursus pengembangan profesionalisme bidang teknologi Informasi sebagaimana dimaksud pada ayat (1).

(3) Bimbingan teknis dan kursus pengembangan profesionalisme dapat dilaksanakan di dalam dan di luar negeri dengan durasi waktu pelaksanaan 1 (satu) minggu sampai dengan 6 (enam) bulan.

(4) Bimbingan teknis dan kursus pengembangan profesionalisme didalam negeri dapat dilaksanakan pada lembaga-lembaga pemerintah dan lembaga

swasta yang tersertifikasi secara nasional maupun internasional.

(5) Bimbingan teknis dan kursus pengembangan profesionalisme di luar negeri dapat dilaksanakan di perguruan tinggi atau lembaga internasional lainnya yang menyediakan kursus singkat dibidang teknologi Informasi.

(6) Bimbingan teknis dan kursus pengembangan profesionalisme bidang teknologi Informasi sebagaimana dimaksud pada ayat (1) meliputi:

a. pengelolaan perangkat keras (*hardware*);

b. pengelolaan perangkat lunak (*software*);

c. manajemen teknologi Informasi;

d. sistem Informasi; dan

e. keamanan Informasi.

(7) Sumber daya aparatur yang telah mengikuti bimbingan teknis dan kursus di bidang teknologi Informasi sebagaimana dimaksud pada ayat (1) dikembalikan ke Perangkat Daerah semula.

Pasal 24

(1) Workshop dan seminar sebagaimana dimaksud pada pasal 20 ayat (4) bertujuan untuk meningkatkan kompetensi aparatur dalam mengelola teknologi Informasi.

(2) Workshop dan seminar sebagaimana dimaksud pada ayat (1) dapat dilaksanakan oleh:

a. Dinas;

b. Perangkat Daerah yang membidangi pengelola sumberdaya manusia;

c. instansi pusat;

d. perguruan tinggi dan

e. pihak swasta.

(3) Workshop dan seminar bidang teknologi Informasi meliputi informasi terbaru tentang perangkat keras (*hardware*), perangkat lunak (*software*), manajemen teknologi informasi, sistem Informasi dan keamanan Informasi.

(4) Sumber daya aparatur yang telah mengikuti Workshop dan seminar sebagaimana dimaksud pada ayat (1) berkewajiban untuk menyampaikan dan menyebarkan informasi yang didapat pada Perangkat Daerah tempat bertugas.

Bagian Ketiga
Pembinaan Karir
Pasal 25

(1) Pembinaan karir sebagaimana dimaksud dalam Pasal 19 ayat (2) huruf b dilaksanakan dengan ketentuan:
   a. Pembinaan jabatan fungsional di bidang Keamanan Informasi; dan
   b. Pengisian formasi jabatan pimpinan tinggi dan jabatan administrator sesuai dengan standar kompetensi yang ditetapkan.
(2) Pembinaan karir sebagaimana dimaksud pada ayat (1), dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Keempat
Pendayagunaan
Pasal 26

(1) Pendayagunaan sebagaimana dimaksud dalam Pasal 19 ayat (2) huruf c dilaksanakan agar seluruh sumberdaya manusia yang bertugas di bidang Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan.
(2) Pendayagunaan sebagaimana dimaksud pada ayat (1), dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima
Pemberian Tunjangan Pengamanan Persandian
Pasal 27

(1) Tunjangan pengamanan Persandian sebagaimana dimaksud dalam Pasal 19 ayat (2) huruf d adalah bentuk insentif tambahan yang diberikan kepada pegawai negeri yang diangkat dan ditugaskan sebagai pengelola pengamanan Persandian.
(2) Pengangkatan pegawai negeri sebagaimana yang dimaksud pada ayat (1) ditetapkan dengan Keputusan Gubernur.
(3) Tunjangan pengamanan Persandian dibayarkan terhitung mulai tanggal 1 (satu) bulan berikutnya setelah pegawai negeri yang bersangkutan secara nyata melaksanakan tugas.

(4) Pemberian tunjangan pengamanan Persandian sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan kemampuan keuangan Daerah dan ketentuan peraturan perundang-undangan.

BAB V
TIM PENGELOLA KEAMANAN INFORMASI
Pasal 28

(1) Untuk pelaksanaan Keamanan Informasi, dibentuk tim pengelola Keamanan Informasi yang ditetapkan dengan Keputusan Gubernur.
(2) Tim pengelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) berasal dari Dinas dan unsure Perangkat Daerah terkait yang terdiri dari:
    a. penanggungjawab;
    b. koordinator; dan
    c. anggota.
(3) Tim pengelola Keamanan Informasi sebagaimana dimaksud pada ayat (2) memiliki tugas sebagai berikut:
    a. mengkoordinasikan pelaksanaan kebijakan tata kelola Keamanan Informasi pada Perangkat Daerah;
    b. membantu untuk memastikan langkah perbaikan yang dilakukan sesuai saran dan rekomendasi hasil pelaksanaan pengawasan dan evaluasi serta audit Keamanan Informasi pada Perangkat Daerah;
    c. mengkoordinasikan penanganan gangguan atau insiden Keamanan Informasi pada Perangkat Daerah;
    d. melakukan pengawasan dan evaluasi, serta audit internal terhadap pelaksanaan kebijakan tata kelola Keamanan Informasi pada Perangkat Daerah; dan
    e. memberi masukan kepada Gubernur untuk meningkatkan pelaksanaan Keamanan Informasi dalam penyelenggaraan pemerintahan.
(4) Koordinator sebagaimana dimaksud pada ayat (2) dijabat oleh kepala Dinas.
(5) Tim pengelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) bertanggung jawab dan melaporkan kegiatannya kepada Gubernur melalui kepala Dinas.

BAB VI
KOORDINASI
Pasal 29

(1) Untuk mendukung pelaksanaan tugas dan fungsi dalam penyelenggaraan Persandian dilingkungan Pemerintah Daerah, Gubernur melalui Dinas dapat berkoordinasi dengan :
    a. BSSN;
    b. kementerian komunikasi dan informatika;
    c. instansi vertikal terkait.
(2) Koordinasi dengan BSSN sebagaimana dimaksud pada ayat (1) huruf a dilakukan dalam rangka pelaksanaan urusan pemerintahan bidang Persandian dan Keamanan Informasi.
(3) Koordinasi dengan kementerian komunikasi dan informatika sebagaimana dimaksud pada ayat (1) huruf b dalam rangka memperkuat infastrukur teknologi Informasi dan komunikasi dalam menjamin keamanan Informasi.
(4) Koordinasi dengan instansi vertikal terkait sebagaimana dimaksud pada ayat (1) huruf c dilakukan dalam rangka meningkatkan kerjasama dalam pelaksanaan program-program dan kegiatan pembangunan Keamanan Informasi untuk mewujudkan keserasian antara kebijakan Daerah dan nasional.

BAB VII
FORUM KOMUNIKASI SANDI DAERAH
Pasal 30

(1) Untuk mendukung pelaksanaan tugas dan fungsi dalam Penyelenggaraan Persandian di lingkungan Pemerintah Daerah, di bentuk FORKOMSANDA yang ditetapkan dengan Keputusan Gubernur.
(2) FORKOMSANDA sebagaimana dimaksud dalam ayat (1) dibentuk untuk mendukung Penyelenggaraan Persandian yang efektif, efisien dan komprehensif guna meningkatkan Keamanan Informasi dilingkungan Pemerintah Daerah.
(3) FORKOMSANDA sebagaimana dimaksud pada ayat (1) diketuai oleh kepala Dinas dan beranggotakan unsure dari:
    a. instansi forum komunikasi pimpinan Daerah;

b. instansi vertikal; dan

c. Perangkat Daerah terkait.

(4) FORKOMSANDA sebagaimana dimaksud pada ayat (1) bertanggungjawab dan melaporkan kegiatannya kepada Gubernur selaku Pembina FORKOMSANDA melalui Dinas.

Pasal 31

FORKOMSANDA sebagaimana dimaksud dalam Pasal 30 ayat (1) mempunyai tugas :

a. menyusun program Kerja tahunan;
b. mendukung pelaksanaan tugas Pemerintah Daerah dan pusat di bidang Persandian dan Keamanan Informasi di Daerah sesuai dengan peraturan perundang-undangan;
c. memberikan masukan, pertimbangan, dan rekomendasi kepada Pemerintah Daerah berkaitan dengan penyelenggaraan Persandian dan Pengamanan Informasi;
d. melaksanakan pembinaan sumberdaya manusia pelaksana siber dan Keamanan Informasi, Persandian dan pendukung Persandian dan Keamanan Informasi di Daerah;
e. membangun kesadaran Keamanan Informasi kepada masyarakat pada umumnya dan aparatur sipil negara; dan
f. melakukan evaluasi dan laporan pelaksanaan program kerja tahunan yang disampaikan kepada Pembina FORKOMSANDA.

Pasal 32

FORKOMSANDA sebagaimana dimaksud dalam Pasal 30 ayat (1), melaksanakan kegiatan:

a. rapat rutin yang diselenggarakan minimal 1 (satu) kali setahun;
b. pertukaran Informasi;
c. latihan dan simulasi;dan/atau
d. kampanye kesadaran Keamanan Informasi.

Pasal 33

FORKOMSANDA sebagimana dimaksud dalam Pasal 30 ayat (1) dapat berkoordinasi dengan:

a. BSSN;
b. Kementerian Komunikasi dan Informatika;
c. Badan Perencana Pembangunan Nasional; dan/atau

d. Kemeterian Dalam Negeri.

Pasal 34

Dalam melaksanakan tugas sebagimana dimaksud dalam Pasal 31, FORKOMSANDA dapat dibantu oleh secretariat dengan beranggotakan aparatur sipil negara pada Dinas yang ditetapkan dengan Keputusan Gubernur.

BAB VIII

PEMBINAAN DAN PENGAWASAN

Pasal 35

Gubernur melakukan pembinaan dan pengawasan penyelenggaraan Persandian untuk Pengamanan Informasi dilingkungan Pemerintah Daerah.

Pasal 36

(1) Pembinaan sebagaimana dimaksud dalam Pasal 35 dilaksanakan secara teknis oleh Dinas.
(2) Pembinaan sebagaimana dimaksud pada ayat (1) dilakukan melalui:
    a. sosialisasi mengenai pengetahuan di bidang Persandian untuk Pengamanan Informasi pada Perangkat Daerah;
    b. asistensi/pendampingan dan konsultasi di bidang Persandian untuk Pengamanan Informasi pada Perangkat Daerah;
    c. literasi terhadap masyarakat dalam penggunaan teknologi Informasi dan komunikasi agar tidak terjadinya perilaku menyimpang;
    d. pembangunan terhadap sumber daya manusia dan infrastruktur Persandian pada Pemerintah Daerah;
    e. penanganan insiden/kejadian serangan siber pada Perangkat Daerah; dan/atau
    f. asistensi/pendampingan, dan konsultasi serta koordinasi dibidang Persandian untuk Pengamanan Informasi.

Pasal 37

(1) Pengawasan sebagaimana dimaksud dalam Pasal 35 dilaksanakan oleh Dinas.

(2) Pengawasan sebagaimana dimaksud dalam ayat (1) dilakukan melalui:

a. peningkatan kesadaran hukum;

b. peningkatan profesionalisme aparatur pelaksana;

c. peningkatan peran dan fungsi pelaporan.

(3) Bentuk Pengawasan yang dapat dilakukan oleh Dinas sebagaimana dimaksud pada ayat (1) diantaranya meliputi:

a. penerapan tata kelola keamanan Informasi dalam rangka mengimplementasikan sistem manajemen Keamanan Informasi pada Perangkat Daerah;

b. pelaksanaan Layanan Keamanan Informasi; dan/atau

c. pemanfaatan jaring komunikasi sandi Pemerintah Daerah.

Pasal 38

(1) Dalam melaksanakan pembinaan dan pengawasan sebagaimana dimaksud dalam Pasal 35, Dinas dapat melakukan koordinasi urusan Persandian dengan Perangkat Daerah terkait dan Pemerintah Kabupaten/Kota.

(2) Koordinasi sebagaimana dimaksud pada ayat (1) dapat dilakukan melalui rapat atau pertemuan yang dilaksanakan oleh Dinas.

(3) Rapat atau pertemuansebagaimanadimaksud pada ayat (2) dilaksanakan paling sedikit 1 (satu) kali dalam1 (satu) tahun.

BAB IX

KETENTUAN PENUTUP

Pasal 39

Peraturan Gubernur ini berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah ProvinsiSumatera Barat.

Ditetapkan di Padang
pada tanggal 30 Januari 2024

GUBERNUR SUMATERA BARAT,

MAHYELDI

Diundangkan di Padang
Pada tanggal 30 Januari 2024

SEKRETARIS DAERAH
PROVINSI SUMATERA BARAT,

HANSASTRI

BERITA DAERAH PROVINSI SUMATERA BARAT TAHUN 2024
NOMOR 2

LAMPIRAN I

PERATURAN GUBERNURSUMATERA BARAT

NOMOR 2 TAHUN 2024

TENTANG

PERATURAN PELAKSANAAN PERATURAN DAERAH NOMOR 10 TAHUN 2019 TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

PRINSIP DAN ASPEK DESAIN KEAMANAN PERANGKAT TEKNOLOGI INFORMASI

1. *Least Privilage.*

Prinsip ini menyatakan bahwa setiap proses yang dilakukan pengguna Perangkat Teknologi Informasi harus beroperasi pada level terendah yang diperlukan untuk menyelesaikan tugasnya. Dalam hal ini diimplementasikan dalam pendefinisian hak akses.

Hak akses adalah hak yang diberikan kepada seluruh pegawai untuk mengakses sistem. setiap pegawai diberikan hak akses yang berguna untuk menunjang fungsi kerja dan pelayanan. Setiap pegawai hanya memperoleh hak akses minimum. Dengan demikian, aksi terhadap sistem dapat dibatasi sehingga terhindar dari melakukan hal-hal yang membahayakan keamanan jaringan komputer dan sistem. Hak akses minimumakan membuat para penyusup dari Internet tidak dapat berbuat banyak saat berhasil menembus sebuah user pada sistem jaringan komputer. Selain itu, hak akses minimum juga mengurangi bahaya ”musuh dalam selimut” yang mengancam sistem dari dalam.

2. *Economy of Mechanism.*

Prinsip ini menyatakan bahwa mekanisme keamanan dari suatu sistem harus sederhana sehingga dapat diverifikasi dan diimplementasi dengan benar.

Contohnya : untuk memperkecil peluang penembusan keamanan sistem komputer harus diberikan pembatasan, misalnya :

a) Pembatasan login, misalnya login kesistem dibatasi
   - pada terminal tertentu saja;
   - pada waktu dan hari tertentu saja.

   Untuk menerapkannya admin membuat penjadwalan yang ketat.
b) Pembatasan dengan call back, yaitu login dapat dilakukan oleh siapapun, bila telah sukses, sistem memutuskan koneksi dan memanggil kembali IP yang disepakati. Penyusup tidak dapat menghubungi lewat sembarang saluran,tapi hanya pada saluran tertentu.
c) Pembatasan jumlah usaha login, misalnya dibatasi sampai 3 kali, dan

segera dikunci dan diberitahukan keadministrator.

3. *Complete Mediation.*

Prinsip ini menyatakan bahwa setiap akses ke sistem komputer harus dicek kedalam informasi kendali akses untuk otorisasi yang tepat. Pada model yang sederhana dan paling banyak dilakukan, pemeriksaan otoritas dilakukan pada saat userlog-on kesistem dan mengaktifkan menu-menu yang sesuai dengan hak aksesnya.

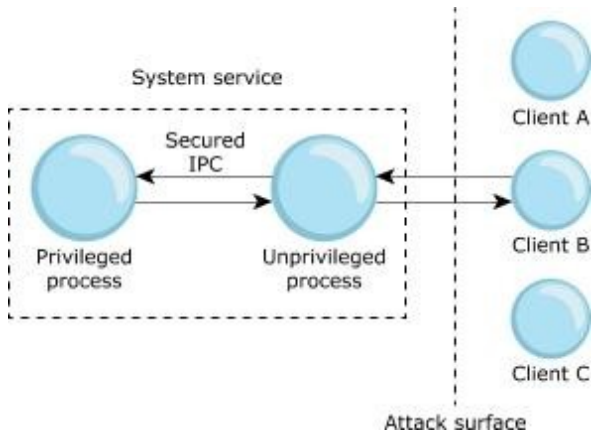
4. *Open Design.*

Prinsip ini menyatakan bahwa mekanisme sekuriti dari suatu sistem harus dapat diinformasikan dengan baik sehingga memungkinkan adanya umpan balik yang dapat dimanfaatkan untuk perbaikan sistem keamanan. Selain itu desain sistem harus bersifat terbuka, artinya jika memiliki kode sumber (source code) maka kode tersebut harus dibuka, dengan maksud untuk meminimalkan kemungkinan adanya lubang (hole) keamanan dalam sistem.

5. *Separation of Priviledge.*

Separation of priviledge adalah cara merancang aplikasi sehingga komponen-komponen dasarnya dibagi menjadi beberapa proses dengan hak istimewa yang berbeda.

Diagram di bawah menggambarkan desain tradisional, dengan layanan sistem yang terdiri dari satu proses istimewa. Dalam contoh ini, permukaan serangan memperlihatkan proses istimewa untuk semua klien.



Separation of priviledge menyatakan bahwa untuk mengakses suatu informasi tertentu seorang user harus memenuhi beberapa persyaratan tertentu. Konsep pemisahan kewenangan berkaitan dengan *Trusted Facility Management*, yang mencakup konsep administrasi pemisahan tugas (separation of duties) dan apa yang perlu diketahui (*need to know*).

Pemisahan Tugas (*Separation of Duties*)

Pada konteks ini, sedikit kewenangan bermakna bahwa pengguna sistem sebaiknya memiliki tingkat hak dan kewenangan yang terendah, kebutuhan untuk melakukan pekerjaan mereka dan juga hanya

membolehkannya untuk jangka waktu yang singkat.

Pada sistem yang umum ditemui, seorang administrator sistem biasanya memiliki kuasa total dari administrasi sistem dan fungsi-fungsi keamanan. Konsolidasi dari kekuatan seperti ini tidak diperbolehkan pada sistem yang aman karena tugas dan fungsi keamanan sebaiknya tidak secara otomatis diberikan ke peran administrator sistem. Pada sistem yang sangat aman, diperlukan tiga peran administratif yang berbeda, antara lain seorang administrator sistem, seorang administrator keamanan yang biasanya adalah seorang Information *System Security Office* (ISSO), dan seorang operator dengan fungsi lebih. Administrator keamanan, administrator sistem, dan operator dapat juga bukan merupakan orang yang berbeda. Namun, ketika administrator sistem memegang peran sebagai administrator keamanan, peran tersebut harus dikontrol dan diaudit. Karena tugas administrator keamanan adalah untuk melakukan fungsi-fungsi keamanan, performa dari kegiatan-kegiatanyangtidakberhubungan dengan keamanan harus dibatas dengan ketat.

6. Least Common Mechanism.

Prinsip ini menyatakan bahwa antar user harus terpisah dalam sistem. Hal ini juga dapat diimplementasikan dengan sistem akses bertingkat.

Sebuah kode kebijakan data mampu menguraikan jenis data yang dianggap sensitif, dan mampu menentukan proses yang ketat untuk mengidentifikasi, menangani dan mengamankan berbaga ijenis data.

Sebuah sistem klasifikasi data yang bertingkat dapat membantu untuk membedakan antara informasi sensitif dan non-sensitif. Langkah-langkah keamanan diberlakukan untuk setiap tingkat data, tingkat pertama yaitu data yang sangat sensitif yang dapat menyebabkan kerusakan parah membutuhkan tingkat keamanan tertinggi dan akses diperbolehkan atas dasar kebutuhan khusus. Tingkat ke-dua yaitu data cukup sensitif yang dapat menimbulkan resiko yang relatif rendah membutuhkan kontrol keamanan yang lebih sedikit dan hak akses internal. Dan tingkat yang ke-tiga yaitu data non-sensitif yang tidak menimbulkan resiko untuk sebuah organisasi, dan membutuhkan keamanan yang sedikit atau tidak ada pembatasan akses.

7. Psychological Acceptability.

Prinsip ini menyatakan bahwa mekanisme pengendalian sistem sekuriti harus mudah digunakan oleh user. Hal ini dapat dilakukan dengan mengadakan survei mengenai perilaku user yang akan menggunakan sistem.

8. Defensein Depth.

Prinsip ini mensyaratkan penggunaan berbagai perangkat keamanan untuk saling membackup. Misalnya dapat dipergunakan *multiplescreening* router, *mirroring harddisk* pada server, dua CDRW untuk satu kali backup data yaitu dua kali sehari (setiap pagi dan sore) pada masing-masing

database sehingga kalau satu dijebol, maka yang satu lagi berfungsi.

9. *Choke point.*

Sistem yang dibangun semuanya harus keluar masuk lewat satu (atau sedikit) gerbang. Syaratnya tidak ada cara lain keluar masuk selain lewat gerbang yang telah ditentukan.

10. *Fail Safe Stance.*

Maksudnya kalau suatu perangkat keamanan rusak, maka secara default perangkat tersebut settingnya akan ke setting yang paling aman. Bila *packet filtering* pada firewall modem router ADSL rusak maka semua paket keluar masuk akan dicegah.

11. *Universal participation.*

Semua orang dalam Pemerintah Daerah harus terlibat dalam proses sekuriti. Setiap tiga bulan sekali dilakukan pelatihan untuk menyegarkan kembali ingatan akan pentingnya mengamankan perangkat keamanan komputer. Didalamnya dilakukan evaluasi untuk peningkatan efisiensi kinerja proses keamanan komputer.

12. *Diversity of Defense.*

Mempergunakan beberapa jenis sistem yang berbeda untuk pertahanan. Maksudnya, kalau penyerang sudah menyerang suatu jenis sistem pertahanan, maka dia tetap akan perlu belajar sistem jenis lainnya.

13. *Simplicity*.

Sistem keamananan jangan terlalu kompleks, karena sulit sekali mengetahui salahnya ada dimana kalau sistem terlalu komplek untuk dipahami. Untuk mempermudah mengetahui bila terjadi kesalahan maka setiap data yang disimpan dalam server akan teridentifikasi siapa yang menyimpan berdasarkan user name dan passwordnya, kapan tanggal dan waktunya, dari *workstation* yang mana, dan apa aksi yang dilakukan. Bila user tidak mempunyai hak untuk menambah dan mengubah data pada sistem aplikasi tertentu tersebut maka akan ada trigger yang memberitahu bahwa sistem menolak adanya perubahan data.

StempelParaf				
No	**Nama**	**Jab**	**Tgl**	**Paraf**
1.	Hansastri	**Sekretaris Daerah**		
2.	Andri Yulika	**Ass. Adm dan Umum**		
3.	Siti Aisyah	**Kepala Dinas**		
4.	Oni Fajar Syahdi	**Sekdin**		
5.	Eko Paisal	**Kabid Siber dan Sandi**		

6.	Roby	Sandiman Muda		

GUBERNUR SUMATERA BARAT,

MAHYELDI

LAMPIRAN II
PERATURAN GUBERNUR SUMATERA BARAT
NOMOR 2 TAHUN 2024
TENTANG
PERATURAN PELAKSANAAN PERATURAN DAERAH NOMOR 10 TAHUN 2019 TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

TATA KELOLA KEAMANAN INFORMASI

BAB I
PENDAHULUAN

A. Tujuan

Tata kelola Keamanan Informasi ini disusun sebagai arahan dan pedoman dalam pengelolaan sistem manajemen keamanan informasi secara terpadu serta untuk pengamanan aset informasi guna memastikan terjaganya aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian (authenticity) dan nirsangkalan (inevitability).

B. Ruang Lingkup

1. Ruang lingkup kebijakan ini adalah seluruh Aset informasi dan Aset pemrosesan informasi yang berada di bawah pengelolaan Pemerintah Daerah Provinsi Sumatera Barat, beserta SKPD Pemilik Aset terkait.
2. Aset informasi adalah 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;
   b. Elektronik, meliputi informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti database, pada *file* di dalam komputer, ditampilkan pada *website*, layar komputer dan dikirimkan melalui jaringan telekomunikasi.

C. Kebijakan

1. Perangkat Daerah berkomitmen untuk mengembangkan, mengimplementasikan, memelihara dan meningkatkan Tata kelola keamanan informasi secara berkesinambungan untuk menjamin keamanan informasi organisasi dari risiko keamanan informasi, baik dari pihak internal maupun eksternal.
2. Seluruh informasi dalam bentuk fisik maupun elektronik, yang dikomunikasikan langsung atau melalui teknologi komunikasi harus dilindungi dari kemungkinan kerusakan, kesalahan penggunaan baik secara sengaja atau tidak, dicegah dari akses oleh pengguna yang tidak berwenang dan dari ancaman terhadap kerahasiaan

(*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian (authenticity) dan nirsangkalan (inevitability).

3. Perangkat Daerah berkomitmen untuk mendukung pemenuhan prasyarat internal maupun eksternal keamanan informasi Perangkat Daerah yang relevan.
4. Perangkat Daerah berkomitmen untuk mematuhi seluruh peraturan perundang-undangan, regulasi dan kewajiban kontrak yang relevan.
5. Perangkat Daerah berkomitmen untuk memastikan ketersediaan dari sumber daya yang dibutuhkan oleh Tata kelola Keamanan Informasi di Perangkat Daerah untuk menjamin terciptanya Tata kelola Keamanan Informasi yang efektif dan efisien.
6. Kontrol Keamanan Informasi beserta sasaran masing-masing kontrol ditetapkan oleh Kepala Dinas secara tahunan, didasarkan atas hasil identifikasi dan analisis resiko yang sesuai dengan ruang lingkup kebijakan Tata kelola Keamanan Informasi, serta prioritisasi dengan mempertimbangkan ketersediaan dan kemampuan sumber daya.
7. Kebijakan Keamanan Informasi harus dikomunikasikan ke seluruh pegawai dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.
8. Perangkat Daerah berkomitmen meningkatkan kepedulian (*awareness*), pengetahuan dan keterampilan tentang Keamanan Informasi bagi pegawai, serta mitra pihak ketiga lain sejauh diperlukan.
9. Seluruh kelemahan Keamanan Informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan Teknologi Informasi dan Komunikasi atau gangguan Keamanan Informasi harus segera dilaporkan kepada Dinas.
10. Seluruh pimpinan di semua tingkatan bertanggung jawab menjamin kebijakan ini diterapkan di seluruh unit kerja di bawah pengawasannya.
11. Seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan aset informasi serta mematuhi kebijakan dan prosedur Keamanan Informasi yang telah ditetapkan.
12. Setiap pelanggaran terhadap kebijakan ini dapat dikenai sanksi administratif sesuai ketentuan peraturan perundang-undangan.
13. Setiap pengecualian terhadap kebijakan ini dan kebijakan turunannya harus mendapat persetujuan dari Gubernur Sumatera Barat.
14. Dokumen ini harus ditinjau paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau apabila terdapat perubahan signifikan dalam proses bisnis organisasi untuk menjamin kesesuaian dan kecukupan dengan kondisi terkini.
15. Setiap perubahan terhadap dokumen ini harus didokumentasikan dan disetujui melalui proses manajemen perubahan.

BAB II

PEDOMAN PELAKSANAAN TATA KELOLA KEAMANAN INFORMASI

A. Tujuan

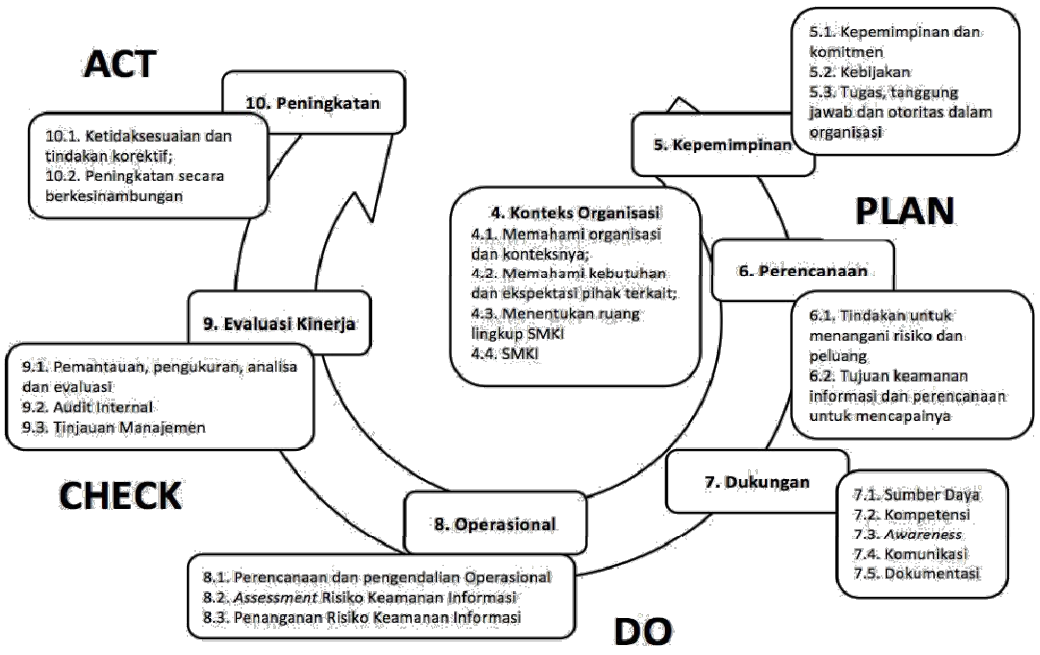
Tata kelola keamanan informasi disusun dalam rangka untuk memastikan efektivitas dan efisiensi dari sistem manajemen keamanan informasi. Kerangka kerja ini akan menjabarkan proses-proses dan aktivitas-aktivitas yang harus dijalankan oleh Perangkat Daerah dalam rangka menetapkan, mengimplementasikan, memelihara Keamanan Informasi dan meningkatkan secara berkesinambungan.

B. Ruang Lingkup

Pedoman pelaksanaan Tata Kelola Keamanan Informasi Sistem yang diatur dalam Peraturan Gubernur ini digunakan untuk mengimplementasikan Manajemen Keamanan Informasi (SMKI) yang merupakan acuan bagi seluruh Perangkat Daerah di lingkungan Pemerintah Provinsi Sumatera Barat .

C. Kebijakan

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



Gambar 1 Penggunaan siklus proses PDCA dalam proses keamanan informasi

2. Proses perencanaan dalam pengembangan Sistem Manajemen Keamanan Informasi meliputi:

a. Perangkat Daerah harus menentukan konteks dan ruang lingkup keamanan organisasi dengan cara :
   1) menentukan dan secara berkala meninjau faktor serta permasalahan internal dan eksternal yang dihadapi oleh organisasi yang :
      1.1 Relevan dengan tujuan dari Perangkat Daerah dan Sistem Manajemen Keamanan Informasi ;
      1.2 Mempengaruhi kemampuan Perangkat Daerah untuk mencapai tujuan keamanan informasi yang diharapkan oleh Perangkat Daerah.
   2) menentukan dan secara berkala meninjau pihak - pihak yang terkait dengan Perangkat Daerah dan dapat mempengaruhi Keamanan Informasi di Perangkat Daerah;
   3) menentukan dan secara berkala meninjau kebutuhan dan ekspektasi terkait Keamanan Informasi dari pihak-pihak yang terkait tersebut;
   4) menentukan dan secara berkala meninjau hubungan dan ketergantungan antar proses dan aktivitas Perangkat Daerah yang dilaksanakan oleh pihak internal maupun pihak eksternal Perangkat Daerah;
   5) menentukan dan secara berkala meninjau ruang lingkup dari tata kelola keamanan informasi di organisasi.

b. Risiko dan peluang yang relevan dengan tata kelola keamanan informasi harus secara jelas ditentukan dan ditangani untuk:
   1) memastikan bahwa tata kelola keamanan informasi mencapai tujuan yang diharapkan;
   2) mencegahatau mengurangi dampak yang tidak diinginkan; dan
   3) mencapai peningkatan yang berkesinambungan.

c. Penentuan risiko dan peluang dilakukan dengan mempertimbangkan aspek-aspek yang telah didefinisikan dalam fase penentuan konteks dan ruang lingkup Perangkat Daerah, yaitu:
   1) Faktor dan permasalahan internal maupun eksternal yang dihadapi Perangkat Daerah; dan
   2) Ekspektasi Keamanan Informasi dari pihak terkait Perangkat Daerah.

3. Perencanaan harus dibuat bagi risiko dan peluang yang telah ditentukan untuk:
   a. menangani risiko dan peluang;
   b. mengintegrasikan dan mengimplementasikan tindakan untuk menangani risiko dan peluang dengan proses tata kelola keamanan informasi; dan
   c. mengevaluasi efektivitas dari tindakan yang diambil dalam rangka menangani risiko dan peluang.

4. Proses manajemen risiko dilakukan melalui proses literatif yang mencakup aktivitas assessment risiko, penanganan risiko, penerimaan risiko dan pengkomunikasian risiko.
5. Seluruh manajemen risiko di organisasi harus dilakukan paling tidak 1 (satu) kali dalam satu tahun atau apabila terdapat usulan atau telah terjadi perubahan yang relevan dan signifikan pada organisasi. Seluruh catatan (*record*) terkait dengan seluruh proses manajemen risiko harus dibuat dan dipelihara.
6. Dalam proses pemilihan dari kontrol terhadap pengendalian risiko tersebut dilakukan pada saat aktifitas penanganan risiko yang merupakan bagian dari proses manajemen risiko.
7. Pemilihan dari kontrol tersebut dapat memperhatikan kontrol Keamanan Informasi berdasarkan standar ISO 27001:2013 atau kontrol lainnya sesuai ketentuan peraturan perundang-undangan.
8. Dalam hal proses pendokumentasian tata kelola keamanan informasi perlumemperhatikan aspek sebagai berikut:
   a. Dokumentasi tata kelola keamanan informasi di Perangkat Daerah perlu mencakup informasi terdokumentasi yang disyaratkan oleh ISO 27001:2013 yang mencakup namun tidak terbatas pada:
      1) ruang lingkup tata kelola keamanan informasi;
      2) kebijakan dan tujuan keamanan informasi;
      3) metodologi assessment dan penanganan risiko;
      4) *statement of applicability*;
      5) rencana penanganan risiko;
      6) laporan *assessment* risiko;
      7) pendefinisian tugas dan tanggung jawab keamanan informasi;
      8) inventarisasi aset;
      9) aturan terkait penggunaan aset;
      10) kebijakan pengendalian akses;
      11) prosedur operasional untuk manajemen TI;
      12) prinsip rekayasa sistem secara aman;
      13) kebijakan keamanan terkait penyedia jasa;
      14) prosedur pengelolaan insiden;
      15) prosedur keberlanjutan bisnis;
      16) prasyarat hukum, regulasi dan kontraktual;
      17) catatan terkait pelatihan, kemampuan, pengalaman dan kualifikasi;
      18) hasil pemantauan dan pengukuran tata kelola keamanan informasi;
      19) program audit internal;
      20) hasil audit internal;
      21) hasil dari tinjauan manajemen;

22) hasil dari tindakan korektif;
23) *log* dari aktifitas pengguna, pengecualiaan dan kejadian keamanan; dan
24) informasi terdokumentasi yang dibutuhkan untuk menjamin efektifitas dari tata kelola keamanan informasi.

b. Dokumen yang relevan dengan tata kelola keamanan informasi dan berasal dari pihak eksternal seperti dokumen peraturan perundang-undangan harus diidentifikasi dan dikendalikan;
c. Terkait proses peninjauan dan pembaruan dokumentasi, hal-hal berikut berlaku:
   1) semua dokumentasi tata kelola keamanan informasi harus ditinjau paling sedikit satu kali dalam 1 (satu) tahun atau apabila terdapat perubahan dan/atau perubahan organisasi untuk menjamin kesesuaian dan kecukupannya dengan kondisi terkini tata kelola keamanan informasi dan keamanan informasi di organisasi;
   2) peninjauanharus dilakukan oleh pemilik dari dokumentasi dan dapat melibatkan pihak-pihak yang terkait dengan dokumentasi dan/atau proses yang relevan dengan dokumentasi tersebut;
   3) setiap pengkinian terhadap dokumentasi tata kelola keamanan informasi sebagai hasil dari peninjauan dokumentasi harus disetujui oleh manajemen yang relevan di Perangkat Daerah;
d. Terkait proses salinan, distribusi dan retensi dokumentasi, hal-hal berikut berlaku:
   1) salinan dari dokumentasi tata kelola keamanan informasi harus didistribusikan kepada pihak internal yang terkait untuk memastikan operasional tata kelola keamanan informasi secara efektif;
   2) akses ke dokumentasi tata kelola keamanan informasi untuk pihak internal akan diberikan berdasarkan kebutuhan pengguna untuk mengakses dokumentasi tersebut (*need to know basis*);
   3) pihak eksternal yang memerlukan akses kepada dokumentasi tata kelola keamanan informasi akan diberikan akses hanya setelah kontrol Keamanan Informasi yang memadai telah diimplementasikan. Hal ini mencakup namun tidak terbatas pada akses *read only* atau perjanjian kerahasiaan;
   4) daftar distribusi harus ditetapkan dan dipelihara untuk mengendalikan distribusi dari dokumentasi tata kelola keamanan informasi; dan
   5) kecuali diputuskan berbeda, seluruh dokumen tata kelola keamanan informasi memiliki masa retensi selama 10 tahun.

9. Perangkat Daerah harus mempertimbangkan penyediaan sumber daya dalam melaksanakan tata kelola keamanan informasi yang mencakup:

a. ketersediaan sumber daya yang dibutuhkan bagi pelaksanaan tata kelola keamanan informasiPerangkat Daerah secara efektif dan efisien sangatlah penting. Oleh karena itu perencanaan yang baik sangatlah penting untuk memastikan ketersediaan sumber daya yang tepat pada waktu yang tepat pula;
b. sumber daya yang dibutuhkan oleh Tata Kelola Keamanan Informasi mencakup sumber daya dengan kompetensi dan pemahaman yang memadai, dokumentasi, proses dan solusi teknis, baik berupa perangkat keras maupun perangkat lunak;
c. perencanaan sumber daya Tata Kelola keamanan Informasi dapat dilakukan bersamaan dengan proses perencanaan dan penyusunan anggaran tahunan Perangkat Daerah; dan
d. pelatihan dan program peningkatan kesadaran terkait dengan Tata Kelola Keamanan Informasi dan Keamanan Informasi Perangkat Daerah akan dilakukan secara berkala bagi seluruh pengguna sistem informasi. Program pelatihan dan peningkatan kesadaran tersebut akan dirancang sesuai dengan fungsi dan tanggung jawab pengguna.

10. Komunikasi yang relevan dengan Tata Kelola Keamanan Informasi, baik internal maupun eksternal, harus dikendalikan dan dikoordinasikan untuk memastikan:
a. efektivitas alur pertukaran informasi dalam Perangkat Daerah dan/atau dari dan ke pihak eksternal;
b. tidak ada kebocoran informasi sensitif milik Pemerintah Daerah;
c. jalur komunikasi Tata Kelola Keamanan Informasi mencakup:
   1) komunikasi tatap muka;
   2) surat dan memo internal;
   3) surat elektronik
   4) surat ekternal;
   5) *email*;
   6) *website* Perangkat Daerah;
   7) pengumuman Pemerintah Daerah; dan
   8) material cetak.
d. personil Perangkat Daerah yang tidak ditunjuk untuk memberikan materi informasi tidak diperbolehkan untuk memberikan informasi apapun;
e. informasi terkait dengan Sistem Manajemen Kemanan Informasi dan/atau keamanan informasi yang berasal dari sumber eksternal harus dikirimkan kepada koordinator tim pengelola keamanan informasi untuk peninjauan dan pendistribusian kepada pihak yang relevan. Hal ini mencakup:
   1) penerbitan peraturan hukum dan perundangan yang baru maupun perubahan terhadap peraturan lama;

2) usulan perubahan terhadap prasyarat Keamanan Informasi;
3) teknologi, ancaman dan kelemahan baru terkait Keamanan Informasi.

11. Proses perencanaan dan pengendalian operasional Tata Kelola Keamanan Informasi harus dikoordinasikan dan dikomunikasikan. Proses perencanaan operasional tata kelola keamanan informasi harus dilakukan secara tahunan serta dokumentasikan dan dikomunikasikan kepada pihak yang terkait dengan Keamanan Informasi. Proses pengendalian operasional tata kelola keamanan informasi adalah proses yang dilakukan untuk memastikan pelaksanaan operasional tata kelola keamanan informasi Perangkat Daerah telah sesuai dengan perencanaan yang telah dibuat. Proses pengendalian ini dapat mencakup aktifitas rapat peninjauan dan harus dilakukan paling sedikit 1 (satu) kali dalam tiga bulan serta melibatkan personil yang terlibat di tata kelola keamanan informasi Perangkat Daerah.
12. Metode untuk mencegah, mendeteksi dan menindaklanjuti pelanggaran terhadap hukum terkait HAKI perlu disusun dan diimplementasikan. Hal ini dapat mencakup aktivitas pemantauan, pengukuran, peninjauan dan/atau audit.
13. Pemantauan, pengukuran, analisis dan evaluasi dari implementasi dan operasional tata kelola keamanan informasi organisasi adalah aktivitas periodik yang dilakukan untuk mengevaluasi kinerja Keamanan Informasi dan efektivitas pelaksanaan tata kelola keamanan informasi Perangkat Daerah. Proses pemantauan, pengukuran, analisis, dan evaluasi mencakup:
    a. metrik pemantauan dan pengukuran harus dipilih secara seksama untuk memastikan bahwa aktivitas pengukuran akan memberikan pemahaman mendalam mengenai kinerja tata kelola keamanan informasi dan kontrol pengendalian Keamanan Informasi Perangkat Daerah;
    b. proses pengukuran tersebut mencakup proses-proses berikut:
        1) penentuan dari metrik pengukuran;
        2) pengukuran dari metrik yang telah ditentukan;
        3) analisis dan evaluasi dari hasil pengukuran.
    c. dalam menentukan metrik pengukuran, aspek-aspek berikut harus dipertimbangkan:
        1) sasaran tata kelola keamanan informasi yang diberikan pada kebijakanPerangkat Daerah;
        2) kontrol Keamanan Informasi yang diimplementasikan;
        3) metode dalam mengumpulkan data dan mengkalkulasi metrik;
        4) target pencapaian dari metrik;
        5) jadwal untuk melakukan pengukuran;
        6) personil yang bertanggung jawab untuk proses pengukuran.

d. metrik pengukuran yang telah ditentukan harus memungkinkan evaluasi dari pencapaian sasaran tata kelola keamanan informasi';
   1) metrik yang telah ditetapkan harus dipantau dengan mengumpulkan data yang relevan dengan metrik;
   2) proses pengukuran harus dilakukan minimal 1 (satu) kali dalam satu tahun terutama untuk mengukur pencapaian dari sasaran tata kelola keamanan informasi;
   3) hasil dari pengukuran harus dianalisis dan dievaluasi untuk menentukan pencapaian dari target pengukuran tersebut;
   4) hasil dari pengukuran harus dilaporkan kepada manajemen puncak Keamanan Informasi dalam rapat tinjauan manajemen Keamanan Informasi;
   5) hasil dari proses pemantauan dan pengukuran efektivitas tata kelola keamanan informasi harus dianalisis dan dievaluasi untuk menentukan apakah implementasi dan operasi Keamanan Informasi Perangkat Daerah:
      1.1 sesuai dengan kebijakan, tujuan, standar dan prosedur tata kelola keamanan informasi Perangkat Daerah;
      1.2 memadai untuk menghadapi kebutuhan dan tantangan kerja serta teknologi terkini; dan
      1.3 sesuai dengan rencana tata kelola keamanan informasi yang sudah dibuat.

14. Peninjauan Keamanan Informasi secara independen harus secara rutin dilakukan.
    a. peninjauan tersebut harus mencakup:
       1) kontrol dan area keamanan informasi, seperti keamanan fisik, jaringan atau akses *logical*;
       2) kebijakan, proses dan prosedur yang relevan dengan tata kelola keamanan informasi;
       3) kepatuhan implementasi tata kelola keamanan informasi dan Keamanan Informasi dengan kebijakan, proses dan prosedur Keamanan Informasi Perangkat Daerah serta prasyarat hukum, perundangan serta kewajiban kontraktual terkait dengan Sistem Manajeman Kemanan Informasi;
       4) peninjauan teknis terhadap fasilitas pengolahan informasi dan sarana pendukungnya.
    b. Hasil dari peninjauan harus didokumentasikan dan dilaporkan kepada Koordinator Tim Pengelola Keamanan Informasi.
    c. setiap permasalahan dan/atau ketidaksesuaian harus segera ditindaklanjuti dengan cara mengidentifikasi tindakan korektif dan/atau peningkatan yang sesuai.
15. Instansi harus melakukan proses audit internal dengan ketentuan sebagai berikut:

a. audit internal tata kelola keamanan informasi di Perangkat Daerah harus dilaksanakan minimal satukali dalam satu tahun dan harus mencakup seluruh ruang lingkup Sistem Manajemen Keamanan Informasi (SMKI);
b. audit internal tata kelola keamanan informasi harus dilakukan oleh auditor yang memiliki kompetensi yang memadai serta memiliki objektifitas dan imparsialitas terhadap proses audit;
c. auditor yang dipilih untuk proses audit harus ditunjuk secara formal oleh Koordinator Tim Pengelola Keamanan Informasi;
d. sebuah program audit tahunan tata kelola keamanan infromasi harus ditetapkan oleh koordinator audit internal tata kelola keamanan informasi dan harus dikomunikasikan kepada koordinator Tim Pengelola Keamanan Informasi;
e. program audit harus mencakup jadual, metode, kriteria dan ruang lingkup, tanggung jawab serta prasyarat pelaporan dari audit;
f. proses audit harus dilakukan sesuai dengan program audit yang telah ditetapkan secara formal;
g. temuan audit harus diklasifikasikan berdasarkan kritikalitas dan cakupan dari temuan tersebut menjadi:
   1) mayor, ketidaksesuaian ini mengindikasikan tidak berjalannya sama sekali sebuah proses tata kelola keamanan informasi atau kontrol Keamanan Informasi, atau apabila sebuah temuan dapat menyebabkan dampak buruk terhadap proses atau sistem kritikal Perangkat Daerah;
   2) minor, ketidaksesuaian ini mengindikasikan sebuah kealpaan/problem kecil yang tidak mengindikasikan bahwa sebuah proses Manajemen Keamanan Informasi atau kontrol Keamanan Informasi tidak berjalannya sama sekali, atau apabila sebuah temuan tidak akan menyebabkan dampak buruk terhadap proses atau sistem kritikal Perangkat Daerah; dan
   3) peluang untuk perbaikan, kategori temuan ini bukan merupakan sebuah ketidaksesuaian namun mengindikasikan bahwa sebuah area dapat diperbaiki untuk meningkatkan kinerja dari proses atau sistem.
h. setiap ketidaksesuaian dan/atau peluang untuk perbaikan yang ditemukan dalam proses audit harus dicatat secara formal oleh auditor dan diterima oleh *auditee*;
i. setiap ketidaksesuaian harus dikoreksi dan ditingkatkan oleh *auditee* dalam jangka waktu yang disepakati dengan cara merencanakan dan melaksanakan koreksi dan tindakan korektif;
j. laporan audit harus dilaporkan kepada manajemen puncak Perangkat Daerah dan dikomunikasikan kepada koordinator Tim Pengelola Keamanan Informasi;
k. koordinator Tim Pengelola Keamanan Informasi dan auditor internal tata kelola keamanan informasi bertanggung jawab untuk

memantau dan memverifikasi koreksi, tindakan korektif maupun peningkatan terkait ketidaksesuaian yang ditemukan dalam audit;

l. verifikasi dari auditor internal tata kelola keamanan informasi dibutuhkan sebelum ketidaksesuaian yang ditemukan dapat dinyatakan ditutup secara formal.

16. Manajemen Puncak Perangkat Daerah wajib untuk melaksanakan tinjauan manajemen Keamanan Informasi minimal satu kali dalam satu tahun atau apabila terjadi perubahan signifikan terhadap manajemen keamanan informasi di Perangkat Daerah. Tinjauan ini dilakukan untuk menjamin terjaganya kesesuaian, kecukupan dan efektivitas dari manajemen keamanan informasi di Perangkat Daerah, dengan memperhatikan hal-hal sebagai berikut:

a. tinjauan manajemen Keamanan Informasi harus dihadiri oleh:
   1) manajemen puncak dari Tim Pengelola Keamanan Informasi di Perangkat Daerah;
   2) koordinator Tata Kelola Keamanan Informasi Perangkat Daerah;
   3) koordinator atau petugas fungsional pengelola manajemen keamanan informasi.

b. Apabila dibutuhkan, tinjauan manajemen Keamanan Informasi dapat dihadiri oleh:
   1) pemangku kepentingan yang relevan dari manajemen keamanan informasi di unit kerja yang membidangi teknologi informatika;
   2) *subject matter expert* yang memadai.

c. Tinjauan manajemen Keamanan Informasi harus mencakup masukan sebagai berikut:
   1) status dari tindakan yang diputuskan pada tinjauan manajemen terdahulu;
   2) perubahan baik internal maupun eksternal yang terkait dengan Keamanan Informasi;
   3) masukan terkait kinerja Keamanan Informasi yang mencakup *trend* pada:
      a. ketidaksesuaian dan tindakan korektif;
      b. hasil pemantauan dan pengukuran;
      c. hasil audit, baik internal maupun eksternal; dan
      d. pemenuhan dari sasaran keamanan informasi.
   4) masukan dari pihak terkait;
   5) hasil dari assessment risiko dan status rencana penanganan risiko;
   6) peluang untuk peningkatan secara berkesinambungan.

d. berdasarkan dari masukan tersebut, tinjauan manajemen keamanan Informasi harus menghasilkan keluaran sebagai berikut:
   1) keputusan terkait peningkatan manajemen keamanan informasi secara berkesinambungan; dan

2) peluang dan kebutuhan untuk perubahan manajemen keamanan informasi.

e. setiap keluaran dari tinjauan manajemen keamanan informasi harus digunakan sebagai dasar bagi peningkatan dan perencanaan tahunan manajemen keamanan informasi.

17. Ketidaksesuaian manajemen keamanan informasi didefinisikan sebagai kondisi dimana adanya prasyarat manajemen keamanan informasi yang tidak terpenuhi. Setiap ketidaksesuaian atau tidak terpenuhinya prasyarat manajemen keamanan informasi harus di identifikasi dan di laporkan:

a. identifikasi dan laporan dari setiap ketidaksesuaian dapat didapatkan melalui:
   1) proses pengelolaan insiden keamanan informasi;
   2) peninjauan internal manajemen keamanan informasi;
   3) proses audit internal manajemen keamanan informasi;
   4) proses pemantauan dan pengukuran manajemen keamanan informasi;
   5) peninjauan dan/atau proses audit eksternal terhadap manajemen keamanan informasi atau keamanan informasi; dan
   6) laporan dan masukan dari *stakeholder* yang terkait.

b. setiap ketidaksesuaian yang terjadi, harus ditangani secara tepat dengan cara:
   1) melakukan koreksi yang sesuai untuk mengendalikan dan memperbaiki ketidaksesuaian yang telah diidentifikasi; dan
   2) menanganisetiap akibat dari ketidaksesuaian yang mungkin terjadi.

c. untuk setiap ketidaksesuaian, evaluasi harus dilakukan untuk mengevaluasi kebutuhan untuk mengambil tindakan korektif untuk menghilangkan penyebab dari ketidaksesuaian supaya ketidaksesuaian tersebut tidak terjadi lagi atau terjadi ditempat lain.

d. tindakan korektif yang diambil harus sesuai dengan dampak dari ketidaksesuaian tersebut untuk memastikan bahwa ketidaksesuaian tersebut tidak berulang atau terjadi ditempat lain dalam ruang lingkup manajemen keamanan informasi.

e. evaluasi untuk menentukan apakah perlu untuk mengambil setiap tindakan korektif harus dilakukan dengan melakukan:
   1) peninjauan terhadap ketidaksesuaian yang terjadi;
   2) menentukan penyebab dari ketidaksesuaian;
   3) menentukan jika ada kejadian dimana ketidaksesuaian yang sama telah terjadi, atau dapat berpotensi untuk terjadi.

f. apabila ditentukan bahwa tindakan korektif memang perlu untuk diambil maka harus dilakukan perencanaan dan implementasi dari tindakan korektif.
g. setelah koreksi dan tindakan korektif telah diambil, sebuah peninjauan harus dilakukan untuk menjamin efektifitasnya dalam mencegah terjadinya kembali atau terjadinya ketidaksesuaian tersebut ditempat lain.

18. Kesesuaian, kecukupan dan efektifitas dari manajemen keamanan informasiPerangkat Daerah harus secara berkesinambungan ditingkatkan.
19. Inisiatif peningkatan harus secara formal diidentifikasi, direncanakan, diimplementasikan dan ditinjau.
20. Identifikasi dari peningkatan harus dilakukan berdasarkan *log*, laporan dan hasil dari:
    a. proses pengelolaan insiden Keamanan Informasi;
    b. peninjauan internal manajemen keamanan informasi;
    c. proses audit internal manajemen keamanan informasi;
    d. proses pemantauan dan pengukuran manajemen keamanan informasi;
    e. peninjauan dan/atau proses audit eksternal terhadap manajemen keamanan informasi atau keamanan informasi; dan
    f. laporan dan masukan dari *stakeholder* yang terkait.
21. Perencanaan dan implementasi dari inisiatif peningkatan harus ditinjau untuk memastikan bahwa inisiatif tersebut dapat mencapai tujuannya.
22. Dokumentasi yang relevan dengan proses peningkatan secara berkesinambungan harus dibuat dan dipelihara.

BAB III
MANAJEMEN RISIKO

A. Tujuan

Tujuan dari manajemen resiko adalah untuk mengelola risiko Keamanan Informasi yang dihadapi oleh Perangkat Daerah atau Pemerintah Daerah dalam rangka untuk mempersiapkan diri terhadap terjadinya risiko beserta dampaknya.

B. Ruang Lingkup

Ruang lingkup dari manajemen risiko memastikan Perangkat Daerah dapat menerapkan proses Pengelolaan Risiko yang mencakup kegiatan:

1. Penetapan konteks;
2. *Assessment* risiko;
3. Penanganan risiko;
4. Pemantauan dan peninjauan risiko;
5. Komunikasi dan koordinasi risiko.

C. Kebijakan

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

a. identifikasi risiko :
   1) mengidentifikasi ancaman, merupakan aktifitas untuk mengidentifikasi ancaman terhadap risiko keamanan informasi;
   2) ancaman didefinisikan sebagai potensi penyebab insiden yang tidak diinginkan yang dapat menyebabkan kerusakan/kerugian bagi Perangkat Daerah dan sistemnya;
   3) sebuah ancaman tidak dapat dikatakan sebuah risiko apabila tanpa kombinasi dengan kelemahan yang dapat dieskplotasi;
   4) mengidentifikasi kelemahan dilakukan setelah pengidentifikasian ancaman dilakukan;
   5) kelemahan didefinisikan sebagai potensi kekurangan pada proses dan kontrol keamanan yang dapat dieksplotasi oleh satu ancaman atau lebih;
   6) mengidentifikasi dampak merupakan aktifitas yang dilakukan untuk mengidentifikasi potensi dampak jika ancaman yang teridentifikasi, mengeksploitasi kelemahan yang ada;
   7) risiko harus dialokasikan ke pemilik risiko; dan
   8) pemilik risiko bertanggung jawab untuk mengelola risiko yang telah teridentifikasi.

b. analisis risiko :
   1) menilai dampak potensial yang akan terjadi apabila risiko yang teridentifikasi terwujud;
   2) kriteria dampak merupakan parameter untuk menentukan tingkat kerugian terhadap risiko yang terjadi.

Tabel Dampak Resiko Manajemen Keamanan Informasi

Tingkat Dampak	Operasional	Peraturan / Hukum	Aset Informasi	Reputasi
1 (ringan)	Penundaan proses bisnis setengah hari	Tidak ada pelanggaran hukum	Tidak ada kebocoran atau kehilangan aset informasi.	Tidak ada dampak terhadap reputasi Perangkat Daerah
2 (Sedang)	Penundaan proses bisnis 1 hari	Pelanggaran ringan dengan surat peringatan	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat PUBLIK.	Mengganggu kepercayaan sebagian kecil pihak eksternal. Berdampak pada reputasi Perangkat

				Daerah namun reputasi dapat dipulihkan dalam waktu tidak terlalu lama.
3 (Berat)	Penundaan proses bisnis 3 hari	Pelanggaran sedang yang dikenakan sanksi administratif	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat TERBATAS.	Mengganggu kepercayaan sebagian besar pihak eksternal. Berdampak pada reputasi Perangkat Daerah dan pemulihan reputasi membutuhkan waktu yang lama.
4 (Sangat Berat)	Penundaan lebih dari 3 hari	Pelanggaran berat dengan sanksi hukum	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat RAHASIA.	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat RAHASIA.

3) Menilai kemungkinan realistis terjadinya risiko yang teridentifikasi; dan
4) Kriteria kecenderungan merupakan parameter untuk menentukan tingkat kejadian terhadap Risiko.

kriteria kecenderungan adalah sebagai berikut:

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

5) Evaluasi risiko :
   1.1 membandingkan hasil analisis risiko dengan kriteria risiko yang sudah ditetapkan;
   1.2 risiko yang masuk dalam kriteria penerimaan risiko akan diterima;
   1.3 risiko yang tidak masuk dalam kriteria penerimaan risiko perlu mendapatkan penanganan; dan
   1.4 setiap penanganan risiko harus diberikan prioritas.

4. Hasil evaluasi risiko harus dianalisis terkait risiko tersebut dapat diterima dalam level tertentu berdasarkan kriteria penerimaan risiko yang telah ditetapkan atau memerlukan penanganan risiko lebih lanjut. Tabel risiko adalah matriks antara nilai dari dampak dan kecenderungan yang menghasilkan tingkat risiko. Tabel risiko adalah sebagai berikut :

Tabel Risiko

5. Dalam hal risiko tersebut tidak dapat diterima, Perangkat Daerah harus menerapkan penanganan risiko yang diperlukan yang mencakup:
   a. mengendalikan/*control* adalah merupakan tindakan pengendalian risiko dengan mengurangi dampak maupun kemungkinan terjadinya risiko melalui menerapkan suatu sistem atau aturan;
   b. menghindari/*avoid* adalah tindakan pengendalian risiko dengan tidak melakukan suatu aktivitas atau memilih aktivitas lain dengan output yang sama untuk menghindari terjadinya risiko;
   c. mengalihkan/transfer adalah tindakan pengendalian risiko dengan mengalihkan seluruh atau sebagian tanggung jawab pelaksanaan suatu proses kepada pihak ketiga.
6. Penanganan risiko harus memadai untuk mengurangi risiko ke tingkat yang dapat diterima berdasarkan kriteria penerimaan risiko.
7. Pemilik risiko harus memastikan setiap rencana penanganan risiko telah memadai dan relevan bagi risiko yang ada.
8. Setiap rencana penanganan risiko harus diberikan prioritas oleh pemilik risiko.
9. Setiap keputusan terkait dengan penanganan risiko dan kontrol keamanan risiko yang relevan harus disetujui oleh Pimpinan Perangkat Daerah terkait.

10. Perangkat Daerah harus melakukan proses pemantauan dan peninjauan risiko untuk memastikan efektifitas kontrol yang dilakukan yang mencakup:
    a. proses pemantauan dan peninjauan risiko adalah proses berkesinambungan untuk memastikan bahwa :
        1) risiko baru telah terindentifikasi, di-*assess* dan ditangani;
        2) setiap perubahan terhadap risiko yang sudah ada telah teridentifikasi, di-*assess* dan ditangani;
        3) kontrol keamanan yang sudah ada telah memadai dan efektif dalam menanganirisiko.
    b. proses pemantauan dan peninjauan risiko harus dilakukan secara formal dan rutin;
    c. Perangkat Daerah harus menentukan frekuensi pemantauan dan peninjauan risiko.
11. Perangkat Daerah harus melakukan proses komunikasi dan koordinasi risiko untuk memastikan pengelolaan penanganan kontrol terkendali dan efektif dalam mengurangi tingkat Risiko yang diharapkan.
12. Metode komunikasi dan koordinasi risiko harus ditetapkan yang meliputi:
    a. proses komunikasi dan koordinasi risiko merupakan proses berkesinambungan untuk mengkomunikasi dan mengkoordinasikan setiap informasi, aktifitas dan keputusan terkait dengan risiko keamanan informasi dan proses manajemen risiko;
    b. setiap informasi, aktifitas dan keputusan harus dikomunikasikan dan dikoordinasikan dengan pemilik risiko, personil terkait dan Kepala Perangkat Daerah; dan
    c. setiap komunikasi dan koordinasi eksternal terkait risiko keamanan informasi dan manajemen risiko harus disetujui oleh Kepala Perangkat Daerah.

BAB IV
KEAMANAN SUMBER DAYA MANUSIA

A. Tujuan

Kebijakan keamanan sumber daya manusia ditetapkan untuk memberikan pedoman dalam mengelola keamanan sumber daya manusia dalam ruang lingkup Tata kelola keamanan informasi dalam Sistem Manajemen Keamanan Informasi di Pemerintah Provinsi Sumatera Barat.

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan sumber daya manusia terdiri dari:

1. Pegawai dalam lingkungan Pemerintah Provinsi Sumatera Barat;
2. pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Provinsi Sumatera Barat.

C. Kebijakan

1. Pegawai di lingkungan Pemerintah Daerah dan pihak eksternal yang akan berhubungan dengan pengelolaan data dan informasi, harus melalui proses *screening* untuk memastikan bahwa mereka sesuai dengan tugas dan tanggung jawab yang akan mereka dapatkan.
2. Proses *screening* perlu mencakup verifikasi terhadap latar belakang kandidat sesuai dengan peraturan hukum perundang-undangan serta etika yang ada.
3. Pegawai dalam lingkungan Pemerintah Daerah dan pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah harus menandatangani perjanjian kerahasiaan (*non-disclosure agreement*) dengan memperhatikan tingkat sensitivitas dari aset yang diakses.
4. Setiap pegawai Pemerintah Daerah maupun pihak eksternal harus mematuhi seluruh kebijakan dan prosedur Perangkat Daerah terkait keamanan informasi.
5. Setiap pegawai Pemerintah Daerah maupun pihak eksternal harus diberikan informasi yang memadai terkait tugas dan tanggung jawab terkait keamanan informasi yang mereka miliki.

6. Program peningkatan kesadaran keamanan informasi (*awareness*) secara berkelanjutan untuk menjaga dan meningkatkan kesadaran keamanan informasi dari pegawai harus dilaksanakan.
7. Setiap pelanggaran terhadap kebijakan dan prosedur terkait Keamanan Informasi harus ditindaklanjuti dan apabila diperlukan, tindakan pendisiplinan harus diambil sesuai dengan peraturan yang berlaku.
8. Tanggung jawab dan kewajiban terkait keamanan informasi yang tetap berlaku setelah pemberhentian atau perubahan status kepegawaian harus didefinisikan, dikomunikasikan dan ditegakkan kepada pegawai Pemerintah Daerah maupun eksternal.
9. Hal ini mencakup tanggung jawab keamanan informasi yang tercakup dalam perjanjian kerja seperti:
    a. Seluruh aset organisasi harus dikembalikan setelah pemberhentian kepegawaian;
    b. Seluruh hak akses organisasi harus dinonaktifkan atau dihapus setelah pemberhentian kepegawaian; dan
    c. Seluruh hak akses organisasi harus disesuaikan setelah perubahan status kepegawaian.

BAB V

PENGELOLAAN ASET

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup kebijakan terkait pengelolaan aset informasi terdiri dari:

1. klasifikasi, pelabelan dan penanganan data dan informasi yang terdapat pada Pemerintah Daerah Provinsi Sumatera Barat terkait Tata Kelola Kemanan Informasi dan.
2. penanganan aset, pengolahan dan penyimpanan data dan informasi dalam ruang lingkup Pemerintah Provinsi Sumatera Barat.

C. Kebijakan

1. Gubernur menetapkan pemilik aset informasi di setiap Perangkat Daerah di Lingkungan Pemerintah Provinsi Sumatera Barat, beserta perangkat fisik pengolah data dan informasi yang terkait.
2. Pemilik aset data dan informasi memiliki tanggung jawab untuk:
   a. mengidentifikasi seluruh aset data dan informasi dan fasilitas pengolahan dan penyimpanan data dan informasi;
   b. mendokumentasikan dalam daftar inventaris aset terkait tata kelola keamanan informasi, serta senantiasa memperbaharui daftar inventaris aset terkait tata kelola keamanan informasi tersebut sesuai kondisi terkini; dan
   c. memastikan bahwa setiap aset telah diklasifikasikan dan dilindungi secara memadai.
3. Aset pengolahan dan penyimpanan data dan informasi yang diinventaris adalah aset dalam bentuk:
   a. perangkat keras, meliputi perangkat keras yang digunakan untuk mengolah dan menyimpan data dan informasi dalam bentuk fisik maupun elektronik, yang mencakup namun tidak terbatas pada komputer, *notebook, server*, *harddisk drive,* USB *disk*;
   b. perangkat lunak, meliputi perangkat lunak yang digunakan untuk mengolah data dan informasi dalam bentuk elektronik,

yang mencakup namun tidak terbatas pada sistem operasi, aplikasi, dan *database*;

c. perangkat jaringan, meliputi perangkat keras dan lunak yang digunakan untuk membentuk dan infrastruktur jaringan telekomunikasi, yang mencakup namun tidak terbatas pada *hub, switch, router, firewall,* IDS, IPS, dan *network monitoring tools*;

d. perangkat pendukung meliputi perangkat digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan data dan informasi yang mencakup namun tidak terbatas pada *genset,* UPS, AC, rak *server,* lemari penyimpanan informasi dan CCTV;

e. layanan, meliputi layanan yang digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan data dan informasi yang mencakup namun tidak terbatas pada layanan jaringan komunikasi, layanan *hosting* dan *co-location,* layanan pemeliharaan perangkat dan sistem, dan layanan pemasangan infrastruktur; dan

f. sumber daya manusia meliputi personil baik internal maupun eksternal yang terlibat dalam pengolahan dan penyimpanan informasi.

4. Pemilik aset dapat mendelegasikan tugas pengamanan dan pemeliharaan aset kepada pihak ketiga penyedia pengelola aset, namun tanggung jawab akhir terhadap aset tetap berada pada pemilik aset.

5. Aset pengolahan dan penyimpanan data dan informasi harus secara berkala dipelihara dengan memadai.

6. Apabila dalam pemeliharaan aset pengolahan dan penyimpanan data dan informasi tersebut harus menggunakan jasa pihak ketiga penyedia, maka:

   a. kontrak pemeliharaan perlu dibuat dengan pihak ketiga penyedia jasa yang kompeten dan relevan; dan

   b. peralatan yang dibawa keluar untuk pemeliharaan harus diperiksa untuk mencegah kebocoran informasi.

7. dalam proses penghapusan aset harus dilakukan secara aman dengan metode yang dapat mencegah kebocoran data dan informasi seperti menghancurkan secara fisik harddisk drive.

8. Semua aset data dan informasi serta pengolahan dan penyimpanan informasi milik Pemerintah Daerah Provinsi Sumatera Barat harus dikembalikan setelah personil pengguna tidak memiliki hubungan kepegawaian lagi dengan Pemerintah Provinsi Sumatera Barat , misalnya karena pengunduran diri, pension atau pindah tugas.

9. Ketentuan dalam proses pengembalian aset tersebut mencakup:
   a. pengembalian aset harus terdokumentasi secara formal;
   b. untuk pengembalian aset yang disebabkan oleh terhentinya status kepegawaian, informasi yang tersimpan dalam aset harus di-backup dan informasi yang tersimpan dalam aset harus dihapus secara aman, antara lain dengan secureformat atau melakukan instalasi ulang sistem operasi secara menyeluruh; dan
   c. media penyimpanan backup informasi harus diamankan secara fisik, antara lain dengan menyimpan dalam lemari terkunci dengan akses yang terbatas.
10. Aset pengolahan informasi, seperti komputer dan laptop yang akan digunakan kembali baik oleh pihak internal maupun eksternal harus diperiksa untuk menjamin tidak ada informasi sensitif yang tersimpan dalam aset tersebut.
11. Perangkat Daerah harus mendefinisikan klasifikasi aset informasi dengan mempertimbangkan sebagai berikut:
    a. Aset informasi diklasifikasikan berdasarkan tingkat sensitivitas informasi serta tingkat kritikalitas sistem, yang meliputi:
       1) klasifikasi aset informasi secara berkala; dan
       2) pengguna yang diijinkan mengakses aset informasi.
    b. pemberian label klasifikasi informasi harus dilakukan secara konsisten terhadap seluruh aset informasi;
    c. klasifikasi aset informasi dan seberapa tingkat kerahasiaan aset informasi, didefinisikan sesuai ketentuan peraturan perundang-undangan, diuraikan sesuai tabel berikut:

Klasifikasi Aset Informasi	Deskripsi
Rahasia*(Confidential)*	Aset Informasi yang sangat peka dan beresiko tinggi yang pembocoran atau penyalahgunaan akses terhadapnya bisa mengganggu kelancaran operasional secara temporer atau mengganggu citra dalam reputasi instansi
Internal*(InternalUse Only)*	Informasi yang telah terdistribusi secara luas di lingkungan internal instansi/ lembaga yang penyebarannya secara internal tidak lagi memerlukan izin dari pemilik informasi dan resiko penyebarannya tidak menimbulkan kerugian signifikan

Publik	Aset informasi yang secara sengaja dipublikasikan secara luas, merupakan informasi yang wajib disediakan dan diumumkan secara serta merta, dan informasi yang wajib tersedia setiap saat

12. Untuk kepentingan penyelenggaraan pengelolaan aset informasi dalam Kebijakan Sistem Manajemen Keamanan Informasi dalam pelaksanaan tata kelola keamanan informasi perlu diberikan penjelasan contoh-contoh aset informasi rahasia dan internal, yaitu:

Klasifikasi Aset Informasi	Contoh
Rahasia (Confidential)	User ID, Password, Personal Identification Number (PIN), Log Sistem, Hasil *Penetration test*, data konfigurasi sistem, *Internet Protocol Address* (IP Address)
Internal (Internal Use Only)	Panduan penggunaan sistem dan aplikasi, kebijakan dan prosedur keamanan informasi, dokumen *Business Continuity* Plan

13. Setiap pemilik data dan informasi harus memperhatikan keamanan data dan informasi yang tersimpan dalam media penyimpanan informasi antara lain:
    a. dalam hal data yang tersimpan di dalam media bersifat rahasia, perlu diberikan proteksi kata sandi untuk melindungi data;
    b. dalam hal tidak lagi dibutuhkan atau digunakan, seluruh data yang tersimpan beserta seluruh backupan data dan informasi tersebut di dalam media harus sepenuhnya dihapus sehingga tidak lagi dapat dipulihkan;
    c. data yang tersimpan di dalam media yang akan dibuang harus mendapatkan perlakuan khusus guna meminimalkan terjadinya kebocoran informasi kepada pihak yang tidak sah, yaitu:
        1) data yang tersimpan di dalam media yang memuat informasi rahasia harus dibuang dengan cara dihancurkan atau dibakar; dan
        2) data yang tersimpan di dalam media yang memuat informasi lainnya harus dilakukan penghapusan total dengan cara-cara tertentu yang tidak lagi dapat dipulihkan.
14. Panduan terkait pelabelan dan penanganan aset informasi berdasarkan klasifikasi aset informasi adalah sebagai berikut:

Kalsifikasi Tipe	Publik	Internal	Rahasia

Dokumen dan catatan (record) dalam bentuk non elektronik (hardcopy)	Tidak diperlukan penanganan khusus	Diberi label Internal	Diberi label rahasia
Map penyimpanan dokumen	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Diberi label rahasia
Amplop pengiriman surat internal (didalam kantor)	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Amplop diberi label rahasia
Amplop untuk surat eksternal (keluar kantor)	Tidak diperlukan penanganan khusus	Pada amplop ditandai internal	• Menggunakan 2 amplop, dimana amplop pertama dimasukan kedalam amplop kedua; • Pada amplop pertama ditandai “rahasia” dan pada amplop kedua tidak diberikan tanda apapun.
Dokumen dan catatan (record) dalam bentuk elektronik (softcopy)	Tidak diperlukan penanganan khusus	Memberikan label internal pada bagian awal dari nama file atau pada bagian tertentu dari file properties	Memberikan label rahasia pada bagian tertentu dari *file properties*
Publikasi/distribusi	Tidak ada pembatasan	• Tersedia untuk personal internal SKPD pemilik informasi • Distribusi kepada pihak eksternal dibatasi	• Distribusi kepada pihak eksternal sangat dibatasi untuk kebutuhan pekerjaan. • Apabila memungkinkan, informasi rahasia tidak disalin oleh pihak eksternal

		berdasakan kebutuhan pekerjaan maupun operasional di lingkungan Pemda. • Distribusi kepada pihak eksternal perlu seijin pemilik informasi. • Sensitifitas dan kritikalitas informasi perlu diberitahukan kepada	(*eyes only*). • Distribusi kepada pihak eksternal perlu seijin pemilik Informasi. • Sensitifitas dan kritikalitas informasi perlu diberitahukan kepada pihak eksternal. • Pihak ketiga harus disertai perjanjian kerahasiaan (NDA - *non disclosure agreement*).
Pencetakan informasi	Tidak ada pembatasan.	Dibatasi hanya untuk kebutuhan internal.	Pencetakan hanya pada *printer* organisasi dan diusahakan tidak mencetak menggunakan jasa pencetakan eksternal.
Surat menyurat internal (di dalam kantor)	Pastikan nama dan alamat tujuan sudah benar.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat internal.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat internal. • Menginformasikan kepada penerima akan pengiriman informasi tersebut. • Mengkonfirmasi kepada penerima bahwa informasi yang dikirim

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

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

			eksternal (*externalharddisk*, atau *flashdisk*) harus disimpan pada tempat penyimpanan yang terkunci.
Penyimpanan pada pihak ketiga	Tidak diperlukan penanganan khusus	Harus disertai dengan perjanjian kerahasiaan (*non disclosure agreement* - NDA).	Harus disertai dengan perjanjian kerahasiaan (*non disclosure agreement* - NDA).
Penghancuran (*disposal*)	• Tidak diperlukan penanganan khusus. • Masih dapat digunakan kembali sebagai kertas untuk pekerjaan (*scrap paper*).	• Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi. • Masih dapat digunakan kembali untuk kebutuhan mencetak informasi dengan klasifikasi yang sama.	• Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi • Dihancurkan dengan metode pemusnahan dan informasi tidak dapat diakses kembali (dihancurkan secara fisik atau *secure format*).
Pengamanan pada komputer penyimpan informasi	Tidak diperlukan penanganan khusus.	• *Screen saverlock* harus aktif jika meninggalkan komputer / terminal. • *Sign-off* komputer / terminal jika tidak digunakan atau pulang kerja	• *Screen saverlock* harus aktif jika meninggalkan komputer / terminal. • *Sign-off* komputer / terminal jika tidak digunakan atau pulang kerja. • *File perlu* dienkripsi / *password*.
Kehilangan atau kebocoran	Tidak diperlukan penanganan	Harus dilaporkan kepada pemilik	Harus dilaporkan kepada pemilik informasi dan unit kerja pengelola

informasi	khusus.	informasi	insiden keamanan informasi di lingkungan Pemerintah Daerah.

15. Informasi yang dianggap kritikal oleh Perangkat Daerah harus di-*backup* secara memadai untuk menjamin ketersediaannya.
16. hal yang perlu dipertimbangkan dalam proses backup informasi meliputi:
    a. pemilik informasi bertanggung jawab untuk menentukan informasi yang membutuhkan *backup*, frekuensi dan metode *backup* serta waktu retensi untuk setiap *backup* informasi yang ada;
    b. pernyataan formal terkait informasi yang dibutuhkan untuk di-*backup* beserta metode dan frekuensi dari *backup* harus ditentukan bersama dengan personil yang bertugas melaksanakan proses *backup* serta harus dinyatakan secara jelas dalam sebuah rencana *backup* resmi;
    c. *backup* informasi harus disimpan sesuai dengan masa retensi dari informasi utama;
    d. masa retensi harus dinyatakan secara jelas dalam rencana *backup*; dan
    e. perlindungan terhadap *backup* informasi harus dilakukan berdasarkan klasifikasi dari informasi utama.
17. Perangkat Daerah menyediakan akses *internet* dan *email* kepada pegawainya hanya untuk kebutuhan pekerjaan dan operasional Pemerintah Provinsi Sumatera Barat .
18. Ketentuan dalam pengguaan internet dan email adalah sebagai berikut:
    a. pengguna dilarang menggunakan akses internet dan *email* Perangkat Daerah untuk kegiatan melanggar hukum dan aktifitas yang dapat membahayakan keamanan jaringan Pemerintah Daerah;
    b. pengguna dilarang untuk menggunakan akses internet dan *email* Perangkat Daerah untuk mengakses, mendistribusikan, mengunggah dan/atau mengunduh:
        1) materi pornografi;
        2) materi bajakan seperti, perangkat lunak, *file* musik dan *video*/*film*;

3) materi yang melecehkan, mendiskriminasikan, yang membakar emosi atau menimbulkan kebencian atau membuat pernyataan palsu atau yang bersifat merusak mengenai orang lain;
4) situs yang dapat menimbulkan risiko serangan malware, penyusupan atau *hacking* ke jaringan Pemerintah Daerah.

19. pengguna disarankan untuk tidak membagi informasi pribadi melalui situs internet atau media sosial.
20. pengguna dilarang untuk mendistribusikan informasi Pemerintah Daerah yang bersifat rahasia tanpa izin dari pemilik informasi.
21. pesan penyangkalan ini harus dituliskan pada akhir setiap e-mail. "*Pesan ini mungkin berisi informasi rahasia dan hanya ditujukan kepada pihak yang dituju. Apabila anda bukanlah pihak yang dituju, anda dilarang untuk mengungkapkan, menyebarkan atau menyalin isi email ini. Apabila anda mendapatkan email ini tanpa sengaja mohon segera hubungi pengirim email dan hapus email ini segera. Pemerintah Daerah Provinsi Sumatera Barat tidak bertanggung jawab untuk pengiriman informasi ini secara lengkap dan tepat dan juga tidak bertanggung jawab untuk keterlambatan dalam pengiriman email ini.*"
22. Dinas yang mengelola akun *email* Perangkat Daerah berhak untuk mem-*block* akun *email* Perangkat Daerah dan akun email dinas Pegawai pada saat terdapat bukti memadai terkait penyalahgunaan dan/atau pelanggaran keamanan.

BAB VI
PENGENDALIAN AKSES

A. Tujuan

Tujuan dari pengendalian akses adalah untuk:

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

B. Ruang Lingkup

Ruang Lingkup dari pengendalian akses adalah akses ke aset data dan informasi dan aset pengolahan dan penyimpanan data dan informasi dalam lingkungan Pemerintah Daerah Provinsi Sumatera Barat yang mencakup :

1. persyaratan pengendalian akses;
2. pengendalian akses jaringan;
3. pengelolaan akses pengguna;
4. tanggung jawab pengguna; dan
5. pengendalian akses atas sistem dan aplikasi.

C. Kebijakan

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

g. peninjauan terhadap hak akses pengguna harus didokumentasikan secara formal; dan
h. setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan cara menyesuaikan atau mencabut hak akses yang menyimpang.

2. Pengendalian akses jaringan di lingkungan Perangkat Daerah meliputi:
   a. penggunaan layanan jaringan (*network services*) hanya diperbolehkan secara terbatas, sesuai kebutuhan ketugasan dan kepentingan Perangkat Daerah, layanan lainnya yang tidak diperlukan harus dinonaktifkan;
   b. jaringan komunikasi dalam lingkungan Perangkat Daerah harus dipisahkan kedalam *domain* jaringan yang terpisah sesuai dengan kebutuhan dan operasional, dalam rangka untuk mengamankan jaringan internal Perangkat Daerah dan aset di jaringan tersebut;
   c. akses secara *remote* ke jaringan internal Perangkat Daerah dari jaringan publik harus sangat dibatasi baik dari perangkat yang digunakan maupun waktu untuk kebutuhan *troubleshooting* dan harus dilakukan melalui *secure channel*, antara lain dengan menggunakan teknologi VPN; dan
   d. pemberian akses pengguna terhadap jaringan, baik LAN maupun WAN, dilakukan melalui mekanisme formal.

3. Pengelolaan akses terhadap pengguna di Perangkat Daerah harus memenuhi ketentuan sebagai berikut:
   a. pemilik Aset Informasi harus memiliki manajemen identitas pengguna yang mencakup proses pendaftaran dan terminasi pengguna, yang didalamnya termasuk:
      1) identitas pengguna (*user account*) harus unik, melekat ke setiap individu tunggal, sehingga setiap tindakan pengguna dapat dipertanggungjawabkan;
      2) tidak diijinkan menggunakan satu identitas pengguna yang digunakan secara bersama-sama oleh lebih dari satu individu, kecuali untuk tujuan tertentu yang sebelumnya harus mendapatkan persetujuan dari pihak berwenang; dan
      3) memastikan secara berkala bahwa tidak ada identitas pengguna yang terduplikasi atau redundan sehingga seluruh identitas pengguna aktif adalah sesuai dengan pegawai Perangkat Daerah aktif.
   b. pendaftaran, modifikasi dan pencabutan hak akses pengguna mencakup proses pembuatan *user* ID, memberikan hak akses kepada *user* ID serta mencabut hak akses dan *user* ID.
   c. pendaftaran, modifikasi dan pencabutan hak akses pengguna harus disetujui oleh atasan dari pengguna yang memohon hak akses

tersebut dan pemilik informasi dan/atau sistem. Persetujuan tersebut harus diberikan sesuai dengan aturan pemberian akses.

d. identitas pengguna harus diotorisasi secara formal oleh pejabat berwenang pada pemilik aset informasi. Akses atas sistem dan aplikasi hanya dapat diaktifkan jika proses otorisasi telah selesai.
e. identitas pengguna pada sistem, seperti *user* ID, harus bersifat unik untuk memungkinkan mengidentifikasi dan meminta pertanggungjawaban pengguna.
f. pemberian informasi otentikasi suatu pengguna yang bersifat rahasia harus dilakukan melalui proses formal yang mencakup:
    1) informasi otentikasi perdana yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama mengakses sistem atau aplikasi;
    2) informasi otentikasi bawaan (*default*) dari penyedia barang/jasa harus segera diganti pada saat instalasi sistem atau aplikasi;
g. pemilik Aset harus melakukan tinjauan secara berkala atas seluruh hak akses pengguna secara berkala, dengan tambahan tinjauan insidental yang dilakukan pada saat:
    1) terjadinya proses kepegawaian, seperti promosi, mutasi, terminasi; dan
    2) terjadinya perubahan struktur organisasi.
h. hak akses khusus (*privileged access rights*) dari sistem informasi dalam lingkungan Perangkat Daerah, seperti *administrator, root,* hak akses untuk memodifikasi *database* atau hak akses untuk membuat, memodifikasi atau mencabut pengguna dalam sistem aplikasi, harus sangat dibatasi kepada personil yang terotorisasi dan sedapat mungkin hanya dimiliki oleh pegawai Negeri Sipil (PNS) atau Aparatur sipil Negara (ASN).
i. Hak akses khusus harus disetujui dan didokumentasikan secara formal.
j. alokasi dari hak akses khusus harus ditinjau secara berkala dan setiap terdapat perubahan dalam status penggunaan akses tersebut.
k. setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan menyesuaikan atau menghapus hak akses khusus yang menyimpang.
l. apabila memungkinkan, hak akses khusus harus dialokasikan secara individual dan tidak di-*share*. Hal ini dilakukan untuk menjamin akuntabilitas dari pengguna khusus.
m. Apabila hak akses khusus tidak bisa dialokasikan secara individual, kontrol tambahan seperti *dual custody,* harus diimplementasikan untuk menghindari penyalahgunaan.

n. jejak audit (*log*) untuk hak akses khusus pada sistem informasi dalam lingkungan Pemerintah Daerah harus diaktifkan.

4. Setiap pengguna harus mempunyai tanggung jawab dalam penggunaan *User ID* dan *password* yaitu:
   a. pengguna harus menjaga kerahasiaan dan keamanan *password* pribadi atau kelompok serta informasi otentikasi rahasia lainnya*;*
   b. pengguna harus segera mengganti informasi otentikasi rahasia jika terindikasi bahwa informasi tersebut telah diketahui oleh orang lain;
   c. *password* yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama pada saat mengakses sistem atau aplikasi;
   d. *password* untuk mengakses sistem informasi dalam lingkungan Perangkat Daerah harus memiliki karakteristik sebagai berikut:
      1) memiliki panjang minimum 12 karakter;
      2) mengandung kombinasi huruf besar, huruf kecil dan nomor;
      3) tidak terdiri dari kata atau nomor yang mudah ditebak seperti password, admin, 12345678 atau abc123; dan
      4) tidak terdiri dari informasi pribadi seperti ulang tahun pengguna, nama Perangkat Daerah atau nama pengguna;
   e. *password* untuk mengakses sistem informasi dalam lingkungan Pemerintah Daerah harus diganti paling sedikit setiap 3 (tiga) bulan sekali;
   f. pada saat penggantian, *password* sebelumnya tidak boleh digunakan kembali sampai setelah 3 siklus pergantian *password*;
   g. prosedur *login* dari sistem harus menjamin keamanan dari *password* dengan cara:
      1) tidak menampilkan *password* yang dimasukkan;
      2) tidak menyediakan pesan bantuan pada saat proses *login* yang dapat membantu pengguna yang tidak berwenang;
   h. pengguna wajib menggunakan kata sandi yang berbeda untuk keperluan ketugasan dan pribadi.
5. pengendalian akses sistem dan aplikasi yang dikelola oleh Perangkat Daerah meliputi:
   a. pemilik aset informasi harus memastikan bahwa sistem dan aplikasi dibawah pengelolaannya memiliki fasilitas manajemen hak akses pengguna, manajemen kata sandi yang baik, serta mekanisme otentikasi pengguna yang aman;
   b. fasilitas manajemen hak akses pengguna harus mampu membatasi akses informasi sesuai ketugasannya (*role based access control*);

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

Parameter Otentikasi	Rahasia & Internal	Publik
Jumlah gagal *login* sebelum penguncian	3 kali	10 kali
Durasi *timeout* sebelum terminasi sesi otomatis	5 Menit	20 menit

6. penggunaan program *utility khusus* dalam operasional sistem di lingkungan Perangkat Daerah harus mempertimbangkan keamanan sebagai berikut yaitu penggunaan program *utility* khusus seperti *registry cleaner* atau *system monitoring* yang dapat mengambil alih

kendali sistem/aplikasi atau mendapatkan hak akses khusus pada sistem/aplikasi harus sangat dibatasi berdasarkan kebutuhan operasional pengguna.

7. Perangkat Daerah yang mengelola aplikasi harus memastikan bahwa *source code* dikelola dan disimpan secara memadai baik yang dikembangkan oleh internal Perangkat Daerah maupun yang dikembangkan oleh penyedia jasa aplikasi.
8. Apabila *source code* dari penyedia jasa aplikasi tidak dapat diserahkan kepada pengelola aplikasi, Perangkat Daerah bersama penyedia jasa aplikasi tersebut harus mempertimbangkan *escrow aggreeement* untuk memastikan kelangsungan operasional sistem aplikasi jika ada pengembangan selanjutnya.
9. Pengendalian terhadap akses ke *source code* aplikasi sebagai berikut:
   a. Untuk sistem aplikasi yang dikembangkan secara internal dan/atau dibeli dengan *source code*, pengendalian akses harus diimplementasikan untuk mencegah akses tanpa izin ke *source code* tersebut.
   b. Pengendalian tersebut mencakup:
      1) Tidak menyimpan *source code* pada sistem operasional;
      2) Menyimpan *source code* pada lokasi fisik yang aman dari ancaman akses tanpa izin maupun ancaman kerusakan karena kondisi lingkungan;
      3) Membatasi akses secara fisik maupun logical ke *source code* program hanya kepada pengembang dan personil yang berwenang;
      4) Mengimplementasikan metode *versioning* dan proses manajemen perubahan untuk menjamin integritas dari *source code* aplikasi.

BAB VII
KRIPTOGRAFI

A. Tujuan

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

B. Ruang Lingkup

Ruang Lingkup kebijakan terkait teknologi kriptografi adalah penggunaan teknologi kriptografi dalam pengolahan dan penyimpanan informasi di lingkungan Pemerintah Daerah .

C. Kebijakan

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

BAB VIII

KEAMANAN FISIK DAN LINGKUNGAN

A. Tujuan

Tujuan dari kebijakan keamanan fisik dan lingkungan adalah untuk:

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

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan fisik dan lingkungan adalah pengamanan fisik dan lingkungan bagi area kerja dan penyimpanan perangkat pengolahan dan penyimpanan data dan informasi, seperti *data center*, *disaster recovery center* atau ruang arsip.

C. Kebijakan

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

f. area bongkar muat atau penerimaan barang harus diamankan dan dipantau untuk mencegah akses tanpa izin ke *data center, disaster recovery center* dan ruang arsip Pemerintah Daerah ; dan

g. *delivery* dari barang harus dilaporkan dan diperiksa sebelum barang tersebut dapat dipindahkan dari area bongkar muat atau penerimaan barang ke *data center, disaster recovery center* dan ruang arsip Pemerintah Daerah.

4. Pengendalian akses pengunjung ke dalam area di lingkungan Perangkat Daerah harus memperhatikan keamanan fisik yang meliputi:
   a. kunjungan ke dalam area tersebut harus disetujui secara formal oleh pengelolaan area tersebut;
   b. selama kunjungan di dalam area tersebut, pengunjung harus senantiasa didampingi oleh petugas yang telah mendapatkan otorisasi;
   c. kartu identitas pengunjung perlu diverifikasi, disimpan oleh petugas selama kunjungan, dan dikembalikan sesudah selesai kunjungan; dan
   d. setiap pengunjung ke dalam area harus tercatat, mencakup jam masuk dan keluar, serta selalu dimonitor kesesuaiannya dengan rekaman CCTV.
5. Perangkat Daerah harus memperhatikan aspek pengamanan terhadap perangkat yang digunakan melalui:
   a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya pencurian, akses oleh pihak yang tidak berwenang, kebakaran, air, debu, dan sebagainya;
   b. seluruh perangkat di dalam area harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang berwenang untuk menjamin keberlangsungan efektivitas fungsionalnya;
   c. pemeliharaan yang dilakukan oleh pihak ketiga, harus dilaksanakan sesuai dengan kesepakatan tingkat layanan *(service level agreement/ SLA*) yang menjabarkan tingkat pemeliharaan dan kinerja yang harus dipenuhi pihak ketiga;
   d. bagi pemeliharaan yang tidak dapat dilakukan di lokasi kantor Perangkat Daerah, maka informasi rahasia dan kritikal yang tersimpan dalam peralatan tersebut harus dipindahkan terlebih dahulu;
   e. pemeliharaan perangkat yang mengharuskan dibawa dari luar area harus atas persetujuan pejabat berwenang.

f. peralatan pengolahan dan penyimpanan informasi yang tidak digunakan lagi oleh Pemerintah Daerah, baik karena rusak, diganti, atau karena sebab lainnya harus dipastikan tidak lagi menyimpan informasi sensitif dan kritikal; dan

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

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

a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya kebakaran, kebocoran, debu, dan sebagainya;

b. seluruh perangkat di dalam *data center* harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang kompeten dan berwenang sesuai dengan rekomendasi dari pembuat perangkat tersebut;

c. *data center* harus dilengkapi dengan ups, generator listrik cadangan, perangkat pemadam kebakaran, dan diusahakan terdapat perlindungan kejut listrik (petir, tegangan tidak stabil);

d. *data center* dan *disaster recovery center* dilengkapi dengan sistem sensor deteksi asap, air, suhu dan kelembaban, yang dapat terpantau;

e. parameter temperatur dan kelembaban berikut perlu dijaga untuk *data center* meliputi:

1) temperatur antara 18° - 26° celcius;

2) kelembaban (rh) antara 40% - 60%.

f. kabel listrik dan jaringan telekomunikasi yang membawa data atau mendukung layanan sistem informasi harus dilindungi dari penyambungan yang tidak sah (penyadapan) atau kerusakan.

BAB IX

KEAMANAN OPERASIONAL SISTEM INFORMASI

A. Tujuan

Tujuan dari kebijakan keamanan operasional sistem informasi adalah untuk:

1. Memastikan pengoperasian aset pengolahan dan penyimpanan data dan informasi di Pemerintah Daerah secara benar dan aman;
2. Memastikan terlindunginya aset data dan informasi beserta aset pengolahan dan penyimpanan data dan informasi di Pemerintah Daerah dari ancaman *malware;*
3. Melindungi terjadinya kehilangan atas aset data dan informasi;
4. Tersedianya catatan (*log*) atas aktivitas sistem informasi sebagai barang bukti; dan
5. Mencegah terjadinya eksploitasi atas kelemahan sistem informasi pada Pemerintah Provinsi Sumatera Barat .

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan operasional sistem informasi adalah pengoperasian aset pengolahan dan penyimpanan informasi di lingkungan Pemerintah Daerah.

C. Kebijakan

1. Aktivitas operasional terkait fasilitas pengolahan data dan informasi serta fasilitas komunikasi harus memiliki prosedur yang terdokumentasi dengan baik;
2. Prosedur operasional tersebut harus tersedia bagi pengguna yang memerlukannya;
3. Seluruh perubahan pada fasilitas pengolahan informasi yang dapat berimplikasi pada Keamanan Informasi, perlu diperlakukan secara terkendali, mencakup antara lain:
   a. menyusun perencanaan mengenai perubahan yang mungkin terjadi serta melakukan pengujian terkait terpenuhinya persyaratan keamanan;
   b. melakukan kajian atas implikasi Keamanan Informasi yang mungkin terjadi;
   c. mengajukan persetujuan secara formal atas perubahan yang akan dilakukan; dan
   d. mencatat seluruh perubahan yang telah dilakukan.

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

Parameter Backup	Klasifikasi Sistem	
	Vital	*Sensitive/ Non-Sensitive*
Cakupan Backup	Aplikasi, Database	Aplikasi, Database
Frekuensi Backup	Harian	Bulanan

(Recovery PointObjective)		
Pengujian *Restore*	Triwulanan	Semesteran

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

BAB X

KEAMANAN KOMUNIKASI

A. Tujuan

Tujuan dari kebijakan keamanan komunikasi adalah untuk:

1. memastikan perlindungan atas informasi pada jaringan komputer beserta fasilitas pendukung pengolahan informasi;
2. menjaga keamanan informasi yang dipertukarkan, baik di dalam Perangkat Daerah maupun antar Perangkat Daerah eksternal.

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan komunikasi adalah untuk:

1. pengendalian jaringan;
2. keamanan layanan jaringan;
3. pemisahan jaringan; dan
4. pertukaran informasi.

C. Kebijakan

1. Jaringan internal Perangkat Daerah harus diamankan untuk menjamin:
   a. pencegahan akses tanpa izin ke jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan;
   b. keamanan dari informasi milik Perangkat Daerah yang dikirimkan melalui jaringan; dan
   c. integritas dan ketersediaan dari layanan jaringan organisasi.
2. Tugas dan tanggung jawab untuk pengelolaan jaringan dan keamanan harus dialokasikan dan apabila memungkinkan dipisahkan dari penanggung jawab opersional sistem aplikasi dan *data center*.
3. Konfigurasi dari jaringan, perangkat aktif dan perangkat keamanan jaringan harus ditinjau secara berkala untuk:
   a. memastikan kesesuaian dengan kondisi terkini; dan
   b. mengidentifikasi kerawanan pada jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan.
4. Jaringan internal Perangkat Daerah harus dipisahkan dari jaringan eksternal dengan menggunakan *security gateway* atau *firewall*dan harus dikonfigurasikan untuk:
   a. memfilter *traffic* tanpa izin maupun *traffic* yang mencurigakan; dan
   b. apabila memungkinkan memfilter dan mencegah infeksi *malware* ke jaringan internal*;*

5. Koneksi ke *security gateway* atau *firewall* harus diotentikasikan, diotorisasi dan diamankan dengan metode pengamanan yang sesuai, misalnya dengan *virtual private network* (VPN), *secure shell* (SSH) atau metode kriptografi.
6. Kebijakan dan log *firewall* harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan.
7. Koneksi eksternal harus diputuskan secara otomatis setelah tidak aktif selama 20 menit.
8. Akses dari jaringan eksternal yang dilakukan oleh *vendor* pihak ketiga hanya dapat diberikan untuk kebutuhan *troubleshooting* dan harus secara formal disetujui dan didokumentasikan dan harus dibatasi waktunya sesuai dengan kebutuhan dari akses.
9. Jaringan internal Perangkat Daerah harus disegmentasi baik secara fisik maupun *logical* untuk meningkatkan keamanan dan untuk mengendalikan akses dan *traffic* jaringan berdasarkan kritikalitas dari sistem dalam jaringan Perangkat Daerah.
10. Segmentasi jaringan harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan untuk menjamin kesesuaian dengan prasyarat keamanan terkini.
11. *Routing* jaringan harus dilakukan berdasarkan pengendalian terhadap alamat sumber dan tujuan.
12. Tanggung jawab untuk merubah *routing* jaringan hanya diberikan kepada administrator jaringan yang diberi izin.
13. Aturan untuk *routing* harus ditinjau paling tidak satu kali dalam tiga bulan untuk mendeteksi dan mengkoreksi adanya kesalahan atau *routing* tanpa otorisasi.
14. Perangkat jaringan harus ditempatkan pada lokasi yang aman untuk menghindari akses tanpa izin dan ancaman fisik maupun lingkungan.
15. Akses, baik fisik maupun *logical* ke perangkat jaringan harus dibatasi untuk tujuanadministrasi dan pemeliharaan jaringan.
16. *Port* dan layanan jaringan, baik fisik maupun *logical,* yang tidak digunakan tidak boleh diaktifkan.
17. Akses ke *port* yang digunakan untuk kebutuhan *diagnostic* dan konfigurasi perangkat jaringan dan keamanan jaringan, seperti *console port,* harus sangat dibatasi dan diberikan kepada:
    a. administrator jaringan dan keamanan jaringan Perangkat Daerah;
    b. pihak ketiga yang telah disetujui dan bekerja untuk kepentingan Perangkat Daerah.
    c. aplikasi monitoring jaringan dan keamanan jaringan yang telah disetujui.

18. Semua perangkat jaringan harus dapat diidentifikasi secara fisik maupun *logical* dengan penamaan yang disepakati dan konsisten.
19. Perangkat jaringan yang dimiliki oleh pihak eksternal harus secara memadai dipisahkan dari perangkat jaringan milik Perangkat Daerah.
20. Mekanisme keamanan, tingkat layanan dan prasyarat lain untuk semua layanan jaringan harus diidentifikasi dan dimasukkan kedalam perjanjian layanan jaringan.
21. Akses ke layanan jaringan Perangkat Daerah hanya diberikan kepada personil yang terotorisasi berdasarkan prinsip *need to have*.
22. Penggunaan pihak ketiga penyedia layanan jaringan harus dimonitor untuk menjamin kesesuaian dengan prasyarat keamanan Perangkat Daerah.
23. Layanan jaringan organisasi harus diamankan menggunakan metode yang dapat mencakup metode otentikasi atau metode kriptografi yang kuat untuk menjamin keamanan dari pengiriman informasi menggunakan jaringan dan layanan jaringan.
24. Terkait aspek pertukaran data dan informasi melalui fasilitas jaringan komunikasi, Perangkat Daerah harus memperhatikan perjanjian kerahasiaan merupakan perikatan formal antara pemilik aset data dan informasi dengan penerima data dan informasi, yang ketentuan didalamnya memuat:
    a. pemberian izin penggunaan data dan informasi dari pemilik aset data dan informasi kepada penerima data dan informasi untuk keperluan dan periode waktu yang spesifik, dimana pihak penerima data dan informasi wajib menjaga kerahasiaan data dan informasi serta mengupayakan pencegahan terjadinya kebocoran atau penyebaran data dan informasi secara tidak sah;
    b. hak dari pemilik aset data dan informasi untuk melakukan audit dan pemantauan aktivitas penerima data dan informasi berkaitan dengan penggunaan informasi sensitif; dan
    c. konsekuensi yang harus ditanggung penerima data dan informasiapabila terjadi pelanggaran atas perjanjian kerahasiaan.

BAB XI
AKUISISI, PENGEMBANGAN DAN PEMELIHARAAN SISTEM

A. Tujuan

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

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan komunikasi adalah untuk:

1. persyaratan keamanan sistem informasi;
2. keamanan dalam proses pengembangan dan *support;*
3. data pengujian.

C. Kebijakan

1. Perangkat Daerah harus menetapkan dan mendokumentasikan secara jelas persyaratan keamanan data dan informasi yang relevan sebelum pengembangan, perluasan, atau pengadaan sistem informasi baru.
2. Persyaratan keamanan harus diidentifikasi secara jelas di dalam dokumen persyaratan dan spesifikasi perangkat lunak (*Software)*
3. Spesifikasi ini harus disetujui oleh pemilik data dan informasi, pemilik proses bisnis dan pengembang sistem, sebelum fase pengkodean (*coding*) dalam pengembangan system.
4. Informasi yang digunakan oleh aplikasi Perangkat Daerah yang ditransimisikan melalui jaringan publik (internet) harus diamankan dari aktivitas penipuan, kemungkinan adanya perselisihan kontrak, dan pengungkapan dan/atau perubahan informasi tanpa izin.
5. Pengamanan informasi terhadap informasi yang ditransmisikan melalui sistem informasi yang digunakan dapat mencakup namun tidak terbatas pada:
   a. Proses otentikasi dan otorisasi terhadap pengguna aplikasi;
   b. Perlindungan untuk memastikan kerahasiaan dan integritas informasi yang dipertukarkan melalui jaringan publik;
   c. Perlindungan terhadap *session* transaksi untuk menghindari duplikasi dan/atau modifikasi;
   d. Mengamankan jalur komunikasi antara pihak-pihak yang terlibat
6. Aturan untuk pengembangan sistem harus ditetapkan dan diimplementasikan untuk proses pengembangan sistem di Perangkat Daerah yang mencakup:

a) pengamanan dari lingkungan pengembangan, seperti pemisahan lingkungan pengembangan baik secara fisik dan/atau logical, pengendalian akses, pengelolaan perubahan;
b) panduan *secure coding*;
c) pengedalian versi aplikasi;
d) penyimpanan dari *source code*;
e) metode pengujian untuk mengidentifikasi dan memperbaiki *vulnerability*.

7. Perubahan terhadap sistem selama siklus pengembangan sistem harus dikendalikan melalui proses manajemen perubahan yang berlaku di Perangkat Daerah;
8. Apabila *platform* operasional, misalnya sistem operasi, *database* dan/atau *middleware*, dari sistem informasi Perangkat Daerah mengalami perubahan, aplikasi kritikal Perangkat Daerah harus ditinjau dan diuji untuk memastikan tidak ada dampak buruk terhadap operasional dan keamanan organisasi;
9. Perangkat Daerah harus menetapkan lingkungan pengembangan yang aman untuk pengembangan dan integrasi sistem Perangkat Daerah. Hal ini dapat mencakup namun tidak terbatas pada:
    a. Pemisahan lingkungan pengembangan baik secara fisik dan/atau logical;
    b. Pengendalian akses;
    c. Perpindahan data dari dan ke lingkungan pengembangan;
10. Perangkat Daerah harus mengawasi aktivitas pengembangan sistem yang dialihdayakan (*outsourced*). Hal ini dapat mencakup:
    a. perjanjian terkait lisensi dan kepemilikan sistem;
    b. pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari sistem;
    c. prasyarat dokumentasi untuk sistem;
    d. perjanjian dengan pihak ketiga sebagai penjamin;
    e. hak untuk melakukan audit proses pengembangan dan kontrol yang diimplementasikan oleh vendor.
11. Pengujian dari fitur keamanan sistem harus dilakukan pada saat pengembangan sistem informasi Perangkat Daerah;
12. Pengujian ini dilakukan berdasarkan prasyarat keamanan sistem yang telah ditetapkan;
13. Kriteria dan jadwal untuk pengujian penerimaan sistem harus ditetapkan untuk sistem informasi baru, *upgrade* dan versi baru dari sistem informasi Perangkat Daerah;
14. Pengujian penerimaan sistem harus dilakukan sesuai dengan kriteria dan jadwal yang ditetapkan.

15. Pengamanan terhadap data hasil pengujian perlu diperhatikan sebagai berikut:
    a. data untuk pengujian sistem harus dipilih secara hati-hati untuk menghindari pengungkapan atau perubahan informasi sensitif oleh pihak yang tidak berhak, serta melindung dari kemungkinan kerusakan dan kehilangan informasi;
    b. *masking* data harus dilakukan apabila data operasional yang sensitif digunakan untuk keperluan pengujian;
    c. data operasional yang digunakan untuk keperluan pengujian harus dihapus segera setelah proses pengujian telah selesai dilaksanakan.

BAB XII
HUBUNGAN KERJA DENGAN PIHAK LUAR (*SUPPLIER*)

A. Tujuan

Tujuan dari kebijakan mengenai hubungan kerja dengan pihak luar (*supplier*) adalah untuk memastikan perlindungan atas aset Perangkat Daerah dalam jangkauan akses pihak luar dan memelihara tingkat layanan yang dsetujui dari keamanan informasi sesuai dengan perjanjian dengan pihak luar.

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai hubungan kerja dengan pihak luar (*supplier*) adalah para pihak luar dalam lingkungan Pemerintah Provinsi Sumatera Barat

C. Kebijakan

1. Perangkat Daerah harus mempertimbangkan aspek keamanan data dan informasi dalam hubungan dengan pihak luar mulai dari pemilihan, penunjukan, monitoring, evaluasi, sampai dengan terminasi.
2. Pemilihan dari penyedia jasa Perangkat Daerah harus mengikuti kriteria berikut:
   a. kompetensi, pengalaman dan catatan dari organisasi;
   b. kepastian dari kemampuan penyedia jasa untuk menyediakan layanan;
   c. kepastian dari kemampuan penyedia jasa untuk menjaga ketersediaan dari penyediaan layanan pada saat kondisi normal atau kondisi bencana (apabila terjadi bencana alam atau kegagalan dalam penyediaan layanan);
3. Berdasarkan pengelompokan pihak luar yang telah bekerjasama, Perangkat Daerah wajib mendefinisikan pembatasan aset dan aset data dan informasi apa saja yang diperbolehkan untuk diakses oleh setiap kelompok pihak luar, serta senantiasa memantau akses yang telah dilakukan.
4. Perangkat Daerah menetapkan persyaratan Keamanan Informasi bagi setiap pihak luar yang mengakses aset informasi, serta senantiasa memantau kepatuhan pihak luar terhadap persyaratan tersebut. Pihak luar yang menangani aset informasi dengan klasifikasi rahasia perlu menandatangani Perjanjian Kerahasiaan.
5. Kewajiban pihak luar dan tingkat layanan harus ditetapkan secaraformal dalam kontrak kerja;
6. Perangkat Daerah harus memastikan pengelolaan *delivery* layanan dari pihak luar dengan memperhatikan:
   a. layanan yang diserahkan kepada Perangkat Daerah oleh pihak pihak luar harus secara berkala dipantau, dan ditinjau;
   b. proses pemantauan dilakukan untuk memverifikasi kesesuaian dari tingkat layanan yang diberian dan prasyarat keamanan data dan informasi dengan perjanjian kerja;
   c. proses peninjauan dilakukan untuk mengidentifikasi problem terkait penyediaan layanan dan aspek keamanan informasi dalam penyediaan layanan oleh pihak luar;
   d. peninjauan dari penyediaan layanan oleh supplier harus dilaksanakan paling sedikit satu kali dalam tiga bulan;
7. Perangkat Daerah dapat melakukan audit terhadap penyediaan layanan yang diberikan pihak luar.

8. Ketentuan dalam pelaksanaan audit kepada pihak luar sebagai berikut:
    a. tanggung jawab untuk mengaudit tingkat layanan dimiliki oleh pihak, baik internal maupun eksternal, yang memiliki independensi dari pengguna layanan yang diberikan oleh pihak luar dan ditunjuk secara formal;
    b. audit terhadap penyediaan layanan oleh pihak luar harus dilakukan paling sedikit satu kali dalam satu tahun;
    c. setiap ketidaksesuaian yang ditemukan dalam proses peninjauan dan audit harus dikelola dan ditindaklanjuti;
9. Perubahan terhadap layanan yang diberikan oleh pihak luar harus dikelola, dengan memperhatikan kritikalitas dari proses bisnis pengguna layanan dan layanan yang diberikan oleh supplier;
10. Perubahan terhadap layanan yang diberikan oleh pihak luar harus dipastikan tidak akan mengganggu aspek kerahasiaan dari informasi Perangkat Daerah serta integritas dan ketersediaan dari informasi dan layanan Perangkat Daerah;
11. Perubahan terhadap layanan yang diberikan oleh pihak luar harus disetujui oleh manajemen Perangkat Daerah yang relevan dan diformalisasikan dalam kontrak kerja.

BAB XIII

PENANGANAN INSIDEN KEAMANAN INFORMASI

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan penanganan insiden keamanan informasi adalah:

1. tanggung jawab dan prosedur;
2. pelaporan atas kejadian insiden keamanan informasi; dan
3. pelaporan atas kelemahan keamanan informasi.

C. Kebijakan

1. Kejadian keamanan informasi adalah sebuah kejadian pada sistem, layanan ataupun jaringan yang dapat mengindikasikan adanya pelanggaran keamanan informasi atau kegagalan keamanan atau kejadian yang mungkin memiliki keterkaitan dengan keamanan data dan informasi.
2. Kelemahan keamanan informasi adalah sebuah kelemahan yang teridentifikasi pada sistem, layanan atau jaringan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab dan dapat menyebabkan pelanggaran terhadap kebijakan keamanan informasi.
3. Insiden keamanan informasi adalah kejadian keamanan informasi yang tidak diinginkan dan tidak diperkirakan dimana kejadian tersebut menimbulkan gangguan terhadap operasional bisnis dan mengancam keamanan informasi.
4. Guna memastikan proses penanganan insiden yang responsif dan efektif, perlu dikembangkan berbagai prosedur yang mencakup:
   a. perencanaan dan persiapan penanganan insiden;
   b. pemantauan, analisis, dan pelaporan atas insiden;
   c. pencatatan atas aktivitas penanganan insiden;
   d. penanganan bukti forensik;
   e. penilaian dan pengambilan keputusan atas insiden dan kelemahan keamanan informasi; dan
   f. pemulihan insiden.

5. Seluruh pegawai di Lingkungan Pemerintah Daerah Provinsi Sumatera Barat dan pihak ketiga yang mengalami atau mengetahui gangguan insiden keamanan informasi maupun yang masih bersifat dugaan atas kelemahan keamanan informasi pada sistem elekronik Pemerintah Provinsi Sumatera Barat wajib sesegera mungkin melaporkan sesuai prosedur pelaporan insiden yang berlaku.
6. Setiap kejadian insiden keamanan informasi harus dianalisis, diklasifikasikan, dan ditentukan skala prioritas penanganannya. Penanganan insiden beserta pemulihannya dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.
7. Perangkat Daerah harus mengklasifikasikan insiden keamanan informasi untuk memprioritaskan penanganan insiden. Klasifikasi insiden tersebut adalah sebagai berikut:
   a. insiden keamanan informasi diklasifikasikan berdasarkan dampaknya menjadi berikut:
      1) mayor, apabila insiden tersebut menyebabkan terhentinya proses operasional pekerjaan Perangkat Daerah;
      2) minor, apabila insiden tersebut menyebabkan gangguan yang tidak menghentikan proses operasional pekerjaan Perangkat Daerah.
   b. insiden keamanan informasi diklasifikasikan berdasarkan tingkat kepentingannya menjadi berikut:
      1) *emergency*, apabila insiden tersebut dapat atau telah menghentikan proses operasional Perangkat Daerah dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah;
      2) normal, apabila insiden tersebut insiden tersebut tidak menghentikan proses operasional Perangkat Daerah dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah.
8. Setiap insiden keamanan informasi harus ditangani dengan baik untuk mencegah meluasnya insiden, untuk memulihkan layananatau informasi yang mungkin hilang dan untuk meminimalisasi dampak dari insiden.
9. Setiap tindakan yang diidentifikasi untuk menangani kejadian, kelemahan dan insiden keamanan informasi harus dikonsultasikan kepada koordinator SumbarProv-CSIRT dan/atau personil yang kompeten dan relevan dengan kejadian, kelemahan dan insiden keamanan informasi.
10. Setiap tindakan penanganan kejadian, kelemahan dan insiden Keamanan Informasi harus didokumentasikan dengan baik.

BAB XIV

KELANGSUNGAN USAHA (*BUSINESS CONTINUITY*)

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai kelangsungan usaha (*business continuity*) adalah:

1. keberlanjutan Keamanan Informasi;
2. redundansi fasilitas pengolahan informasi.

C. Kebijakan

1. Perangkat Daerah harus menetapkan, mendokumentasikan, mengimplementasikan dan memelihara proses, prosedur dan kontrol yang diperlukan untuk menjamin keberlanjutan keamanan data dan informasi sesuai prasyarat yang telah ditetapkan pada saat dan setelah terjadinya gangguan besar atau bencana.
2. Perangkat Daerah harus memverifikasi kontrol keberlanjutan keamanan data dan informasi yang telah ditetapkan dan diimplementasikan secara berkala untuk menjamin kesesuaian dan efektivitasnya pada saat dan setelah terjadinya gangguan besar atau bencana.
3. Perangkat Daerah harus menetapkan prasyarat untuk keberlanjutan keamanan informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis organisasi untuk menjamin keberlanjutan dari keamanan informasi di Perangkat Daerah, pada saat dan setelah terjadinya gangguan besar atau bencana.
4. Prasyarat keamanan informasi dapat diintegrasikan pada siklus proces *business continuity management* (BCM) yang mencakup:
   a. memahami kebutuhan organisasi;
   b. menentukan strategi BCM;
   c. mengembangkan dan mengimplementasikan rencana penanggulangan/keberlanjutan bisnis;
   d. pengujian, pemeliharaan dan peninjauan rencana penanggulangan/ keberlanjutan bisnis;

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

BAB XV

KEPATUHAN

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai kepatuhan:

1. kepatuhan dengan prasyarat hukum dan kontraktual;
2. peninjauan Keamanan Informasi

C. Kebijakan

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

5. Perangkat Daerah harus memastikan privasi dan perlindungan terhadap informasi terkait dengan pribadi (*personally identifiable information*) sesuai dengan prasyarat hukum, perundangan,regulasi dan kontraktual;
6. Pimpinan Perangkat Daerah harus secara rutin memantau dan meninjau kepatuhan dari personil, proses kerja dan pemrosesan informasi dalam area tanggung jawabnya terhadap kebijakan dan standard Keamanan Informasi Perangkat Daerah serta prasyarat Keamanan Informasi yang berlaku;
7. Pada saat terjadi ketidaksesuaian, pimpinan Perangkat Daerah bertanggung jawab untuk menangani ketidaksesuaian yang terjadi sesuai dengan kebijakan terkait penanganan ketidaksesuaian dan peningkatan Tata Kelola Keamanan Informasi dalam menunjang Sistem Manajemen Keamanan Informasi;
8. Sistem informasi Perangkat Daerah harus ditinjau untuk menganalisis kepatuhan teknis dengan kebijakan dan standard keamanan yang berlaku serta dengan prasyarat keamanan informasi yang relevan dan berlaku, paling tidak satu kali dalam satu tahun;
9. Apabila diperlukan, peninjauan tersebut dapat melibatkan personil yang memiliki kualifikasi di bidang keamanan informasi untuk mendapatkan pemahaman yang mendalam mengenai risiko keamanan informasi yang mungkin muncul dari pengecualian tersebut.

StempelParaf				
No	**Nama**	**Jab**	**Tgl**	**Paraf**
1.	Hansastri	**Sekretaris Daerah**		
2.	Andri Yulika	**Ass. Adm dan Umum**		
3.	Siti Aisyah	**Kepala Dinas**		
4.	Oni Fajar Syahdi	**Sekdin**		
5.	Eko Paisal	**Kabid Siber dan Sandi**		
6.	Roby charma	**Sandiman Muda**		

GUBERNUR SUMATERA BARAT,

MAHYELDI