



GUBERNUR LAMPUNG
PERATURAN GUBERNUR LAMPUNG
NOMOR 30 TAHUN 2021

TENTANG

**PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH PROVINSI LAMPUNG**

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR LAMPUNG,

Menimbang :

- a. bahwa penyelenggaraan pemerintahan daerah diarahkan untuk mewujudkan kesejahteraan masyarakat melalui peningkatan pelayanan kepada masyarakat;
- b. bahwa untuk mendukung pelayanan kepada masyarakat dengan perlindungan informasi publik perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian;
- c. bahwa untuk melaksanakan ketentuan Pasal 4 ayat (1) huruf Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;
- d. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a, huruf b, dan huruf c perlu menetapkan Peraturan Gubernur tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintah Provinsi Lampung;

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 14 Tahun 1964 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 3 Tahun 1964 tentang Pembentukan Daerah Tingkat I Lampung dengan mengubah Undang-Undang Nomor 25 Tahun 1959 tentang Pembentukan Daerah Tingkat I Sumatera Selatan (Lembaran Negara Republik Indonesia Tahun 1964 Nomor 80 menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 1964 Nomor 95, Tambahan Lembaran Negara Republik Indonesia Nomor 2688);
3. Undang-Undang Nomor 23 Tahun 2006 tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 124, Tambahan Lembaran Negara Republik Indonesia Nomor 4674) sebagaimana telah diubah dengan Undang-Undang Nomor 24 Tahun 2013 tentang Administrasi Kependudukan (Lembaran Negara Republik Indonesia Tahun 2013 Nomor 232, Tambahan Lembaran Negara Republik Indonesia Nomor 5475);

4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
5. 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);
6. 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 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);
7. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
8. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);
9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 18 Tahun 2019 tentang Jabatan Fungsional Sandiman (Berita Negara Republik Indonesia Tahun 2019 Nomor 1010);
10. Peraturan Kepala Sandi Negara Nomor 10 Tahun 2012 tentang Pedoman Pengelolaan dan Perlindungan Informasi Berklasifikasi Milik Pemerintah (Berita Negara Republik Indonesia Tahun 2012 Nomor 808);
11. Peraturan Kepala Sandi Negara Nomor 5 Tahun 2014 tentang Standar Algoritma Kriptografi pada Instansi Pemerintah (Berita Negara Republik Indonesia Tahun 2014 Nomor 1862);
12. Peraturan Kepala Lembaga Sandi Negara Nomor 6 Tahun 2016 tentang Pengendalian Persandian (Berita Negara Republik Indonesia Tahun 2016 Nomor 1123);
13. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2014 Nomor 2036) sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan Atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2018 Nomor 1714);
14. Peraturan Badan dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);

15. Peraturan Daerah Nomor 4 Tahun 2019 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Provinsi Lampung Tahun 2019 Nomor 4, Tambahan Lembaran Daerah Provinsi Lampung Nomor 491);
16. Peraturan Gubernur Nomor 56 Tahun 2019 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta Tata Kerja Perangkat Daerah Provinsi Lampung (Berita Daerah Provinsi Lampung Tahun 2019 Nomor 56);

MEMUTUSKAN:

Menetapkan : **PERATURAN GUBERNUR TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH PROVINSI LAMPUNG.**

**BAB I
KETENTUAN UMUM**

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Daerah adalah Provinsi Lampung.
2. Pemerintahan Daerah adalah Pemerintah Provinsi Lampung.
3. Gubernur adalah Gubernur Lampung.
4. Dinas Komunikasi, Informatika dan Statistik yang selanjutnya disebut Dinas adalah Dinas Komunikasi, Informatika dan Statistik Provinsi Lampung.
5. Kepala Dinas Komunikasi, Informatika dan Statistik yang selanjutnya disingkat Kepala Dinas adalah Kepala Dinas Komunikasi, Informatika dan Statistik Provinsi Lampung.
6. Perangkat Daerah yang selanjutnya disingkat PD adalah Perangkat Daerah di lingkungan Pemerintah Daerah.
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 disebut JKS adalah keterhubungan antar pengguna persandian melalui jaring telekomunikasi.
9. 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 Balai Sertifikasi Elektronik pada Badan Siber dan Sandi Negara.

10. Dokumen Elektronik adalah setiap Informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya yang dapat dilihat, ditampilkan, dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
11. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, dan menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan informasi elektronik.
12. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah Lembaga Pemerintah yang menyelenggarakan tugas pemerintah dibidang keamanan siber dan persandian.

Pasal 2

Peraturan Gubernur ini dimaksudkan untuk memberikan pedoman dalam melaksanakan kebijakan, program, dan kegiatan penyelenggaraan Persandian untuk pengamanan informasi di lingkungan Pemerintah Provinsi Lampung.

Pasal 3

Peraturan Gubernur ini bertujuan untuk:

- a. menciptakan harmonisasi dalam pembagian urusan pemerintahan bidang Persandian;
- b. menjadi pedoman dalam melaksanakan penyelenggaraan Persandian untuk pengamanan Informasi di lingkungan Pemerintah;
- c. meningkatkan efektivitas pelaksanaan kebijakan, program dan kegiatan penyelenggaraan persandian untuk pengamanan informasi;

Pasal 4

Ruang lingkup penyelenggaraan Persandian dari Peraturan Gubernur ini meliputi:

- a. penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah; dan
- b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.

BAB II

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI PEMERINTAH DAERAH

Bagian Kesatu Umum

Pasal 5

Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah sebagaimana dimaksud dalam Pasal 4 huruf a 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 6

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 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.

Pasal 7

- (1) Rencana strategis pengamanan informasi sebagaimana dimaksud dalam Pasal 6 huruf a disusun oleh Gubernur sesuai dengan kewenangannya.
- (2) Penyusunan rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.
- (3) Rencana strategis sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. 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;
- (4) Rencana strategis Pengamanan Informasi yang telah disusun sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah.
- (5) Dalam melakukan penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) Dinas dapat melakukan koordinasi dan konsultasi kepada Badan Siber dan Sandi Negara.

Pasal 8

- (1) Arsitektur keamanan informasi sebagaimana dimaksud dalam Pasal 6 huruf b ditetapkan oleh Gubernur atas usulan Pimpinan Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian.
- (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) Arsitektur keamanan informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.
- (4) Arsitektur keamanan informasi dilakukan evaluasi oleh Gubernur pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu waktu sesuai dengan kebutuhan.
- (5) Dalam melakukan penyusunan Arsitektur keamanan informasi sebagaimana dimaksud pada ayat (1), Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian dapat melakukan koordinasi dan konsultasi kepada BSSN.

Pasal 9

- (1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 huruf c ditetapkan oleh Gubernur atas usulan Pimpinan Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian.
- (2) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. keamanan sumber daya teknologi informasi;
 - b. keamanan akses kontrol;
 - c. keamanan data dan informasi;
 - d. keamanan sumber daya manusia;
 - 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), Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian dapat melakukan koordinasi dan konsultasi kepada BSSN.

Bagian Ketiga Pengelolaan Sumber Daya Keamanan Informasi

Pasal 10

- (1) Pengelolaan sumber daya keamanan informasi sebagaimana dimaksud dalam Pasal 5 huruf b dilaksanakan oleh Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian.
- (2) Pengelolaan sumber daya keamanan informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. pengelolaan aset keamanan teknologi informasi dan komunikasi;
 - b. pengelolaan sumber daya manusia; dan
 - c. manajemen pengetahuan.

Pasal 11

- (1) Pengelolaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud dalam Pasal 10 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 12

- (1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf b dilakukan oleh Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian.
- (2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses sebagai berikut:
 - a. pengembangan kompetensi;
 - b. pembinaan karir;
 - c. pendayagunaan; dan
 - d. pemberian pengamanan persandian.

Pasal 13

- (1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf a dilaksanakan dengan ketentuan:
 - a. melalui pendidikan dan pelatihan pembentukan dan penjenjangan fungsional, pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, workshop, seminar, dan kegiatan lainnya yang terkait pengembangan kompetensi sumber daya manusia di bidang Keamanan Informasi;
 - b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya, atau Pemerintah Daerah; dan
- (2) Pembinaan karir sebagaimana dimaksud dalam Pasal 12 ayat (2) 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 2 ayat (2) huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di bidang Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar Kompetensi kerja pegawai yang ditetapkan.
- (4) Pemberian tunjangan pengamanan persandian sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf d adalah pemberian tunjangan khusus kepada Aparatur Sipil Negara yang diangkat sebagai pengelola pengamanan persandian di lingkungan Pemerintah Daerah yang lingkup tugas dan tanggung jawabnya meliputi bidang pengamanan persandian sesuai dengan ketentuan peraturan Perundang-undangan.
- (5) Pemberian tunjangan pengamanan persandian di lingkungan Pemerintah Daerah ditetapkan dengan Keputusan Gubernur atas usulan Pimpinan Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian
- (6) Pengelolaan sumber daya Keamanan Informasi dilaksanakan oleh Perangkat Daerah yang melaksanakan urusan pemerintah bidang persandian.
- (7) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (5) terdiri atas:
 - a. Pengelolaan aset keamanan teknologi informasi dan komunikasi;
 - b. Pengelolaan sumber daya manusia; dan
 - c. Manajemen pengetahuan.

Pasal 14

- (1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf c dilakukan oleh Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian.
- (2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.
- (3) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi pemerintah daerah.
- (4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi pemerintah daerah.
- (5) Dalam pelaksanaan manajemen pengetahuan, Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian dapat melakukan koordinasi dan konsultasi dengan BSSN.

Bagian Keempat Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Pasal 15

Pengamanan Sistem Elektronik dan pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 5 huruf c dilaksanakan oleh Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 16

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 15 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 17

- (1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 16, Dinas 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 insides pada 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 18

- (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 19

- (1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 18 ayat (1) Pemerintah Daerah dapat menyelenggarakan Pusat Operasi Pengamanan Informasi sesuai 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 insides keamanan Sistem Elektronik dengan memperhatikan aspek personel, proses pelaksanaan, dan ketersediaan teknologi.

Pasal 20

- (1) Pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 15 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.
- (2) Pengamanan Informasi nonelektronik sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Dinas sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 21

- (1) Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian melaksanakan audit Keamanan Informasi di lingkup Pemerintah Daerah.
- (2) Audit Keamanan Informasi 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 22

- (1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf d dilaksanakan oleh Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian.
- (2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
- a. Gubernur dan Wakil Gubernur;
 - b. Perangkat Daerah;
 - c. Aparatur sipil negara pada Pemerintah Daerah; dan
 - d. Pihak lainnya;

Pasal 23

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 22 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 penyediaan perangkat teknologi Keamanan Informasi dan jaring komunikasi sandi;
- 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 di bidang Keamanan Informasi dan/atau persandian;
- j. pengelolaan pusat operasi Pengamanan Informasi;
- k. penanganan insiden Keamanan Sistem Elektronik;
- 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 kegiatan kontra penginderaan;
- n. konsultasi Keamanan Informasi bagi Pengguna Layanan;
- o. jenis Layanan Keamanan Informasi lainnya; dan
- p. forensik digital.

Pasal 24

- (1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 23, Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian 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.

BAB III PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Pasal 25

- (1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 4 huruf b ditetapkan oleh Gubernur.
- (2) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (1) untuk menentukan jaring komunikasi sandi internal Pemerintah Daerah.
- (3) Jaring komunikasi sandi internal Pemerintah Daerah sebagaimana dimaksud pada ayat (2) terdiri atas:
 - a. Jaring komunikasi sandi antar Perangkat Daerah;
 - b. Jaring komunikasi sandi internal Perangkat Daerah; dan
 - c. Jaring komunikasi sandi Pimpinan Daerah;
- (4) Jaring komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh Perangkat Daerah.
- (5) Jaring komunikasi sandi internal Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar Pengguna Layanan di lingkup internal Perangkat Daerah.
- (6) Jaring komunikasi sandi Pimpinan Daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Gubernur, Wakil Gubernur, dan Kepala Perangkat Daerah.

Pasal 26

- (1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 25 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 Perangkat Daerah dan internal Perangkat Daerah;
 - c. teknologi informasi dan komunikasi;
 - d. infrastruktur komunikasi; dan
 - e. kompetensi personel.
- (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 jaringan komunikasi sandi;
 - b. topologi atau bentuk atau model keterhubungan jaringan komunikasi sandi 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 Perangkat Daerah dalam bentuk keputusan Gubernur.
- (6) Keputusan Gubernur sebagaimana dimaksud pada ayat (5) paling sedikit memuat:
 - a. entitas Pengguna Layanan yang terhubung dalam jaringan komunikasi sandi;
 - 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.

Pasal 27

- (1) Pola hubungan komunikasi sandi antar perangkat daerah yang telah ditetapkan sebagaimana dimaksud dalam Pasal 26 ayat (5), diimplementasikan dengan memanfaatkan perangkat dan/atau aplikasi yang telah diamankan dengan persandian;
- (2) Perangkat dan/atau aplikasi yang telah diamankan dengan persandian sebagaimana dimaksud pada ayat (1), terdiri atas:
 - a. *handphone* bersandi;
 - b. *handytalky* bersandi;
 - c. *secure chat application*;
 - d. *secure e-mail*;
 - e. *file encryption*; dan
 - f. perangkat dan/atau aplikasi yang telah diamankan dengan persandian lainnya.

BAB IV PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 28

- (1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.
- (2) Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali.
- (3) Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) kepada Gubernur dan Kepala BSSN.

Pasal 29

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

BAB V PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 30

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dilaksanakan oleh BSSN dan Gubernur sebagai wakil Pemerintah Pusat sesuai dengan kewenangannya.

Pasal 31

- (1) Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar perangkat daerah dilakukan oleh Gubernur.
- (2) Pembinaan dan Pengawasan teknis sebagaimana dimaksud pada ayat (1) dilakukan Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian sesuai dengan ketentuan peraturan perundang-undangan.
- (3) Perangkat Daerah yang melaksanakan urusan pemerintahan bidang persandian menyampaikan Pembinaan dan Pengawasan teknis sebagaimana dimaksud pada ayat (2) disampaikan ke BSSN.

Pasal 32

- (1) Dalam melaksanakan pembinaan dan pengawasan teknis sebagaimana dimaksud dalam Pasal 30, Pemerintah Daerah sesuai dengan kewenangannya 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 33

Pendanaan pelaksanaan penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah bersumber dari:

- a. Anggaran Pendapatan dan Belanja Daerah Provinsi; dan
- b. Sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

**BAB VII
PENUTUP**

Pasal 34

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Lampung.

Ditetapkan di Telukbetung
pada tanggal 13 Agustus 2021

GUBERNUR LAMPUNG,

ttd

ARINAL DJUNAIDI

Diundangkan di Telukbetung
pada tanggal 13 Agustus 2021

SEKRETARIS DAERAH PROVINSI LAMPUNG,

ttd

FAHRIZAL DARMINTO

Salinan sesuai aslinya
Kepala Biro Hukum,



Fuadi Jailani, SH, MH
Pembina Tingkat I

NIP. 19650905 199103 1 004