GUBERNUR KALIMANTAN TIMUR

SALINAN

PERATURAN GUBERNUR KALIMANTAN TIMUR

NOMOR 20 TAHUN 2022

TENTANG

PEDOMAN PENYELENGGARAAN PERSANDIAN
UNTUK PENGAMANAN INFORMASI PEMERINTAH DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR KALIMANTAN TIMUR,

Menimbang :

a. bahwa dalam rangka melindungi informasi di lingkungan Pemerintah Provinsi Kalimantan Timur, perlu melakukan upaya pengamanan informasi melalui penyelenggaraan persandian;

b. bahwa berdasarkan ketentuan Pasal 4 ayat (2) Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, Gubernur sesuai dengan kewenangan bertanggung jawab terhadap penyelenggaraan persandian untuk pengamanan informasi;

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

Mengingat :

1. Pasal 18 Ayat (6) Undang-Undang Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan 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 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);

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 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
4. Undang-Undang Nomor 10 Tahun 2022 tentang Provinsi Kalimantan Timur (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 70, Tambahan Lembaran Negara Republik Indonesia Nomor 6781);
5. Peraturan Presiden Nomor 79 Tahun 2021 tentang Tunjangan Jabatan Fungsional Sandiman (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 199);
6. 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 Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan Atas Peraturan Menteri Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2018 Nomor 157);
7. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
8. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);

MEMUTUSKAN :

Menetapkan : PERATURAN GUBERNUR TENTANG PEDOMAN PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI PEMERINTAH DAERAH.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Daerah adalah Provinsi Kalimantan Timur.
2. Gubernur adalah Gubernur Kalimantan Timur.
3. Pemerintah Daerah adalah Gubernur sebagai unsur penyelenggaraan pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan otonom Provinsi Kalimantan Timur.
4. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Gubernur dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
5. Kabupaten/Kota adalah Kabupaten/Kota se-Provinsi Kalimantan Timur.
6. Dinas Komunikasi dan Informatika yang selanjutnya disebut Dinas Kominfo adalah PD 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. Jaring Komunikasi Sandi yang selanjutnya disingkat JKS adalah keterhubungan antar pengguna Persandian melalui jaring telekomunikasi.
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. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi elektronik.
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. Sumber Daya Manusia yang selanjutnya disingkat SDM adalah sumber daya manusia aparatur pemerintah Daerah.
15. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

16. Pusat Operasi Pengamanan Informasi adalah pusat operasi kegiatan pengamanan informasi dengan melakukan proses pengawasan, perlindungan dan penanggulangan insiden keamanan informasi dengan memperhatikan aspek personil, proses pelaksanaan dan ketersediaan teknologi.

Pasal 2

Peraturan Gubernur ini dimaksudkan untuk memberikan pedoman bagi Pemerintah Daerah dalam melaksanakan kebijakan, program, dan kegiatan penyelenggaraan Persandian untuk Pengamanan Informasi.

Pasal 3

Peraturan Gubernur ini bertujuan untuk:
a. menciptakan harmonisasi dalam melaksanakan Persandian untuk Pengamanan Informasi antara Pemerintah Pusat dan Pemerintah Daerah;
b. meningkatkan komitmen, efektivitas, dan kinerja Pemerintah Daerah dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan Persandian untuk Pengamanan Informasi; dan
c. memberikan pedoman bagi Pemerintah Daerah dalam menetapkan pola hubungan komunikasi sandi antar PD, dengan Pemerintah Pusat dan Pemerintah Kabupaten/Kota.

Pasal 4

Ruang lingkup Peraturan Gubernur ini meliputi:
a. penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah;
b. penetapan pola hubungan komunikasi sandi antar PD dan dengan Pemerintah Kabupaten/Kota;
c. pemantauan, evaluasi dan pelaporan;
d. pembinaan dan pengawasan teknis; dan
e. pendanaan.

BAB II
PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 5

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

(2) Penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) diintegrasikan dengan dokumen perencanaan pembangunan Daerah berupa Rencana Pembangunan Jangka Panjang Daerah (RPJPD), Rencana Pembangunan Jangka Menengah Daerah (RPJMD), dan Rencana Kerja Pemerintah Daerah (RKPD).

Pasal 6

(1) Gubernur bertanggung jawab terhadap penyelenggaraan Persandian untuk Pengamanan Informasi.

(2) Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah sebagaimana dimaksud pada ayat (1) dilaksanakan melalui:
   a. penyusunan kebijakan Pengamanan Informasi;
   b. pengelolaan sumber daya Keamanan Informasi;
   c. pengamanan Sistem Elektronik dan pengamanan informasi nonelektronik; dan
   d. penyediaan layanan Keamanan Informasi.

Bagian Kedua
Penyusunan Kebijakan Pengamanan Informasi

Pasal 7

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf a dilakukan dengan:
a. menyusun rencana strategis Pengamanan Informasi;
b. menetapkan arsitektur Keamanan Informasi; dan
c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

Pasal 8

(1) Penyusunan rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 7 huruf a dilakukan oleh Dinas Kominfo.

(2) Rencana strategis sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. tujuan, sasaran, program, kegiatan, dan target pelaksanaan Pengamanan Informasi setiap tahun untuk jangka waktu 5 (lima) tahun; dan
   b. peta rencana penyelenggaraan Pengamanan Informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun untuk jangka waktu 5 (lima) tahun.

(3) Rencana strategis Pengamanan Informasi yang telah disusun sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam rencana pembangunan jangka menengah Daerah.

(4) Dalam melakukan penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) huruf a, Dinas Kominfo dapat melakukan koordinasi dan konsultasi kepada BSSN.

Pasal 9

(1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 7 huruf b ditetapkan oleh Gubernur.

(2) Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) memuat:
   a. infrastruktur teknologi informasi;
   b. desain keamanan perangkat teknologi Informasi dan keamanan jaringan; dan
   c. aplikasi keamanan perangkat teknologi Informasi dan keamanan jaringan.

(3) Dalam melakukan penyusunan Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1), Gubernur dapat melakukan koordinasi dan konsultasi kepada BSSN melalui Dinas Kominfo.

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

(5) Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (4) dilakukan evaluasi oleh Gubernur pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu-waktu sesuai dengan kebutuhan.

Pasal 10

(1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 7 huruf c ditetapkan oleh Gubernur.

(2) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) paling sedikit terdiri atas:
   a. keamanan sumber daya teknologi informasi;
   b. keamanan akses kontrol;
   c. keamanan data dan informasi;
   d. keamanan SDM;
   e. keamanan jaringan;
   f. keamanan surat elektronik;
   g. keamanan pusat data; dan/atau
   h. keamanan komunikasi.

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

Bagian Ketiga
Pengelolaan Sumber Daya Keamanan Informasi

Pasal 11

(1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf b dilaksanakan oleh Dinas Kominfo.

(2) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. pengelolaan aset keamanan teknologi informasi dan komunikasi;
   b. pengelolaan SDM; dan
   c. manajemen pengetahuan.

Pasal 12

(1) Pengelolaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi Informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.

(2) Aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi, dan/atau memulihkan insiden Keamanan Informasi dalam Sistem Elektronik.

Pasal 13

Pengelolaan SDM sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b dilakukan melalui serangkaian proses sebagai berikut:
a. pengembangan kompetensi;
b. pembinaan karir;
c. pendayagunaan; dan
d. pemberian tunjangan.

Pasal 14

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 13 huruf a dilaksanakan dengan ketentuan:
   a. melalui tugas belajar, pendidikan dan pelatihan pembentukan dan penjenjangan fungsional, pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, workshop, seminar, dan kegiatan lainnya yang terkait pengembangan kompetensi SDM di bidang Keamanan Informasi;
   b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya, atau Pemerintah Daerah; dan

c. memenuhi jumlah waktu paling sedikit seorang pegawai untuk meningkatkan kompetensi bidangnya.

(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 13 huruf b dilaksanakan dengan ketentuan:
a. pembinaan jabatan fungsional di bidang Keamanan Informasi; dan
b. pengisian formasi jabatan pimpinan tinggi, jabatan administrator, dan jabatan pengawas sesuai dengan standar kompetensi yang ditetapkan.

(3) Pendayagunaan sebagaimana dimaksud dalam Pasal 13 huruf c dilaksanakan agar seluruh SDM yang bertugas di bidang Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan.

(4) Pemberian tunjangan sebagaimana dimaksud dalam Pasal 13 huruf d, sesuai ketentuan peraturan perundang-undangan.

Pasal 15

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c dilakukan untuk meningkatkan kualitas layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.

(2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi Pemerintah Daerah.

(3) Manajemen pengetahuan sebagaimana dimaksud pada ayat (2) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi Pemerintah Daerah.

(4) Dalam pelaksanaan manajemen pengetahuan, Pemerintah Daerah berkoordinasi dan dapat melakukan konsultasi dengan BSSN.

Bagian Keempat
Pengamanan Sistem Elektronik dan Pengamanan Informasi Non Elektronik

Pasal 16

Pengamanan Sistem Elektronik dan pengamanan Informasi non elektronik sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf c dilaksanakan oleh Dinas Kominfo sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 17

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 16 terdiri atas:

a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirsangkal terhadap data dan Informasi;
b. penjaminan ketersediaan infrastruktur yang terdiri atas pusat data, jaringan intra pemerintah, dan sistem penghubung layanan penyelenggaraan pemerintahan berbasis elektronik; dan
c. penjaminan keutuhan, ketersediaan, dan keaslian aplikasi.

Pasal 18

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 17, Dinas Kominfo melakukan:
   a. identifikasi;
   b. deteksi;
   c. proteksi; dan
   d. penanggulangan dan pemulihan.

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

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

(4) Proteksi sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan kegiatan mitigasi risiko dan penerapan pelindungan 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 19

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 16, 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 BSSN dan/atau lembaga penyelenggara Sertifikasi Elektronik dalam negeri yang telah diakui.

(3) Untuk mendapatkan Sertifikat elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 20

(1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 19 ayat (1), Pemerintah Daerah dapat menyelenggarakan pusat operasi Pengamanan Informasi sesuai dengan standar yang ditetapkan oleh BSSN.

(2) Pusat operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk pengamanan Sistem Elektronik dengan melakukan proses pengawasan, penanggulangan, dan pemulihan atas insiden keamanan Sistem Elektronik dengan memperhatikan aspek personel, proses pelaksanaan, dan ketersediaan teknologi.

Pasal 21

(1) Pengamanan informasi non elektronik sebagaimana dimaksud dalam Pasal 16 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi non elektronik.

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

Pasal 22

(1) Dinas Kominfo melaksanakan audit Keamanan Informasi di lingkup Pemerintah Daerah.

(2) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (1) meliputi audit keamanan Sistem Elektronik dan audit pelaksanaan sistem manajemen.

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

Bagian Kelima
Penyediaan Layanan Keamanan Informasi

Pasal 23

(1) Penyediaan layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf d dilaksanakan oleh Dinas Kominfo.

(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna layanan yang terdiri atas:
   a. Gubernur dan Wakil Gubernur;
   b. PD;
   c. pegawai atau aparatur sipil negara pada Pemerintah Daerah; dan
   d. pihak lainnya.

Pasal 24

Jenis layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 23 ayat (1) meliputi:

a. identifikasi kerentanan dan penilaian risiko 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 melalui penyandiaan perangkat teknologi Keamanan Informasi dan JKS;
e. fasilitasi sertifikasi penerapan manajemen pengamanan Sistem Elektronik;
f. audit keamanan Sistem Elektronik;
g. audit keamanan pelaksanaan sistem manajemen;
h. literasi Keamanan Informasi dalam rangka peningkatan kesadaran Keamanan Informasi dan pengukuran tingkat kesadaran Keamanan Informasi di lingkungan Pemerintah Daerah dan publik;
i. peningkatan kompetensi sumber daya manusia SDM di bidang Keamanan Informasi dan/atau persandian;
j. pengelolaan Pusat Operasi Pengamanan Informasi;
k. penanganan insiden Keamanan Sistem Elektronik;
l. forensik digital;
m. perlindungan Informasi pada kegiatan penting Pemerintah Daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
n. perlindungan Informasi pada aset/fasilitas penting milik atau yang akan digunakan Pemerintah Daerah melalui kegiatan kontra penginderaan;
o. konsultasi Keamanan Informasi bagi pengguna layanan; dan/atau
p. jenis layanan Keamanan Informasi lainnya.

Pasal 25

(1) Dalam menyediakan layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 24, Dinas Kominfo melaksanakan 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 sebagaimana dimaksud pada ayat (1) merupakan penanganan terhadap keluhan, gangguan, masalah, permintaan, dan/atau perubahan layanan Keamanan Informasi dari pengguna layanan.

(4) Manajemen layanan Keamanan Informasi sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen layanan Keamanan Informasi.

Pasal 26

(1) Kegiatan audit sebagaimana dimaksud dalam Pasal 24 huruf f dan huruf g, digunakan untuk mengukur tingkat kerawanan dan keamanan Sistem Elektronik.

(2) Kegiatan audit sebagaimana dimaksud pada ayat (1) dilaksanakan secara berkala paling sedikit 1 (satu) tahun sekali, atau jika terjadi pembaharuan/perubahan/peningkatan/perbaikan pada Sistem Elektronik di lingkungan Pemerintah Daerah.

(3) Laporan hasil kegiatan audit merupakan informasi berklasifikasi dan dapat digunakan sebagai dasar untuk melakukan pengembangan Sistem Elektronik.

Pasal 27

(1) Pusat Operasi Pengamanan Informasi sebagaimana dimaksud dalam Pasal 24 huruf j merupakan suatu infrastruktur terpusat untuk melaksanakan kegiatan Pengamanan Informasi dengan melakukan proses pengawasan, perlindungan, dan penanggulangan insiden keamanan informasi dengan memperhatikan aspek personil, proses pelaksanaan, dan ketersediaan teknologi.

(2) Pemerintah Daerah bersama *Network Operation Center* (NOC) setempat menyelenggarakan Pusat Operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (1).

(3) Pusat Operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (2) dibangun secara terpusat dan terhubung dengan BSSN agar kegiatan berlangsung secara responsif.

Pasal 28

(1) Kegiatan Pengamanan Informasi lainnya sebagaimana dimaksud dalam Pasal 24 huruf p merupakan kegiatan yang dilaksanakan untuk mendukung Pengamanan Informasi.

(2) Kegiatan Pengamanan Informasi lainnya, sebagaimana dimaksud pada ayat (1), harus mendapatkan persetujuan dari Kepala Dinas Kominfo.

BAB III
PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PD

Pasal 29

(1) Gubernur menetapkan pola hubungan komunikasi sandi antar PD.

(2) Penetapan pola hubungan komunikasi sandi antar PD sebagaimana dimaksud pada ayat (1) untuk menentukan JKS internal Pemerintah Daerah.

(3) JKS internal Pemerintah Daerah sebagaimana dimaksud pada ayat (2) terdiri atas:
a. JKS antar PD;
b. JKS PD; dan
c. JKS pimpinan Daerah.

(4) JKS antar PD sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh PD.

(5) JKS PD sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar pengguna layanan di lingkup internal PD.

(6) JKS pimpinan Daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Gubernur, Wakil Gubernur dan kepala PD.

Pasal 30

(1) Penetapan pola hubungan komunikasi sandi antar PD sebagaimana dimaksud dalam Pasal 26 ayat (1) dilaksanakan melalui:
a. identifikasi pola hubungan komunikasi sandi; dan
b. analisis pola hubungan komunikasi sandi.

(2) Identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf a, dilakukan terhadap:
a. pola hubungan komunikasi pimpinan dan pejabat struktural internal Pemerintah Daerah;
b. alur informasi yang dikomunikasikan antar PD dan internal PD;
c. teknologi informasi dan komunikasi;
d. infrastruktur komunikasi; dan
e. kompetensi personi l.

(3) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2).

(4) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3) memuat:
a. pengguna layanan yang akan terhubung dalam JKS;
b. topologi atau bentuk atau model keterhubungan JKS antar pengguna layanan;
c. perangkat keamanan teknologi Informasi dan komunikasi, dan infrastruktur komunikasi, serta fasilitas lainnya yang dibutuhkan; dan
d. tugas dan tanggung jawab pengelola dan pengguna layanan.

(5) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (4) ditetapkan sebagai pola hubungan komunikasi sandi antar PD oleh Gubernur dalam bentuk keputusan.

(6) Keputusan sebagaimana dimaksud pada ayat (5) paling sedikit memuat:
a. entitas Pengguna layanan yang terhubung dalam JKS;
b. topologi atau bentuk atau model keterhubungan antar Pengguna layanan;

c. sarana dan prasarana yang digunakan; dan
d. tugas dan tanggung jawab pengelola dan pengguna layanan.

(7) Salinan keputusan sebagaimana dimaksud pada ayat (6) disampaikan oleh Gubernur kepada Kepala BSSN.

BAB IV
PEMANTAUAN, EVALUASI DAN PELAPORAN

Pasal 31

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah serta penetapan pola hubungan komunikasi sandi antar PD.

(2) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) terhadap penyelenggaraan persandian dilaksanakan oleh Pemerintah Daerah meliputi:
a. pemantauan dan evaluasi yang bersifat rutin dan insidentil; dan
b. pemantauan dan evaluasi yang bersifat tahunan.

(3) Dinas Kominfo menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) dan laporan hasil pemantauan dan evaluasi Kabupaten/Kota kepada Gubernur dan Kepala BSSN.

Pasal 32

Pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah serta penetapan pola hubungan komunikasi sandi antar PD dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB V
PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 33

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar PD dilaksanakan oleh BSSN dan Gubernur sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 34

(1) Dalam melaksanakan pembinaan dan pengawasan teknis sebagaimana dimaksud dalam Pasal 30, Pemerintah Daerah bersama BSSN menyelenggarakan rapat koordinasi urusan Persandian.

(2) Rapat koordinasi sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam setahun.

BAB VI
PENDANAAN

Pasal 35

Segala pendanaan yang timbul sebagai akibat ditetapkannya Peraturan Gubernur ini dibebankan pada:
a. anggaran Pendapatan dan Belanja Daerah; dan
b. sumber dana lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII
KETENTUAN PENUTUP

Pasal 36

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Kalimantan Timur.

Ditetapkan di Samarinda
pada tanggal 13 Juli 2022

GUBERNUR KALIMANTAN TIMUR,

ttd

ISRAN NOOR

Diundangkan di Samarinda
pada tanggal 13 Juli 2022

Pj. SEKRETARIS DAERAH
PROVINSI KALIMANTAN TIMUR,

ttd

RIZA INDRA RIADI

Salinan sesuai dengan aslinya
SEKRETARIAT DAERAH PROV. KALTIM
KEPALA BIRO HUKUM,

ROZANI ERAWADI
NIP. 19710124 199703 1 007

BERITA DAERAH PROVINSI KALIMANTAN TIMUR TAHUN 2022 NOMOR 20.