GUBERNUR SULAWESI SELATAN

PERATURAN GUBERNUR SULAWESI SELATAN
NOMOR 6 TAHUN 2023
TENTANG

PENYELENGGARAAN PERSANDIAN UNTUK
PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA
GUBERNUR SULAWESI SELATAN,

Menimbang : a. bahwa dalam rangka optimalisasi pelaksanaan persandian di daerah yang berfungsi sebagai pengamanan informasi perlu pedoman penggunaan persandian;

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

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

Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58,

Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan antara Pemerintah Pusat dan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6757);
5. Undang-Undang Nomor 4 Tahun 2022 tentang Provinsi Sulawesi Selatan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 64, Tambahan Lembaran Negara Republik Indonesia Nomor 6775
6. 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);
7. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

8. Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 101);
9. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 1054);
10. Peraturan Daerah Provinsi Sulawesi Selatan Nomor 10 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Provinsi Sulawesi Selatan Tahun 2016 Nomor 10, Tambahan Lembaran Daerah Provinsi Sulawesi Selatan Nomor 293) sebagaimana telah diubah dengan Peraturan Daerah Provinsi Sulawesi Selatan Nomor 11 Tahun 2019 tentang Perubahan atas Peraturan Daerah Provinsi Sulawesi Selatan Nomor 10 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Provinsi Sulawesi Selatan Tahun 2019 Nomor 11, Tambahan Lembaran Daerah Provinsi Sulawesi Selatan Nomor 309);
11. Peraturan Gubernur Sulawesi Selatan Nomor 50 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Perangkat Daerah ~~Provinsi Sulawesi Selatan~~ (Berita Daerah Provinsi Sulawesi Selatan Tahun 2021 Nomor 50);

MEMUTUSKAN:

Menetapkan : PERATURAN GUBERNUR TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Daerah adalah Provinsi Sulawesi Selatan.
2. Pemerintah Daerah adalah Gubernur sebagai unsur penyelenggara Pemerintah Daerah yang memimpin pelaksanaan urusan pemerintah yang menjadi kewenangan Daerah otonom.
3. Gubernur adalah Gubernur Sulawesi Selatan.
4. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Sulawesi Selatan.
5. Perangkat Daerah adalah Perangkat Daerah di lingkungan Pemerintah Provinsi Sulawesi Selatan.
6. Dinas Komunikasi, Informatika Statistik dan Persandian Provinsi Sulawesi Selatan yang selanjutnya disebut Dinas adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang persandian dan keamanan siber.
7. Kepala Dinas adalah Kepala Dinas Komunikasi, Informatika, Statistik dan Persandian Provinsi Sulawesi Selatan.
8. 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.
9. Materiil Sandi yang selanjutnya disebut Matsan adalah barang persandian negara yang memiliki klasifikasi rahasia dan berfungsi sebagai alat pengamanan informasi atau alat analisis sinyal atau bahan/perangkat yang berhubungan dengan proses penyelenggaraan pengamanan informasi.
10. Jaring Komunikasi Sandi yang selanjutnya disingkat JKS adalah keterhubungan antar pengguna persandian melalui jaring telekomunikasi.
11. Alat Pendukung Utama Persandian yang selanjutnya disebut APU Persandian adalah peralatan pendukung yang digunakan dalam kegiatan pengamanan persandian.
12. *Jamming* adalah kegiatan untuk mengacak sinyal di waktu dan tempat tertentu.
13. Operasi Siaga Kontra Penginderaan yang selanjutnya disebut Kontra Penginderaan adalah kegiatan yang dibatasi waktu untuk melakukan pencegahan terhadap pengawasan pihak

lain, termasuk metode-metode yang melibatkan peralatan elektronik seperti *bugsweeping* dan mendeteksi adanya peralatan pengawasan (*surveillance*).

14. *Penetration Test* yang selanjutnya disebut PENTEST adalah pengujian keamanan informasi di mana seorang asesor meniru serangan yang biasa sering terjadi untuk mengidentifikasi metode peretasan fitur keamanan aplikasi, sistem, atau jaringan.
15. *Security Operation Center* yang selanjutnya disingkat SOC adalah kegiatan pengamanan informasi dengan melakukan proses pengawasan, perlindungan, dan penanggulangan insiden keamanan informasi dengan memperhatikan aspek personil, proses pelaksanaan, dan ketersediaan teknologi.
16. *Computer Security Insident Response Team* yang selanjutnya disingkat CSIRT adalah kegiatan penanggulangan dan pemulihan terhadap insiden keamanan siber pada sektor Pemerintah Daerah.
17. 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.
18. Informasi publik adalah informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan Negara dan/atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan Undang-Undang ini serta informasi lain yang berkaitan dengan kepentingan publik.
19. Informasi berklasifikasi adalah informasi publik yang dikecualikan menurut Peraturan Perundang-undangan yang berlaku.
20. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.
21. Pengamanan Informasi adalah segala upaya, kegiatan, dan

tindakan untuk mewujudkan Keamanan Informasi.

22. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
23. 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.
24. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
25. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
26. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

Pasal 2

Pembentukan Peraturan Gubernur ini dimaksudkan sebagai pedoman dalam melaksanakan kebijakan, program, dan kegiatan penyelenggaraan persandian untuk pengamanan informasi di lingkungan Pemerintah Daerah.

Pasal 3

Pembentukan Peraturan Gubernur ini bertujuan untuk:

a. menciptakan harmonisasi dalam pembagian urusan pemerintahan bidang Persandian;
b. memfasilitasi Pemerintah Kabupaten/Kota dalam melaksanakan penyelenggaraan persandian untuk pengamanan informasi;
c. meningkatkan efektivitas pelaksanaan kebijakan, program

dan kegiatan penyelenggaraan persandian untuk pengamanan informasi; dan

d. memberikan pedoman bagi Pemerintah Daerah dalam menetapkan pola hubungan komunikasi sandi antar Perangkat Daerah.

Pasal 4

Ruang lingkup pengaturan dalam peraturan Gubernur ini meliputi :

a. perencanaan;
b. penetapan;
c. implementasi;
d. monitoring dan evaluasi;
e. kerja sama;
f. pelaporan; dan
g. pembiayaan.

BAB II

PERENCANAAN

Pasal 5

(1) Perencanaan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Provinsi Sulawesi Selatan dituangkan dalam bentuk rencana strategis Pengamanan Informasi.

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

(3) 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.

(4) Rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan

Gubernur.

Pasal 6

(1) Rencana strategis Pengamanan Informasi yang telah disusun sebagaimana dimaksud dalam Pasal 5 ayat (1) diintegrasikan ke dalam rencana pembangunan jangka menengah Daerah.

(2) Penyusunan rencana Strategis sebagaimana dimaksud pada ayat (1) dikoordinasikan dan dikonsultasikan oleh Dinas kepada BSSN.

BAB III

PELAKSANAAN

Bagian Kesatu

Umum

Pasal 7

(1) Pelaksanaan persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah meliputi:
   a. penyelenggaraan Persandian untuk Pengamanan Informasi;
   b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah; dan
   c. penyelenggaraan Sertifikat Elektronik di lingkungan Pemerintah Daerah untuk mendukung Sistem Pemerintahan Berbasis Elektronik.

(2) Pelaksanaan persandian untuk pengamanan informasi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Gubernur melalui:
   a. penguatan kapasitas kelembagaan, Sumber Daya Manusia, dan sarana prasarana;
   b. mengoordinasikan kegiatan antar Perangkat Daerah; dan/atau
   c. kerja sama dengan Kabupaten/Kota, Provinsi lain, dan/atau Kabupaten/Kota di Provinsi lain.

Pasal 8

(1) Pelaksanaan persandian untuk pengamanan informasi meliputi:

a. penyediaan analisis kebutuhan penyelenggaraan persandian untuk pengamanan informasi;
b. penyediaan kebijakan penyelenggaraan persandian untuk pengamanan informasi;
c. pengelolaan dan perlindungan informasi;
d. pengelolaan sumber daya persandian meliputi sumber daya manusia, materiil sandi dan jaring komunikasi sandi serta anggaran;
e. penyelenggaraan operasional dukungan persandian untuk pengamanan informasi;
f. pengawasan dan evaluasi penyelenggaraan pengamanan informasi melalui persandian di seluruh Perangkat Daerah; dan
g. koordinasi dan konsultasi penyelenggaraan persandian untuk pengamanan informasi.

(2) Pengamanan informasi sebagaimana dimaksud pada ayat (1) mencakup pengamanan fisik, pengamanan logis dan perlindungan secara administrasi.

Bagian Kedua

Penyelenggaraan Persandian untuk Pengamanan Informasi

Paragraf 1

Umum

Pasal 9

Penyelenggaraan Persandian untuk Pengamanan Informasi dilaksanakan melalui:

a. penyusunan kebijakan Pengamanan Informasi;
b. pengelolaan Sumber Daya Keamanan Informasi;
c. pengamanan Sistem Elektronik dan pengamanan Informasi non Elektronik; dan
d. penyediaan layanan Keamanan Informasi.

Paragraf 2

Penyusunan Kebijakan Pengamanan Informasi

Pasal 10

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf a dilaksanakan dengan:

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

Pasal 11

Penyusunan rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 10 huruf a dilaksanakan sesuai ketentuan Pasal 5 dan Pasal 6 Peraturan Gubernur ini.

Pasal 12

(1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 10 huruf b disusun oleh Dinas.
(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) Penyusunan Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) dikoordinasikan dan dikonsultasikan oleh Dinas kepada BSSN.
(4) Arsitektur Keamanan Informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.
(5) Arsitektur Keamanan Informasi dilakukan evaluasi pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu waktu sesuai dengan kebutuhan.

Pasal 13

(1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 10 huruf c dituangkan dalam Standar Operasional Prosedur yang ditetapkan dengan Keputusan Gubernur.
(2) Penetapan Standar Operasional Prosedur sebagaimana dimaksud pada ayat (1) dapat didelegasikan kepada Kepala

Dinas.

(3) 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 sumber daya manusia;
   e. keamanan jaringan;
   f. keamanan surat elektronik;
   g. keamanan pusat data; dan/atau
   h. keamanan komunikasi.

(4) Penyusunan aturan mengenai tata kelola Keamanan Informasi dilaksanakan oleh Dinas dan dikoordinasikan kepada Unit Kerja Perangkat Daerah yang membidangi urusan pemerintahan di bidang hukum.

(5) Penyusunan aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) dikoordinasikan dan dikonsultasikan oleh Dinas kepada BSSN.

Paragraf 3

Pengelolaan Sumber Daya Keamanan Informasi

Pasal 14

(1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 10 huruf b dilaksanakan oleh Perangkat Daerah terkait.

(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 15

(1) Pengelolaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 14 ayat (2)

huruf a dilakukan oleh Dinas dan berkoordinasi dengan Perangkat Daerah yang membidangi urusan aset daerah.

(2) Pengelolaan aset keamanan teknologi informasi dan komunikasi dilakukan melalui perencanaan, pengadaan, pemanfaatan dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan Ketentuan Peraturan Perundang-undangan.

(3) 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 16

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf b dilakukan oleh Dinas dan berkoordinasi dengan Perangkat Daerah yang membidangi urusan kepegawaian dan Perangkat Daerah yang membidangi urusan pengembangan sumber daya manusia.

(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 tunjangan pengamanan persandian.

Pasal 17

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 16 ayat (2) 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 sumber daya manusia di bidang Keamanan Informasi;

b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya, atau Pemerintah Daerah masing-masing; dan

c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi di bidang Keamanan Informasi.

(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 16 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 16 ayat (2) huruf c dilaksanakan dengan ketentuan:

a. seluruh sumber daya manusia yang bertugas di bidang Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan;

b. untuk memenuhi kebutuhan dan mengantisipasi keterbatasan sumber daya manusia persandian, pegawai yang telah memiliki sertifikasi, keahlian dan/atau pernah mengikuti pendidikan dan pelatihan sandi yang diselenggarakan oleh BSSN tetap ditugaskan secara penuh di bidang persandian dan tidak dimutasi ke bidang tugas lain kecuali promosi jabatan.

Pasal 18

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf c dilakukan untuk meningkatkan kualitas layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.

(2) Manajemen pengetahuan 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) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.

(5) Dalam pelaksanaan manajemen pengetahuan, Dinas berkoordinasi dan berkonsultasi dengan BSSN.

Paragraf 4

Pengamanan Sistem Elektronik dan Pengamanan Informasi non Elektronik

Pasal 19

Pengamanan Sistem Elektronik dan Pengamanan Informasi non Elektronik sebagaimana dimaksud dalam Pasal 9 huruf c dilaksanakan oleh Dinas.

Pasal 20

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 19 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 21

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 20, 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 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 sebagaimana mestinya.

Pasal 22

(1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 21 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 insiden keamanan Sistem Elektronik dengan memperhatikan aspek personel, proses pelaksanaan, dan ketersediaan teknologi.

Pasal 23

(1) Pengamanan informasi non elektronik sebagaimana dimaksud dalam Pasal 19 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 24

(1) Dinas 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.

Paragraf 5

Penyediaan Layanan Keamanan Informasi

Pasal 25

(1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf d dilaksanakan oleh Dinas.

(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. Pegawai atau Aparatur Sipil Negara pada Pemerintah Daerah; dan
d. pihak lainnya sesuai dengan kebutuhan.

Pasal 26

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 25 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 peningkatan 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. 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;
p. penanganan dan Pemulihan Insiden Siber; dan/atau
q. jenis Layanan Keamanan Informasi lainnya.

Pasal 27

(1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 26, Dinas 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.

Bagian Ketiga

Penetapan Pola Hubungan Komunikasi Sandi Antar Perangkat Daerah

Pasal 28

(1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf b ditetapkan oleh Gubernur.
(2) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dan Kabupaten/Kota 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 29

(1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 28 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 (4) memuat:
a. pengguna Layanan yang akan terhubung dalam jaring komunikasi sandi;
b. topologi atau bentuk atau model keterhubungan jaring komunikasi sandi antar Pengguna Layanan;
c. perangkat keamanan teknologi Informasi dan komunikasi, infrastruktur komunikasi, serta fasilitasi 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 oleh Gubernur dalam bentuk Keputusan Gubernur.

(6) Keputusan sebagaimana dimaksud pada ayat (5) paling sedikit memuat:
a. entitas Pengguna Layanan yang terhubung dalam jaring 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 (5) disampaikan oleh Gubernur kepada Kepala BSSN.

Bagian Keempat

Penyelenggaraan Sertifikat Elektronik di Lingkungan Pemerintah Daerah Guna Mendukung Sistem Pemerintahan Berbasis Elektronik

Pasal 30

(1) Dalam melaksanakan Pengamanan Sistem Elektronik, wajib menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.
(2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh Balai Sertifikasi Elektronik.
(3) Penyelenggaraan Sertifikat Elektronik di lingkungan Pemerintah Daerah bertujuan:
    a. meningkatkan kapabilitas dan tata kelola Keamanan Informasi dalam penyelenggaraan Sistem Elektronik;
    b. meningkatkan Keamanan Informasi dalam Sistem Elektronik;
    c. meningkatkan kepercayaan, kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan terhadap implementasi Sistem Elektronik; dan
    d. meningkatkan efisiensi dan efektifitas penyelenggaraan pemerintahan dan pelayanan publik.
(4) Untuk mendapatkan Sertifikat Elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan oleh Otoritas Pendaftaran yang bertanggung jawab melakukan pemeriksaan, pemberian persetujuan atau penolakan atas setiap permintaan penerbitan, pembaruan, dan pencabutan Sertifikat Elektronik yang diajukan oleh pemilik atau calon Pemilik Sertifikat Elektronik.
(5) Dinas berkedudukan sebagai Otoritas Pendaftaran.

BAB IV

FORUM KOMUNIKASI PERSANDIAN DAERAH

Pasal 31

(1) Dalam mendukung penyelenggaraan jaring komunikasi sandi yang efektif, efisien dan komprehensif di lingkungan Pemerintah Daerah, perlu dibentuk Forum Komunikasi Sandi Daerah.

(2) Forum Komunikasi Sandi Daerah sebagaimana dimaksud pada ayat (1) dapat beranggotakan Instansi di lingkungan Pemerintah Daerah, Pemerintah Kabupaten/Kota dan Instansi vertikal di Daerah serta Badan Usaha Milik Daerah/Daerah yang memiliki tugas pokok dan fungsi pengelola persandian dan keamanan informasi daerah.

(3) Forum Komunikasi Sandi Daerah sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Gubernur.

BAB V
PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 32

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

(2) Kepala Dinas melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali dan menyampaikan laporannya kepada Gubernur.

(3) Gubernur menyampaikan laporan pelaksanaan penyelenggaraan sebagaimana dimaksud pada ayat (1) kepada Kepala BSSN sebagai pembina tunggal persandian negara dengan tembusan kepada Menteri Dalam Negeri.

(4) Guna kelancaran pelaksanaan tugas sebagaimana dimaksud pada ayat (1) Gubernur dapat membentuk tim yang susunan keanggotaannya terdiri dari unsur instansi terkait sesuai kebutuhan.

Pasal 33

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 VI
PENDANAAN

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/atau
b. sumber lain yang sah dan tidak mengikat sesuai dengan Ketentuan Peraturan Perundang-undangan.

Pasal 35

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Makassar
pada tanggal 24 Januari 2023
GUBERNUR SULAWESI SELATAN,

ANDI SUDIRMAN SULAIMAN

Diundangkan di Makassar
pada tanggal 24 Januari 2023
Pj. SEKRETARIS DAERAH PROVINSI
SULAWESI SELATAN,

ANDI ASLAM PATONANGI

BERITA DAERAH PROVINSI SULAWESI SELATAN TAHUN 2023 NOMOR 6