GUBERNUR SUMATERA BARAT

PERATURAN DAERAH PROVINSI SUMATERA BARAT
NOMOR 10 TAHUN 2019

TENTANG

PENYELENGGARAAN PERSANDIAN
UNTUK PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR SUMATERA BARAT,

Menimbang :

a. bahwa data dan informasi merupakan aset yang sangat penting dalam sistem komunikasi global sehingga perlu diperhatikan keamanannya;

b. bahwa penerapan teknologi informasi dan komunikasi dalam mendukung pemerintahan melalui penyelenggaraan sistem pemerintahan berbasis elektronik pada Pemerintah Daerah Provinsi Sumatera Barat menimbulkan risiko semakin beragam dan kompleks yang dapat mengganggu, membahayakan, dan/atau menggagalkan pelaksanaan tugas pemerintahan daerah dan pelayanan publik sehingga perlu diselenggarakan persandian untuk pengamanan informasi yang dilaksanakan secara sistematis, terstruktur, dan komprehensif;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Daerah tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi;

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 61 Tahun 1958 tentang Penetapan Undang-Undang Darurat Nomor 19 Tahun 1957 tentang Pembentukan Daerah-Daerah Swatantra Tingkat I Sumatera Barat, Jambi dan Riau sebagai Undang-Undang (Lembaran Negara Republik Indonesia Tahun 1958 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 1646);
3. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

Dengan Persetujuan Bersama

DEWAN PERWAKILAN RAKYAT DAERAH
PROVINSI SUMATERA BARAT
dan
GUBERNUR SUMATERA BARAT

MEMUTUSKAN:

Menetapkan : PERATURAN DAERAH TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Daerah ini yang dimaksud dengan:

1. Daerah adalah Provinsi Sumatera Barat.
2. Gubernur adalah Gubernur Sumatera Barat.
3. Wakil Gubernur adalah Wakil Gubernur Sumatera Barat.
4. Pemerintah Daerah adalah Pemerintah Provinsi Sumatera Barat.
5. Perangkat Daerah adalah unsur pembantu Gubernur dan Dewan Perwakilan Rakyat Daerah Provinsi Sumatera Barat 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 di bidang 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 ataupun 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. Pejabat Pengelola Informasi dan Dokumentasi yang selanjutnya disingkat PPID adalah pejabat yang bertanggung jawab dalam pengumpulan, pendokumentasian, penyimpanan, pemeliharaan, penyediaan, distribusi, dan pelayanan informasi dan dokumentasi di lingkungan Pemerintah Daerah.
13. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat Tanda Tangan Elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam Transaksi Elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik.
14. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
15. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
16. 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 kemanan siber.
17. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan,mengirimkan, dan/atau menyebarkan informasi elektronik.
18. Jaring Komunikasi Sandi adalah keterhubungan antar pengguna persandian melalui jaringan telekomunikasi.

Pasal 2

Penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah berasaskan:

a. kemanfaatan;
b. kehati-hatian;
c. keterpercayaan;
d. keprofesionalan; dan

e. ketahanan.

Pasal 3

Peraturan Daerah ini dimaksudkan sebagai pedoman bagi Dinas dan Perangkat Daerah dalam menyelenggarakan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah.

Pasal 4

Peraturan Daerah ini bertujuan untuk :

a. meningkatkan efektivitas pelaksanaan kebijakan, program dan kegiatan Penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah;
b. menciptakan hubungan komunikasi yang baik dan aman pada seluruh Perangkat Daerah di lingkungan Pemerintah Daerah;
c. membantu Perangkat Daerah dalam Pengamanan Informasi yang bersifat rahasia milik Pemerintah Daerah; dan
d. meningkatkan kinerja Dinas dalam menangani urusan pemerintahan bidang persandian untuk Pengamanan Informasi.

Pasal 5

Ruang lingkup pengaturan dalam Peraturan Daerah ini meliputi:

a. kewenangan Pemerintah Daerah;
b. klasifikasi Informasi;
c. Penyelenggaraan Persandian untuk Pengamanan Informasi;
d. Pola hubungan komunikasi sandi antar Perangkat Daerah;
e. Kerjasama dan Koordinasi.

BAB II

KEWENANGAN PEMERINTAH DAERAH

Pasal 6

(1) Gubernur memimpin dan bertanggung jawab terhadap Penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah yang dibantu oleh Dinas.

(2) Dalam Penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah sebagaimana dimaksud pada ayat (1), Gubernur berwenang:
   a. menetapkan kebijakan Penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah;
   b. melaksanakan penguatan kapasitas kelembagaan, sumber daya manusia, infrastruktur, sarana dan prasarana, serta anggaran; dan
   c. mengkoordinasikan kegiatan bidang Persandian antar Perangkat Daerah;

Pasal 7

Dalam menetapkan kebijakan Penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf a, Pemerintah Daerah mengacu kepada norma, standar, prosedur, dan kriteria yang ditetapkan oleh BSSN dan peraturan perundang-undangan.

BAB III
KLASIFIKASI INFORMASI

Bagian Kesatu
Umum

Pasal 8

Pemerintah Daerah melaksanakan Pengamanan Informasi dan Informasi non elektronik.

Pasal 9

(1) Pengamanan Informasi dan Informasi non elektronik sebagaimana dimaksud dalam Pasal 8 dilakukan terhadap Informasi publik dan Informasi yang dikecualikan.
(2) Informasi publik sebagaimana dimaksud pada ayat (1) merupakan informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh Pemerintah Daerah yang berkaitan dengan

Penyelenggaraan Pemerintahan Daerah serta informasi lain yang berkaitan dengan kepentingan publik sesuai dengan ketentuan peraturan perundang-undangan.

(3) Informasi yang dikecualikan sebagaimana dimaksud pada ayat (1) merupakan informasi publik yang apabila dibuka dan diberikan kepada pemohon informasi publik dapat:
   a. menghambat proses penegakan hukum;
   b. mengganggu kepentingan perlindungan hak atas kekayaan intelektual;
   c. membahayakan pertahanan dan keamanan Negara;
   d. mengungkapkan kekayaan alam Indonesia;
   e. merugikan ketahanan ekonomi nasional;
   f. merugikan kepentingan hubungan luar negeri;
   g. mengungkapkan isi akta otentik yang bersifat pribadi dan kemauan terakhir ataupun wasiat seseorang;
   h. mengungkap rahasia pribadi;
   i. membocorkan memorandum atau surat-surat antar Badan Publik atau intra Badan Publik, yang menurut sifatnya dirahasiakan kecuali atas putusan Komisi Informasi atau pengadilan; dan
   j. mengungkapkan informasi yang tidak boleh diungkapkan berdasarkan Undang-Undang.

Bagian Kedua
Pengklasifikasian Informasi

Pasal 10

(1) Pengklasifikasian Informasi ditetapkan oleh PPID berdasarkan pengujian konsekuensi secara saksama dan penuh ketelitian sebelum menyatakan Informasi publik tertentu dikecualikan untuk diakses oleh setiap orang.

(2) Dalam melakukan pengujian konsekuensi sebagaimana dimaksud pada ayat (1), PPID wajib:
   a. menyebutkan secara jelas, dan terang informasi tertentu yang akan dilakukan Pengujian Konsekuensi;
   b. mencantumkan peraturan perundang-undangan yang dijadikan dasar pengecualian;

c. mencantumkan konsekuensi; dan
d. mencantumkan jangka waktu.

(3) Penetapan pengklasifikasian Informasi sebagaimana dimaksud pada ayat (1) dilakukan atas persetujuan Gubernur.

Pasal 11

Jangka waktu pengecualian terhadap Informasi yang dikecualikan sebagaimana dimaksud dalam Pasal 10 ayat (1) sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 12

(1) PPID menetapkan Informasi yang dikecualikan yang telah habis Jangka waktu pengecualiannya menjadi Informasi publik paling lama 30 (tiga puluh) hari kerja sebelum berakhirnya jangka waktu pengecualian
(2) Dalam hal PPID tidak melakukan penetapan sebagaimana dimaksud pada ayat (1) maka Informasi yang dikecualikan menjadi Informasi publik pada saat berakhirnya jangka waktu pengecualian.
(3) Informasi yang dikecualikan yang dinyatakan terbuka berdasarkan putusan Komisi Informasi dan pengadilan yang berkekuatan hukum tetap wajib disediakan dan dapat diakses oleh setiap orang.
(4) Informasi yang dikecualikan yang dinyatakan terbuka sebagaimana dimaksud pada ayat (3) dimasukkan ke dalam daftar Informasi publik.

BAB IV
PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 13

(1) Pemerintah Daerah menyusun perencanaan Penyelenggaraan Persandian untuk Pengamanan Informasi.

(2) Perencanaan Penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam perencanaan pembangunan Daerah.

(3) Perencanaan pembangunan Daerah sebagaimana dimaksud pada ayat (2) merupakan bagian integral dari sistem perencanaan pembangunan nasional dan dituangkan dalam dokumen perencanaan pembangunan Daerah.

(4) Dokumen perencanaan pembangunan Daerah sebagaimana dimaksud pada ayat (3) berupa rencana pembangunan jangka panjang Daerah, rencana pembangunan jangka menengah Daerah, dan rencana kerja Pemerintah Daerah.

(5) Penyelenggaraan Persandian untuk Pengamanan Informasi pemerintah daerah dilaksanakan melalui :

a. Penyusunan Rencana Pengamanan Informasi Pemerintah Daerah;
b. Pengelolaan Sumber Daya Keamanan Informasi
c. Penyediaan Layanan Keamanan Informasi; dan
d. Pengamanan Sistem Elektronik dan pengamanan informasi non elektronik;

Bagian Kedua

Penyusunan Rencana Pengamanan Informasi Pemerintah Daerah

Pasal 14

(1) Penyusunan Rencana Pengamanan Informasi sebagaimana dimaksud dalam pasal 13 ayat (5) huruf a dilakukan dengan :

a. menyusun rencana strategis Pengamanan Informasi;
b. menetapkan arsitektur Keamanan Informasi; dan
c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

(2) Pemerintah Daerah melalui Dinas menyusun rencana strategis Pengamanan Informasi;

(3) Rencana strategis sebagaimana dimaksud pada ayat (2) huruf a terdiri atas :

a. tujuan, sasaran, program, kegiatan, dan target pelaksanaan Pengamanan Informasi setiap tahun untuk jangka waktu 5 (lima) tahun.

b. peta rencana penyelenggaraan Pengamanan Informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun untuk jangka waktu 5 (lima) tahun.

(4) Rencana strategis Pengamanan Informasi yang telah disusun sebagaimana dimaksud pada ayat (2) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah.

(5) Arsitektur Keamanan Informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) huruf b berlaku untuk jangka waktu 5 (lima) tahun.

(6) Tata cara Penyusunan Rencana Pengamanan Informasi sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Gubernur.

Bagian ketiga

Pengelolaan Sumber Daya Keamanan Informasi

Paragraf 1

Umum

Pasal 15

(1) Pemerintah Daerah melaksanakan pengelolaan sumber daya Keamanan Informasi.

(2) Sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) meliputi:

a. sarana dan prasarana keamanan teknologi informasi dan komunikasi; dan

b. sumber daya manusia.

(3) Pemerintah Daerah melaksanakan analisis kebutuhan dalam rangka pengelolaan sumber daya Keamanan Informasi.

(4) Hasil analisis kebutuhan sebagaimana dimaksud pada ayat (3) digunakan untuk mewujudkan Keamanan Informasi Pemerintah Daerah.

Paragraf 2

Sarana dan Prasarana Keamanan

Teknologi Informasi dan Komunikasi

Pasal 16

(1) Pemerintah Daerah mengelola sarana dan prasarana keamanan teknologi informasi dan komunikasi dengan tujuan untuk menjamin ketersediaan dan optimalisasi pemanfaatannya sesuai dengan ketentuan peraturan perundang-undangan.
(2) Pengelolaan sarana dan prasarana keamanan teknologi Informasi dan komunikasi dilakukan melalui serangkaian proses perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi.

Pasal 17

Sarana dan prasarana keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 16 terdiri atas:

a. sarana dan prasarana keamanan teknologi informasi dan komunikasi khusus; dan
b. sarana dan prasarana keamanan teknologi informasi dan komunikasi umum.

Pasal 18

(1) Sarana dan prasarana keamanan teknologi informasi dan komunikasi khusus sebagaimana dimaksud dalam Pasal 17 huruf a meliputi:
    a. *jamming*;
    b. kontra penginderaan; dan
    c. pusat operasi Pengamanan Informasi (*security operation centre)*.
(2) Sarana dan prasarana keamanan teknologi informasi dan komunikasi umum sebagaimana dimaksud dalam Pasal 17 huruf b meliputi:
    a. materiil sandi;
    b. Jaring Komunikasi Sandi; dan
    c. tempat kegiatan sandi.

(3) Pengadaan atau penyedian sarana dan prasarana keamanan teknologi informasi dan komunikasi khusus sebagaimana dimaksud pada ayat (1) oleh Pemerintah Daerah dilakukan melalui:
   a. permohonan fasilitasi kepada BSSN; dan/atau
   b. pengadaan secara mandiri oleh Pemerintah Daerah.

(4) Pengadaan secara mandiri oleh Pemerintah Daerah sebagaimana dimaksud pada ayat (3) huruf b dilakukan terhadap sarana dan prasarana keamanan teknologi informasi dan komunikasi khusus yang telah tersertifikasi keamanannya oleh BSSN dan dilakukan berdasarkan rekomendasi dari BSSN sesuai dengan ketentuan peraturan perundang-undangan.

(5) Ketentuan lebih lanjut mengenai tata cara permohonan Fasilitasi penyedian sarana dan prasarana keamanan teknologi informasi dan komunikasi khusus kepada BSSN sebagaimana dimaksud pada ayat (3) huruf a diatur dengan Peraturan Gubernur.

Pasal 19

(1) Sarana dan prasarana keamanan teknologi informasi dan komunikasi umum sebagaimana dimaksud dalam Pasal 17 huruf b berupa perangkat keras dan/atau perangkat lunak serta fasilitas lainnya yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisa, menanggulangi, dan/atau memulihkan insiden Keamanan Informasi dalam pengelolaan Sistem Elektronik Pemerintah Daerah.

(2) Pengadaan atau penyedian sarana dan prasarana keamanan teknologi informasi dan komunikasi umum sebagaimana dimaksud pada ayat (1) dilakukan oleh Pemerintah Daerah dan dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Paragraf 3

Sumber Daya Manusia

Pasal 20

(1) Dinas mengelola sumber daya manusia untuk menjamin keberlangsungan dan peningkatan mutu Layanan Keamanan Informasi.

(2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) mencakup aparatur sipil negara pengelola Keamanan Informasi pada Perangkat Daerah.

(3) Ketentuan lebih lanjut mengenai penggelolaan Sumber daya manusia sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Gubernur.

Bagian Keempat

Pengamanan Informasi Elektronik

dan Pengamanan Informasi Non Elektronik

Paragraf 1

Pengamanan Informasi Sistem Elektronik

Pasal 21

(1) Pemerintah Daerah menerapkan Pengamanan Informasi dalam pengelolaan Sistem Elektronik sesuai dengan ketentuan peraturan perundang-undangan.

(2) Pengamanan Informasi dalam pengelolaan sebagaimana dimaksud pada ayat (1) mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirsangkal terkait:
   a. data dan Informasi;
   b. Infrastruktur; dan
   c. aplikasi.

(3) Data dan Informasi sebagaimana dimaksud pada ayat (2) huruf a merupakan Informasi publik.

(4) Infrastruktur sebagaimana dimaksud pada ayat (2) huruf b terdiri atas:
   a. pusat data;
   b. jaringan intra; dan
   c. sistem penghubung layanan Sistem Elektronik.

(5) Pusat Data sebagaimana dimaksud pada ayat (4) huruf a merupakan fasilitas yang digunakan untuk menempatkan sistem elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.

(6) Jaringan Intra sebagaimana dimaksud pada ayat (4) huruf b merupakan jaringan tertutup yang menghubungkan antar simpul jaringan pada Pemerintah Daerah.

(7) Sistem penghubung layanan sistem elektronik sebagaimana dimaksud pada ayat (4) huruf c merupakan perangkat integrasi/penghubung untuk melakukan pertukaran layanan Sistem Elektronik.

Pasal 22

(1) Dalam melaksanakan Pengamanan Informasi Sistem Elektronik sebagaimana dimaksud dalam Pasal 21, Dinas melakukan:
   a. deteksi;
   b. identifikasi;
   c. proteksi;
   d. penanggulangan dan pemulihan.

(2) Deteksi sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui kegiatan analisis untuk menentukan adanya ancaman atau kejadian insiden pada Sistem Elektronik.

(3) Identifikasi sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui kegiatan analisis kerawanan dan risiko terhadap Sistem Elektronik.

(4) Proteksi sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan kegiatan mitigasi risiko dan penerapan perlindungan terhadap Sistem Elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintahan berbasis elektronik.

(5) Penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (1) huruf d dilakukan dengan kegiatan penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Pasal 23

(1) Dalam melaksanakan Pengamanan Informasi Sistem Elektronik sebagaimana dimaksud dalam Pasal 21, Pemerintah Daerah wajib menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik

(2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh penyelenggara Sertifikat Elektronik BSSN dan/atau lembaga penyelenggara Sertifikasi Elektronik Indonesia dalam negeri yang telah diakui.

(3) Dinas dapat menjadi otoritas pendaftaran penggunaan Sertifikat Elektronik dari penyelenggara Sertifikat Elektronik BSSN sesuai dengan ketentuan peraturan perundang-undangan.

(4) Penggunaan Sertifikat Elektronik dalam penyelenggaraan Sistem Elektronik sebagaimana dimaksud ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 24

(1) Dalam mendukung layanan Sistem Elektronik, Pemerintah Daerah dapat menyelenggarakan pusat operasi Pengamanan Informasi *(security operation centre*) sesuai standar yang ditetapkan oleh BSSN.

(2) Penyelenggaraan pusat operasi Pengamanan Informasi (*security operation centre*) bertujuan untuk mendukung fungsi deteksi, identifikasi, proteksi, penanggulangan, serta pemulihan insiden Keamanan Informasi.

Pasal 25

Penyelenggaraan pusat operasi Pengamanan Informasi (*security operation centre*) sebagaimana dimaksud dalam Pasal 24 harus memenuhi standar teknis dan prosedur sesuai dengan ketentuan peraturan perundang-undangan.

Paragraf 2

Pengamanan Informasi Non Elektronik

Pasal 26

(1) Pengamanan Informasi non elektronik dilakukan mulai dari tahap pembuatan, pengiriman/pendistribusian, penyimpanan, dan pemusnahan.

(2) Pengamanan Informasi non elektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Paragraf 3

Manajemen Pengamanan Informasi Sistem Elektronik

Pasal 27

(1) Pemerintah Daerah menerapkan manajemen Pengamanan Informasi Sistem elektronik.
(2) Dinas mengkoordinasikan pelaksanaan manajemen Pengamanan Informasi Sistem Elektronik termasuk manajemen risiko dalam pengelolaan Sistem Elektronik pada setiap Perangkat Daerah.
(3) Manajemen Pengamanan Informasi Sistem Elektronik sebagaimana dimaksud pada ayat (1) bertujuan untuk menjamin keberlangsungan pengelolaan Sistem Elektronik dengan meminimalkan dampak risiko Keamanan Informasi sesuai dengan ketentuan peraturan perundang-undangan.
(4) Manajemen Pengamanan Informasi dilakukan melalui serangkaian proses yang meliputi:
    a. penetapan ruang lingkup;
    b. penetapan penanggung jawab;
    c. perencanaan, dukungan pengoperasian;
    d. evaluasi kinerja; dan
    e. perbaikan berkelanjutan terhadap Keamanan Informasi dalam pengelolaan Sistem Elektronik.

Paragraf 4

Tim Pengelola Keamanan Informasi

Pasal 28

(1) Untuk pelaksanaan tata kelola Keamanan Informasi, dibentuk tim pengelola Keamanan Informasi yang ditetapkan dengan Keputusan Gubernur.
(2) Tim pengelola Keamanan Informasi memiliki fungsi 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.

(3) Ketentuan lebih lanjut mengenai Tim Pengelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Gubernur.

Bagian Kelima
Penyediaan Layanan Keamanan Infromasi

Pasal 29

(1) Dinas memberikan Layanan Keamanan Informasi kepada Pengguna Layanan.
(2) Pengguna Layanan sebagaimana dimaksud pada ayat (1) sebagai berikut:
a. Gubernur dan Wakil Gubernur;
b. Perangkat Daerah;
c. aparatur sipil negara yang bertugas di Pemerintah Daerah; dan
d. pihak lainnya.

Pasal 30

(1) Kegiatan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 29 ayat (1) meliputi:
a. identifikasi kerentanan dan penilaian risiko Keamanan Informasi terhadap Sistem Elektronik;
b. asistensi dan fasilitasi penguatan keamanan Sistem Elektronik;
c. penerapan Sertifikat Elektronik untuk melindungi Sistem Elektronik dan dokumen elektronik;

d. perlindungan Informasi berklasifikasi melalui penyediaan perangkat teknologi Keamanan Informasi dan Jaring Komunikasi Sandi;
e. fasilitasi sertifikasi penerapan manajemen pengamanan Sistem Elektronik;
f. audit Keamanan Informasi;
g. literasi Keamanan Informasi dalam rangka peningkatan kesadaran Keamanan Informasi dan pengukuran tingkat kesadaran Keamanan Informasi;
h. peningkatan kompetensi sumber daya manusia di bidang Keamanan Informasi;
i. pengelolaan pusat operasi Pengamanan Informasi (*Security Operation Center*);
j. penanganan insiden Keamanan Informasi;
k. forensik digital;
l. perlindungan Informasi pada kegiatan penting Pemerintah Daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
m. perlindungan Informasi pada aset/fasilitas penting milik atau yang akan digunakan Pemerintah Daerah melalui kontra penginderaan; dan/atau
n. konsultasi Keamanan Informasi bagi Pengguna Layanan.

(2) Literasi Keamanan Informasi dalam rangka peningkatan kesadaran Keamanan Informasi sebagaimana dimaksud pada ayat (1) huruf g dilakukan terhadap pengguna Layanan Keamanan Informasi dan kepada publik.

Pasal 31

(1) Dinas memberikan layanan Keamanan Informasi dengan terus meningkatkan kapasitas dan kualitas Layanan Keamanan Informasi kepada Pengguna Layanan.
(2) Dalam memberikan Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1), Dinas dapat membuat inovasi sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 32

(1) Dalam memberikan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 31, Dinas harus menerapkan manajemen Layanan Keamanan Informasi.
(2) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan Keamanan Informasi kepada Pengguna Layanan.
(3) Manajemen Layanan Keamanan Informasi dilakukan melalui serangkaian proses pelayanan kepada Pengguna Layanan dan pengoperasian Layanan Keamanan Informasi.
(4) Pelayanan kepada Pengguna Layanan sebagaimana dimaksud pada ayat (3) merupakan kegiatan pelayanan terhadap keluhan, gangguan, masalah, permintaan, dan/atau perubahan Layanan Keamanan Informasi dari Pengguna Layanan.
(5) Pengoperasian Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (3) merupakan kegiatan pendayagunaan dan pemeliharaan berbagai jenis Layanan Keamanan Informasi.
(6) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen Layanan Keamanan Informasi sesuai dengan ketentuan peraturan perundang-undangan.

BAB V

POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Bagian Kesatu

Pola Hubungan Komunikasi Sandi

Pasal 33

Pola hubungan komunikasi sandi antar Perangkat Daerah dilakukan melalui serangkaian kegiatan untuk mengidentifikasi dan menganalisis bentuk/model keterhubungan antar Pengguna Layanan beserta aspek lainnya yang dibutuhkan dalam suatu Jaring Komunikasi Sandi yang dilaksanakan oleh Dinas.

Pasal 34

Pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 33 dilakukan melalui tahapan:

a. identifikasi;
b. analisis; dan
c. penetapan hasil.

Pasal 35

Identifikasi sebagaimana dimaksud dalam Pasal 34 huruf a, meliputi:

a. identifikasi pola hubungan komunikasi Gubernur, Wakil Gubernur, dan pejabat tinggi di lingkungan Pemerintah Daerah yang sedang dilaksanakan;
b. identifikasi alur Informasi yang dikomunikasikan antar Perangkat Daerah;
c. identifikasi dan/atau penyediaan sarana dan prasarana teknologi Informasi dan komunikasi yang digunakan oleh Gubernur, Wakil Gubernur, dan pejabat tinggi di lingkungan Pemerintah Daerah;
d. infrastruktur komunikasi yang ada di wilayah Pemerintah Daerah; dan
e. kompetensi personil yang dibutuhkan.

Pasal 36

(1) Analisis sebagaimana dimaksud dalam Pasal 34 huruf b dilakukan berdasarkan hasil identifikasi pola hubungan komunikasi, meliputi:
    a. identifikasi pengelola layanan penyelenggaraan persandian;
    b. identifikasi sarana dan prasarana; dan
    c. identifikasi pembiayaan.
(2) Identifikasi pengelola layanan penyelenggaraan persandian sebagaimana dimaksud pada ayat (1) huruf a yaitu kegiatan untuk mengidentifikasi personil dan kompetensi yang dibutuhkan dalam Penyelenggaraan Persandian.
(3) Identifikasi sarana dan prasarana sebagaimana dimaksud pada ayat (1) huruf b meliputi identifikasi sarana dan prasarana yang dibutuhkan untuk Penyelenggaraan Persandian.

(4) Identifikasi pembiayaan sebagaimana dimaksud pada ayat (1) huruf c meliputi identifikasi anggaran yang dibutuhkan untuk Penyelenggaraan Persandian.

Pasal 37

Penetapan Hasil identifikasi dan analisis pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 35 dan Pasal 36 dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kedua
Jaring Komunikasi Sandi

Pasal 38

(1) Penyelenggaraan Jaring Komunikasi Sandi Pemerintah Daerah dilakukan untuk menjamin keamanan data, dokumen, daftar Informasi Publik dan daftar informasi yang dikecualikan.
(2) Penyelenggaraan Jaring Komunikasi Sandi sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian kegiatan untuk merencanakan, mengembangkan, mengoperasikan, menggunakan, dan mengendalikan Jaring Komunikasi Sandi Pemerintah Daerah.
(3) Jaring Komunikasi Sandi sebagaimana dimaksud pada ayat (1) menghubungkan antar simpul jaringan dalam internal Pemerintah Daerah, antar Pemerintah Daerah, dan Pemerintah Daerah dengan instansi pusat.
(4) Jaring Komunikasi Sandi sebagaimana dimaksud pada ayat (1) merupakan salah satu layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 30 ayat (1) huruf d.
(5) Jaring Komunikasi Sandi sebagaimana dimaksud pada ayat (2) terdiri atas:
    a. Jaring Komunikasi Sandi internal;
    b. Jaring Komunikasi Sandi eksternal; dan
    c. Jaring Komunikasi Sandi khusus.

Pasal 39

(1) Jaring Komunikasi Sandi internal sebagaimana dimaksud dalam Pasal 38 ayat (5) huruf a, terdiri atas:
   a. Jaring Komunikasi Sandi antar Perangkat Daerah
   b. Jaring Komunikasi Sandi internal Perangkat Daerah; dan
   c. Jaring Komunikasi Sandi pimpinan Daerah.
(2) Jaring Komunikasi Sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (1) huruf a menghubungkan seluruh Perangkat Daerah.
(3) Jaring Komunikasi Sandi internal Perangkat Daerah sebagaimana dimaksud pada ayat (1) huruf b menghubungkan antar Pengguna Layanan di lingkup internal Perangkat Daerah.
(4) Jaring Komunikasi Sandi pimpinan daerah sebagaimana dimaksud pada ayat (1) huruf c menghubungkan antar Gubernur dan Wakil Gubernur, serta kepala Perangkat Daerah.

Pasal 40

(1) Jaring Komunikasi Sandi eksternal sebagaimana dimaksud dalam Pasal 38 ayat (5) huruf b, terdiri atas:
   a. Jaring Komunikasi Sandi antar Pemerintah Daerah; dan
   b. Jaring Komunikasi Sandi Pemerintah Daerah dan Pemerintah Pusat.
(2) Jaring Komunikasi Sandi khusus sebagaimana dimaksud dalam Pasal 38 ayat (5) huruf c dibangun dan dioperasikan dengan ketentuan:
   a. tidak berfungsinya atau terganggunya operasional jaring komunikasi internal dan eksternal Pemerintah Daerah akibat bencana, kerusakan infrastruktur, dan/atau keamanan yang tidak kondusif; dan
   b. adanya kegiatan tertentu atau khusus Pemerintah Daerah yang membutuhkan jaring komunikasi sandi yang bersifat sementara.
(3) Penyelenggaraan Jaring Komunikasi Sandi eksternal sebagaimana dimaksud pada ayat (1) dan Jaring Komunikasi Sandi khusus

sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI
KERJASAMA DAN KOORDINASI

Pasal 41

Dalam Penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah Gubernur melaksanakan kerjasama sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 42

(1) Untuk mendukung pelaksanaan tugas dan fungsi dalam Penyelenggaraan Persandian di lingkungan Pemerintah Daerah, Dinas dapat berkoordinasi dengan:
   a. BSSN;
   b. kementerian yang menyelenggarakan urusan pemerintahan dibidang komunikasi dan informatika;
   c. instansi vertikal terkait yang berada di Daerah; dan/atau
   d. akademisi.

(2) Ketentuan lebih lanjut mengenai Koordinasi sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Gubernur.

BAB VII
FORUM KOMUNIKASI SANDI

Pasal 43

(1) Untuk mendukung pelaksanaan tugas dan fungsi dalam Penyelenggaraan Persandian di lingkungan Pemerintah Daerah, di bentuk Forum Komunikasi Sandi Daerah.

(2) Forum komunikasi Sandi sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Gubernur.

(3) Ketentuan lebih lanjut mengenai susunan dan tata kerja Forum Komunikasi Sandi Daerah sebagaimana dimaksud pada ayat (1) diatur dengan Peraturan Gubernur.

BAB VIII

PEMBINAAN DAN PENGAWASAN

Pasal 44

(1) Gubernur melakukan pembinaan dan pengawasan penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah dan pemerintah daerah kabupaten/kota.
(2) Ketentuan lebih lanjut mengenai pembinaan dan pengawasan penyelenggaraan Persandian sebagaimana yang dimaksud pada ayat (1) diatur dalam Peraturan Gubernur.

BAB IX

PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 45

(1) Gubernur melakukan pemantauan dan evaluasi penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah dan pemerintah daerah kabupaten/kota.
(2) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 46

Gubernur menyampaikan laporan hasil evaluasi penyelenggaraan Persandian untuk pengamanan informasi di lingkungan Pemerintah Daerah dan pemerintah daerah kabupaten/kota kepada menteri yang menyelenggarakan urusan pemerintahan dalam negeri dan BSSN.

BAB X

PEMBIAYAAN

Pasal 47

Pemerintah Daerah wajib menyediakan anggaran untuk Penyelenggaraan Persandian untuk Pengamanan Informasi yang bersumber dari:

a. Anggaran Pendapatan dan Belanja Daerah; dan/atau

b. sumber dana lain yang sah sesuai dengan ketentuan peraturan perundang-undangan.

BAB X

KETENTUAN PENUTUP

Pasal 48

Peraturan pelaksanaan dari Peraturan Daerah ini harus ditetapkan paling lama 1 (satu) tahun terhitung sejak Peraturan Daerah ini diundangkan.

Pasal 49

Peraturan Daerah ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Daerah ini dengan penempatannya dalam Lembaran Daerah Provinsi Sumatera Barat.

Ditetapkan di Padang
pada tanggal 25 November 2019
GUBERNUR SUMATERA BARAT,

Ttd

IRWAN PRAYITNO

Diundangkan di Padang
pada tanggal 25 November 2019
SEKRETARIS DAERAH
PROVINSI SUMATERA BARAT,

Ttd

ALWIS

LEMBARAN DAERAH PROVINSI SUMATERA BARAT TAHUN 2019 NOMOR 10
NOREG PERATURAN DAERAH PROVINSI SUMATERA BARAT TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI: (10-377/2019)

PENJELASAN

ATAS

PERATURAN DAERAH PROVINSI SUMATERA BARAT
NOMOR 10 TAHUN 2019

TENTANG

PENYELENGGARAAN PERSANDIAN
UNTUK PENGAMANAN INFORMASI

I. UMUM

Persandian adalah segala kegiatan yang berkaitan dengan pengamanan informasi milik Pemerintah dan Pemerintah Daerah yang dilaksanakan dengan menerapkan metode dan teknik aplikasi persandian. Pengamanan sandi lebih pada pengamanan logika berbasis informasi teknologi, karena banyak berhubungan dengan multimedia. Hal ini menunjukkan persandian bersifat trans-disiplin, karena menggunakan beragam ilmu sebagai pendukung pengembangan sistem sandi. Pembangunan bidang persandian merupakan salah satu penopang terwujudnya stabilitas pertahanan dan keamanan nasional, karena itu pemerintah pusat maupun daerah wajib mengelola informasi publik yang dimilikinya. Untuk melindungi informasi publik tersebut, perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian untuk melindungi informasi tersebut dari ancaman yang akan menimbulkan kerugian.

Persandian merupakan salah satu urusan wajib yang tidak berkaitan dengan pelayanan dasar. Untuk menjabarkan kewenangan daerah terkait urusan persandian maka dilakukanlah pemetaan urusan persandian dalam rangka penataan kelembagaan perangkat daerah Provinsi bidang persandian sesuai dengan amanat Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah. Dalam Undang-Undang Nomor 23 Tahun 2014 menegaskan bahwa fungsi persandian bukan hanya sebatas kirim terima surat/berita sandi, akan tetapi diperluas menjadi pengamanan informasi secara keseluruhan, melalui pembangunan sistem keamanan informasi Pemerintah Daerah dan

penyediaan sumber daya manusia persandian yang mumpuni. Fungsi persandian untuk pengamanan informasi merupakan tantangan berat karena sumber daya manusia persandian yang ada saat ini belum mempunyai kompetensi yang mencukupi untuk melakukan pengamanan informasi berbasis informasi teknologi. Dengan demikian Pemerintah Daerah memiliki tanggung jawab untuk melaksanakan pengamanan informasi atau sistem elektronik Pemerintah Daerah dan menyiapkan sumber daya manusia yang handal.

Perkembangan teknologi komunikasi dan informasi harus diimbangi dengan kesiapan infrastruktur strategis untuk meminimalisir dampak negatif, antara lain dengan menyediakan regulasi yang mengakomodir ketentuan mengenai pengamanan informasi, kesiapan lembaga, dan kesiapan sumber daya manusia khususnya dibidang persandian untuk pengamanan informasi, sehingga teknologi informasi dapat mendukung peningkatan produktifitas dan kinerja pemerintah daerah.

Semakin canggih teknologi informasi dan komunikasi yang dimanfaatkan tentunya akan membantu dalam meningkatkan efektifitas dan efisiensi penyelesaian tugas. Namun perlu dicermati juga potensi kerawanan dan pemanfaatan kecanggihan teknologi tersebut yang apabila tidak diwaspadai akan mengakibatkan kebocoran informasi dan sistem komunikasi yang diselenggarakan oleh pemerintah daerah kepada publik.

Kebocoran data yang selama ini kerap terjadi dipicu oleh beberapa hal yakni, bersifat teknis seperti hacker, cracker, teroris, spy (mata-mata) dan non teknis seperti penyalahgunaan akun pribadi, gangguan infrastruktur (akibat bencana alam dan lainnya), ketidaktahuan pengguna teknologi, kebocoran individu dan ketidakpedulian terhadap keamanan informasi merupakan sejumlah kerawanan yang kerap digunakan oleh pihak-pihak lain yang tidak bertanggung jawab.

Menjaga kerahasiaan informasi menjadi kewajiban pemerintah daerah, mengingat perkembangan teknologi informasi dan komunikasi tumbuh semakin cepat, yang berdampak pada meningkatnya

ancaman terhadap keamanan informasi, baik kualitas maupun kuantitas.

Secara umum Peraturan Daerah ini memuat materi-materi pokok yang disusun secara sistematis sebagai berikut : ketentuan umum yang memuat pengertian, asas, maksud dan tujuan pengaturan mengenai kewenangan Pemerintah Daerah, klasifikasi Informasi, Penyelenggaraan Persandian untuk Pengamanan Informasi, Pola hubungan komunikasi sandi antar Perangkat Daerah, penyelenggaraan persandian, penyelenggaraan persandian untuk keamanan informasi, sumber daya keamanan informasi, pola hubungan komunikasi sandi antar perangkat daerah, pembinaan dan pengawasan, pemantauan, evaluasi dan pelaporan, pembiayaan dan ketentuan penutup.

II. PASAL DEMI PASAL

Pasal 1

Cukup Jelas.

Pasal 2

Huruf a

Yang dimaksud dengan “asas kemanfaatan” adalah bahwa persandian ditujukan untuk dapat memberikan manfaat bagi setiap orang untuk melindungi haknya pribadi maupun untuk kepentingan masyarakat, bangsa, dan negara, serta kesejahteraan

Huruf b

Yang dimaksud dengan “asas kehati-hatian” adalah bahwa kegiatan persandian merupakan kegiatan pengamanan yang mempunyai risiko yang tinggi dan dampak yang strategis, sehingga harus dilaksanakan secara seksama, dengan didukung pengetahuan yang khusus, didasari prosedur yang ketat, serta sistem yang reliabel.

Huruf c

Yang dimaksud dengan “asas keterpercayaan” adalah bahwa kegiatan persandian harus diselenggarakan demi menjaga kepercayaan pengguna atau publik, sehingga harus

diselenggarakan dengan jaminan akuntabilitas terhadap sistem, sehingga kepercayaan pengguna (consumer confidence) didasarkan atas pengetahuan yang cukup atas adanya suatu risiko dimana pengguna mengetahui bahwa risiko tersebut telah dikelola dengan baik oleh penyelenggara dan didukung oleh keberadaan sistem yang terakreditasi atau tersertifikasi

Huruf d

Yang dimaksud dengan “asas keprofesionalan” adalah bahwa kegiatan persandian harus dilakukan oleh sumber daya manusia yang mempunyai latar belakang pengetahuan yang khusus dan/atau berpengalaman dalam bidang persandian.

Huruf e

Yang dimaksud dengan “asas ketahanan” adalah bahwa kegiatan persandian digunakan untuk melindungi informasi dan komunikasi, serta menjaga keberlangsungan teknis sehingga dapat memulihkan kembali kondisi keamanan sesegera mungkin sekiranya celah keamanan telah dapat diterobos oleh pihak yang tidak bertanggung jawab.

Pasal 3

Cukup Jelas.

Pasal 4

Cukup Jelas.

Pasal 5

Cukup Jelas

Pasal 6

Cukup Jelas.

Pasal 7

Cukup Jelas.

Pasal 8

Cukup Jelas.

Pasal 9

Ayat (1)

Cukup Jelas

Ayat (2)

Cukup Jelas

Ayat (3)

Huruf a

Cukup Jelas

Huruf b

Cukup Jelas

Huruf c

Cukup Jelas

Huruf d

Cukup Jelas

Huruf e

Cukup Jelas

Huruf f

Cukup Jelas

Huruf g

Cukup Jelas

Huruf h

Cukup Jelas

Huruf i

Yang dimaksud dengan “Badan Publik” adalah Lembaga eksekutif, legislatif, yudikatif, dan badan lain yang fungsi dan tugas pokoknya berkaitan dengan penyelenggaraan negara, yang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah atau organisasi non pemerintah sepanjang sebagian atau seluruh dananya bersumber dari Anggaran Pendapatan dan Belanja Negara dan/atau Anggaran Pendapatan dan Belanja Daerah, sumbangan masyarakat, dan/atau luar negeri.

Huruf j

Cukup Jelas

Pasal 10

Cukup Jelas.

Pasal 11

Cukup Jelas.

Pasal 12

Cukup Jelas.

Pasal 13

Cukup Jelas.

Pasal 14

Cukup Jelas.

Pasal 15

Cukup Jelas.

Pasal 16

Cukup Jelas.

Pasal 17

Cukup Jelas.

Pasal 18

Ayat (1)

Huruf a

Yang dimaksud dengan "*jamming';* adalah kegiatan pengamanan rapat pimpinan dengan melakukan pengacakan/mematikan sinyal frekuensi tertentu pada suatu ruangan dengan menggunakan peralatan jammer sehingga peralatan penerima sinyal tidak dapat berfungsi.

Huruf b

Yang dimaksud dengan "kontra penginderaan; adalah kegiatan memindai/mencari kemungkinan adanya alat peralatan penyadapan yang diletakkan oleh pihak tertentu tanpa sepengetahuan pada ruang kerja/rapat/kediaman pimpinan.

Huruf c

Yang dimaksud dengan "pusat operasi Pengamanan Informasi (*security operation center*)" adalah suatu infrastruktur terpusat untuk kegiatan Pengamanan Informasi dengan melakukan proses pengawasan, perlindungan, dan penanggulangan insiden Keamanan

Informasi dengan memperhatikan aspek personil, proses pelaksanaan, dan ketersediaan teknologi.

Ayat (2)

Huruf a

Yang dimaksud dengan “materiil sandi” adalah barang atau benda dalam penyelenggaraan persandian

Huruf b

Cukup Jelas

Huruf c

Cukup Jelas

Ayat (3)

Cukup Jelas

Ayat (4)

Cukup Jelas

Ayat (5)

Cukup Jelas

Pasal 19

Cukup Jelas.

Pasal 20

Cukup Jelas.

Pasal 21

Ayat (1)

Cukup Jelas

Ayat (2)

Yang dimaksud dengan “nirsangkal” merupakan pengamanan informasi dalam bentuk bukti/identitas yang tak terbantahkan bahwa informasi tersebut memang benar dibuat oleh si pembuat informasi dan sekaligus dapat menunjukkan bahwa pemilik informasi tidak akan dapat menyangkal informasi itu miliknya atau telah disahkan olehnya.

Ayat (3)

Cukup Jelas

Ayat (4)

Cukup Jelas

Ayat (5)

Cukup Jelas

Ayat (6)

Cukup Jelas

Ayat (7)

Cukup Jelas

Pasal 22

Cukup Jelas.

Pasal 23

Cukup Jelas.

Pasal 24

Cukup Jelas

Pasal 25

Cukup Jelas.

Pasal 26

Cukup Jelas.

Pasal 27

Cukup Jelas.

Pasal 28

Cukup Jelas

Pasal 29

Ayat (1)

Cukup Jelas.

Ayat (2)

Huruf a

Cukup Jelas.

Huruf b

Cukup Jelas.

Huruf c

Cukup Jelas.

Huruf d

Yang dimaksud dengan “pihak lainnya” adalah para pihak yang ada kaitannya dengan pelaksanaan tugas di bidang Keamanan Informasi.

Pasal 30

Cukup Jelas.

Pasal 31

Cukup Jelas.

Pasal 32

Cukup Jelas

Pasal 33

Cukup Jelas.

Pasal 34

Cukup Jelas.

Pasal 35

Cukup Jelas

Pasal 36

Cukup Jelas.

Pasal 37

Cukup Jelas.

Pasal 38

Cukup Jelas.

Pasal 39

Cukup Jelas.

Pasal 40

Cukup Jelas

Pasal 41

Cukup Jelas.

Pasal 42

Cukup Jelas.

Pasal 43

Cukup Jelas.

Pasal 44

Cukup Jelas.

Pasal 45

Cukup Jelas.

Pasal 46

Cukup Jelas.

Pasal 47

Cukup Jelas.

Pasal 48

Cukup Jelas

Pasal 49

Cukup Jelas

TAMBAHAN LEMBARAN DAERAH PROVINSI SUMATERA BARAT NOMOR 174