SALINAN

GUBERNUR SUMATERA UTARA

PERATURAN GUBERNUR SUMATERA UTARA

NOMOR 17 TAHUN 2025

TENTANG

KEBIJAKAN TATA KELOLA KEAMANAN INFORMASI DAN JARING KOMUNIKASI SANDI

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR SUMATERA UTARA,

Menimbang : a. bahwa informasi merupakan data yang perlu dijaga kerahasiaan dan keamanannya;

b. bahwa dalam rangka meningkatkan komitmen, efektivitas, dan kinerja pemerintah daerah dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan Persandian untuk pengamanan informasi;

c. bahwa ketentuan Pasal 8 Peraturan Kepala Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, menyatakan aturan mengenai tata kelola keamanan informasi ditetapkan oleh Gubernur sesuai dengan kewenangannya;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c perlu menetapkan Peraturan Gubernur tentang Kebijakan Tata Kelola Keamanan Informasi dan Jaring Komunikasi Sandi;

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

2. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-

Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);

3. Undang-Undang Nomor 8 Tahun 2023 tentang Provinsi Sumatera Utara (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 55, Tambahan Lembaran Negara Republik Indonesia Nomor 6864);
4. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);

MEMUTUSKAN :

Menetapkan : PERATURAN GUBERNUR TENTANG KEBIJAKAN TATA KELOLA KEAMANAN INFORMASI DAN JARING KOMUNIKASI SANDI.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Daerah adalah Provinsi Sumatera Utara.
2. Pemerintahan Daerah adalah penyelenggaraan urusan pemerintahan oleh Pemerintahan Daerah dan Dewan Perwakilan Rakyat Daerah menurut asas otonomi dan tugas pembantuan dengan prinsip otonomi seluas luasnya dalam sistem dan prinsip Negara Kesatuan Republik Indonesia sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
3. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
4. Gubernur adalah Gubernur Sumatera Utara.

5. Perangkat Daerah adalah unsur pembantu Gubernur dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
6. Kabupaten/Kota adalah kabupaten/kota di wilayah Sumatera Utara.
7. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Sumatera Utara.
8. Dinas Komunikasi dan informatika yang selanjutnya disebut Dinas adalah Perangkat Daerah yang mempunyai tugas pokok dan fungsi dalam penyelenggaraan Komunikasi dan Informatika.
9. Kepala Dinas adalah Kepala Dinas Komunikasi dan informatika.
10. 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.
11. Materiil Sandi 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.
12. Jaring Komunikasi Sandi yang selanjutnya disebut JKS adalah keterhubungan antar pengguna persandian melalui jaring telekomunikasi.
13. 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 nonelektronik.
14. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.
15. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.

16. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan,mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
17. 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.
18. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
19. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
20. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang 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 Daerah.

Pasal 3

Peraturan Gubernur ini bertujuan:

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 Peraturan Gubernur ini meliputi:

a. perencanaan;
b. pelaksanaan;
c. forum komunikasi Persandian Daerah;
d. pemantauan, evaluasi dan pelaporan;
e. pembinaan dan pengawasan teknis Kabupaten/Kota; dan
f. pendanaan.

BAB II

PERENCANAAN

Pasal 5

(1) Perencanaan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah 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 (RPJMD).

(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;
   c. penyelenggaraan Sertifikat Elektronik di lingkungan Pemerintah Daerah untuk mendukung Sistem Pemerintahan Berbasis Elektronik.

(2) Pelaksanaan persandian untuk pengamanan infomasi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Gubernur melalui :
   a. penguatan kapasitas kelembagaan, SDM dan sarana prasarana;
   b. mengoordinasikan kegiatan antar Perangkat Daerah; dan
   c. kerja sama dengan Kabupaten/Kota, provinsi lain, dan/atau Kabupaten/Kota dari 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 JKS 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 Nonelektronik; 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 Standar Operasional Prosedur 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 oleh Kepala Dinas 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) Standar Operasional Prosedur tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 10 huruf c ditetapkan oleh Kepala Dinas.
(2) Standar Operasional Prosedur 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;
h. keamanan komunikasi.
i. keamanan perangkat teknologi informasi komunikasi;
j. keamanan pusat data;
k. keamanan perangkat *end point*;
l. keamanan *remote working;*
m. keamanan penyimpanan elektronik;
n. pengendalian keamanan dari ancaman virus dan *malware*;
o. persyaratan keamanan terkait pembangunan dan pengembangan aplikasi;
p. pengelolaan aset;
q. keamanan migrasi data;
r. konfigurasi perangkat *IT Security*;
s. pelindungan data pribadi;
t. keamanan komunikasi;
u. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
v. pengendalian keamanan informasi terhadap pihak ketiga;
w. penerapan kriptografi;
x. penanganan insiden keamanan informasi;
y. kelangsungan bisnis atau layanan TIK (*business continuity*);
z. perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plans)*;
aa. audit internal keamanan informasi; dan/atau
bb. aspek prosedur pengendalian keamanan informasi lainnya.

(3) Penyusunan Standar Operasional Prosedur 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 9 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 berdasarkan ketentuan peraturan perundang-undangan.

(3) Aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk:
   a. mengidentifikasi;
   b. mendeteksi;
   c. memproteksi;
   d. menganalisis;
   e. menanggulangi, dan/atau
   f. 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.

(3) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

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 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.

Pasal 18

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf c dilakukan oleh Dinas.
(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 (2) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi Pemerintah Daerah.
(5) Dalam pelaksanaan manajemen pengetahuan, Dinas berkoordinasi dan berkonsultasi dengan BSSN.

Paragraf 4

Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Pasal 19

Pengamanan Sistem Elektronik dan pengamanan informasi nonelektronik 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.

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 nonelektronik sebagaimana dimaksud dalam Pasal 19 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.
(2) Pengamanan Informasi nonelektronik sebagaimana dimaksud pada ayat (1) dilaksanakan berdasarkan 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. Kepala Daerah dan Wakil Kepala Daerah;
    b. Perangkat Daerah;
    c. ASN; dan
    d. pihak lainnya.

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 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 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 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 JKS internal Pemerintah Daerah.

(3) JKS 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) JKS antar perangkat daerah sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh perangkat daerah.

(5) JKS internal perangkat daerah sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar Pengguna Layanan di lingkup internal perangkat daerah.

(6) JKS 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 (2) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2).

(4) Pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 9 huruf c dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.

(5) Pengamanan Informasi nonelektronik sebagaimana dimaksud dalam Pasal 9 huruf c dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

(6) 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, infrastruktur komunikasi, serta fasilitasi lainnya yang dibutuhkan; dan
   d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.

(7) Hasil analisis pola hubungan komunikasi sandi ditetapkan sebagai pola hubungan komunikasi sandi antar perangkat daerah Provinsi yang ditetapkan dengan Keputusan Gubernur.

(8) Keputusan sebagaimana dimaksud pada ayat (7) 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.

(9) Salinan Keputusan Gubernur sebagaimana dimaksud pada ayat (7) disampaikan 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 JKS yang efektif, efisien dan komprehensif di lingkungan Pemerintah Daerah, dibentuk Forum Komunikasi Sandi Daerah.

(2) Forum Komunikasi Sandi sebagaimana dimaksud pada ayat (1) terdiri dari:
   a. Perangkat Daerah;
   b. Pemerintah Kabupaten/Kota;
   c. Instansi vertikal di Daerah ; dan
   d. Badan Usaha Milik Negara/Daerah yang memiliki tugas pokok dan fungsi pengelola persandian dan keamanan informasi daerah.

(3) Forum Komunikasi Sandi Daerah sebagaimana dimaksud pada ayat (1) membahas isu operasional, strategis, atau kebijakan yang memengaruhi anggota dan keseluruhan fungsi organisasi.

(4) 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 penetepan 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 BSSN sebagai pembina tunggal persandian negara dengan tembusan kepada Menteri Dalam Negeri.

(4) Dalam melaksanakan 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 provinsi dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI

PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 34

Gubernur sebagai wakil Pemerintah Pusat melaksanakan pembinaan dan pengawasan teknis terhadap penyelenggaraan persandian untuk Pengamanan Informasi Pemerintah Daerah Kabupaten/Kota dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah Kabupaten/Kota.

Pasal 35

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah Kabupaten/Kota dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah Kabupaten/Kota dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 36

(1) Dalam melaksanakan pembinaan dan pengawasan teknis sebagaimana dimaksud dalam Pasal 34 Gubernur 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 VII

PENDANAAN

Pasal 37

Pendanaan pelaksanaan Peraturan Gubernur ini melalui:

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

BAB VIII

KETENTUAN PENUTUP

Pasal 38

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

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

Salinan Sesuai Dengan Aslinya
KEPALA BIRO HUKUM,

APRILLA H. SIREGAR
Pembina Utama Muda (IV/c)
NIP. 19690421 199003 2 003

Ditetapkan diMedan
pada tanggal 19 Maret 2025
GUBERNUR SUMATERA UTARA,

ttd.

MUHAMMAD BOBBY AFIF NASUTION

Diundangkan di Medan
pada tanggal 21 Maret 2025
Pj. SEKRETARIS DAERAH PROVINSI SUMATERA UTARA,

ttd.

M. A. EFFENDY POHAN

BERITA DAERAH PROVINSI SUMATERA UTARA TAHUN 2025 NOMOR 17