SALINAN

BUPATI MOROWALI UTARA
PROVINSI SULAWESI TENGAH

PERATURAN BUPATI MOROWALI UTARA
NOMOR 21 TAHUN 2023

TENTANG

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MOROWALI UTARA,

Menimbang :
a. bahwa untuk melaksanakan urusan pemerintahan bidang persandian di daerah diperlukan norma, standar, prosedur, dan kriteria;
b. bahwa setiap pemerintah daerah wajib mengelola informasi yang dimilikinya dan untuk melindungi informasi perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian;
c. bahwa berdasarkan ketentuan Pasal 4 ayat (2) Peraturan Badan Siber Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, menyatakan Bupati sesuai dengan kewenangannya bertanggung jawab terhadap Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu menetapkan Peraturan Bupati tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi Daerah;

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

2. Undang-Undang Nomor 12 Tahun 2013 tentang Pembentukan Kabupaten Morowali Utara di Provinsi Sulawesi Tengah (Lembaran Negara Republik Indonesia Tahun 2013 Nomor 83, Tambahan Lembaran Negara Republik Indonesia Nomor 5414);
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 beberapa kali diubah 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);

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DAERAH.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. 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.
2. 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.
3. 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.
4. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.

5. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
6. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan,mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
7. 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.
8. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
9. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
10. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
11. Rencana Strategis Pengamanan Informasi adalah susunan strategi yang diterapkan untuk mengurangi kelemahan dan menurunkan potensial ancaman dan risiko yang terkait dengan teknologi informasi yang berjalan, sehingga kemudian dapat dilakukan proses untuk meredakan risiko (risk mitigation), dan melakukan kontrol dan evaluasi.
12. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
13. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
14. Daerah adalah Kabupaten Morowali Utara.
15. Bupati adalah Bupati Morowali Utara.
16. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Morowali Utara.
17. Dinas Komunikasi dan Informatika Kabupaten Morowali Utara yang selanjutnya disebut Dinas adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang persandian dan keamanan siber.
18. Kepala Dinas adalah Kepala Perangkat Daerah yang mempunyai tugas pokok dan fungsi dalam penyelenggaraan Komunikasi dan Informatika.

Pasal 2

Peraturan Bupati ini dimaksudkan untuk memberikan pedoman dalam melaksanakan kebijakan, program, dan kegiatan penyelenggaraan persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah.

Pasal 3

Pelaksanaan persandian untuk Pengamanan Informasi dilingkungan Pemerintah Daerah bertujuan untuk:

a. menciptakan harmonisasi dalam pembagian urusan pemerintahan bidang Persandian;
b. memfasilitasi Pemerintah Daerah 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 Bupati ini meliputi:

a. perencanaan;
b. pelaksanaan;
c. Forum Komunikasi Persandian Daerah;
d. pemantauan, evaluasi dan pelaporan;
e. pembinaan dan pengawasan teknis kabupaten; dan

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 Bupati.

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 Pemerintah Berbasis Elektronik.

(2) Pelaksanaan Persandian untuk pengamanan infomasi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Bupati melalui :
   a. penguatan kapasitas kelembagaan, sumber daya manusia dan sarana prasarana;
   b. mengoordinasikan kegiatan antar Perangkat Daerah;
   c. kerjasama dengan kabupaten/kota dalam satu provinsi, 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, Matsan 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 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 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 Bupati 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 Bupati.
(2) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) minimal 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) Penyusunan aturan mengenai tata kelola Keamanan Informasi dilaksanakan oleh Dinas dan dikoordinasikan kepada Unit Kerja Perangkat Daerah yang membidangi urusan pemerintahan dibidang hukum.
(4) 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 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 sesuai dengan ketentuan peraturan perundang-undangan.
(3) Aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (2) 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; dan
    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 sebagai pembina dan penyelenggara persandian nasional, tetap ditugaskan secara penuh di bidang persandian dan tidak dimutasi kebidang 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 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 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) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk :
    a. Bupati dan Wakil Bupati;
    b. Perangkat Daerah; dan
    c. pegawai atau Aparatur Sipil Negara pada Pemerintah Daerah.

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 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 Bupati.
(2) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dan 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 Bupati, Wakil Bupati, 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) Pengamanan Informasi nonelektronik sebagaimana dimaksud dalam Pasal 19 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.
(5) Pengamanan Informasi nonelektronik sebagaimana dimaksud pada ayat (4) 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 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.
(7) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (6) ditetapkan sebagai pola hubungan komunikasi sandi antar Perangkat Daerah oleh Bupati dalam bentuk Keputusan Bupati.
(8) Keputusan sebagaimana dimaksud pada ayat (7) 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.

(9) Salinan keputusan sebagaimana dimaksud pada ayat (8) disampaikan kepada Gubernur sebagai wakil pemerintah pusat dan ditembuskan 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 dilingkungan Pemerintah Daerah, perlu dibentuk Forum Komunikasi Sandi Daerah.

(2) Forum Komunikasi Sandi sebagaimana dimaksud pada ayat (1) dapat beranggotakan Instansi dilingkungan Pemerintah Daerah, Pemerintah Kabupaten dan Instansi vertikal di Daerah serta Badan Usaha Milik Daerah yang memiliki tugas pokok dan fungsi pengelola persandian dan Keamanan Informasi Daerah.
(3) Forum Komunikasi Sandi sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Bupati.

BAB V
PEMANTAUAN, EVALUASI, DAN PELAPORAN
Pasal 32

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penatepan 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 Bupati.
(3) Bupati menyampaikan laporan pelaksanaan penyelenggaraan sebagaimana dimaksud pada ayat (1) Kepada Gubernur sebagai wakil pemerintah pusat dan Kepala BSSN sebagai pembina tunggal persandian negara dengan tembusan kepada Menteri Dalam Negeri.
(4) Guna kelancaran pelaksanaan tugas sebagaimana dimaksud pada ayat (1) Bupati 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
PEMBINAAN DAN PENGAWASAN TEKNIS KABUPATEN
Pasal 34

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

Pasal 35

(1) Dalam melaksanakan pembinaan dan pengawasan teknis sebagaimana dimaksud dalam Pasal 34 Bupati 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 VIII
KETENTUAN PENUTUP
Pasal 36

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Morowali Utara.

Ditetapkan di Kolonodale
pada tanggal 29 Desember 2023

BUPATI MOROWALI UTARA,

t t d

DELIS JULKARSON HEHI

Diundangkan di Kolonodale
pada tanggal 29 Desember 2023

SEKRETARIS DAERAH
KABUPATEN MOROWALI UTARA,

t t d

MUSDA GUNTUR

BERITA DAERAH KABUPATEN MOROWALI UTARA TAHUN 2023 NOMOR 21

Salinan sesuai dengan aslinya :
Kepala Bagian Hukum Setda
Kabupaten Morowali Utara,

PEMERINTAH KABUPATEN MOROWALI UTARA
SETDA

BETSI A. POMBALAWO, SH
NIP.19780121 200604 2 027