SALINAN

BUPATI LUWU UTARA
PROVINSI SULAWESI SELATAN

PERATURAN BUPATI LUWU UTARA
NOMOR 9 TAHUN 2022

TENTANG

PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DILINGKUNGAN PEMERINTAH KABUPATEN LUWU UTARA

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI LUWU UTARA,

Menimbang : a. bahwa Pemerintah Daerah dalam mengelola informasi publik yang dimiliki wajib melindungi dari penggunaan yang tidak semestinya;

b. Bahwa untuk melindungi informasi publik perlu dilakukan upaya pengamanan melalui pelaksanaan persandian untuk pengamanan informasi yang diatur dengan peraturan Bupati;

c. Bahwa pelaksanaan persandian untuk pengamanan informasi di Pemerintah Daerah berdasarkan ketentuan Pasal 3 Peraturan Badan Siber Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah;

d. Bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b dan huruf c, perlu menetapkan Peraturan Bupati tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Kabupaten Luwu Utara;

Mengingat : 1. Undang-Undang Nomor 13 Tahun 1999 tentang Pembentukan Kabupaten Daerah Tingkat II Luwu Utara (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 47, Tambahan Lembaran Negara Republik Indonesia Nomor 3826);

2. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154 Tambahan Lembaran Negara Republik Indonesia Nomor 3881);

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 diubah beberapa kali, terakhir dengan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Tahun Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
5. 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);
6. Peraturan Pemerintah Nomor18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 114, Tambahan Lembaran Negara Republik Indonesia Nomor 5887);
7. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185);
8. Peraturan Badan Siber dan Sandi Negara Nomor 10 tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
9. Peraturan Menteri Dalam Negeri Nomor 90 Tahun 2019 tentang Klasifikasi, Kodefikasi, dan Nomenklatur Perencanaan Pembangunan dan Keuangan Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1447)
10. Peraturan Kepala Lembaga Sandi Negara Nomor 14 Tahun 2010 tentang Pedoman Gelar Jaring Komunkasi Sandi (Berita Negara Republika Indonesia Tahun 2010 Nomor 14);
11. PeraturanKepala Lembaga Sandi Negara Nomor 10 Tahun 2012 tentang Pedoman Pengelolaan dan Perlindungan Informasi Berklasifikasi Milik Pemerintah (Berita Negara Republik Indonesia Tahun 2012 Nomor 808);
12. Peraturan Daerah Kabupaten Luwu Utara Nomor 13 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Luwu Utara Tahun 2016 Nomor 13);

13. Peraturan Bupati Luwu Utara Nomor 30 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta Tata Kerja pada Dinas Komunikasi, Informatika, Statistik dan Persandian Kabupaten Luwu Utara;

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI LUWU UTARA TENTANG PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DILINGKUNGAN PEMERINTAH KABUPATEN LUWU UTARA.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Daerah Kabupaten Luwu Utara;
2. Pemerintah Daerah adalah Kepala Daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom;
3. Gubernur adalah Gubernur Sulawesi Selatan
4. Bupati adalah Bupati Luwu Utara;
5. Dinas Komunikasi, Informatika, Statistik dan Persandian Kabupaten Luwu Utara selanjutnya disebut Dinas adalah unsur pembantu Kepala Daerah dalam penyelenggaraan urusan pemerintahan bidang persandian, keamanan informasi, keamanan siber;
6. Persandian adalah kegiatan dibidang 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.
7. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.
8. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.

9. Keamanan Siber adalah praktik untuk melindungi sistem, jaringan, dan program dari serangan digital.
10. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
11. Sertifikat Elektronik adalah sertifikat yangbersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik.
12. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
13. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
14. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan dibidang Persandian, Keamanan Informasi dan Keamanan siber.
15. Urusan Pemerintahan adalah kekuasaan pemerintahan yang menjadi kewenangan Presiden yang pelaksanaannya dilakukan oleh kementerian negara dan penyelenggara pemerintahan daerah untuk melindungi, melayani, memberdayakan, dan menyejahterakan masyarakat
16. Jaring Komunikasi Sandi yang selanjutnya disingkat JKS adalah keterhubungan antar Pengguna Persandian melalui Jaring telekomunikasi yang memanfaatkan persandian dalam komunikasi.

Pasal 2

Peraturan Bupati ini dimaksudkan untuk memberikan pedoman bagi perangkat daerah dalam melaksanakan persandian sebagai pengamanan informasi.

Pasal 3

Pelaksanaan bpersandian untuk pengamanan informasi di lingkungan pemerintah daerah bertujuan untuk:

a. Menciptakan harmonisasi dalam melaksanakan Persandian untuk pengamanan informasi di Pemerintah Daerah;
b. Meningkatkan komitmen, efektivitas, dan kinerja dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan Persandian untuk pengamanan informasi;
c. Memberikan pedoman dalam menetapkan pola hubungan komunikasi sandi antar perangkat daerah; dan
d. Meningkatkan kinerja dan efektivitas Dinas.

Pasal 4

Pelaksanaan persandian untuk pengamanan informasi pemerintah daerah sebagaimana dimaksud dalam Pasal 3 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

(1) 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 (SPBE) dan pengamanan informasi non-elektronik; dan
    d. Penyediaan layanan Keamanan Informasi.

(2) Kepala Daerah bertanggungjawab terhadap Penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) sesuai dengan kewenangannya dibantu oleh Dinas.

(3) Dinas bertanggungjawab atas kinerja pelaksanaan tugas dan fungsi urusan pemerintahan bidang

Persandian.

Bagian Kedua

Penyusunan Kebijakan Pengamanan Informasi

Pasal 6

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf a meliputi:

a. Rencana strategis pengamanan informasi;
b. Arsitektur keamanan informasi; dan
c. Aturan mengenai tata kelola keamanan informasi.

Pasal 7

(1) Rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 6 huruf a disusun oleh Pemerintah Daerah 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) terdiriatas:
   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 yang telah disusun sebagaimana dimaksud pada ayat (1) diintegrasikan kedalam Rencana Pembangunan Jangka Menengah Daerah.

(5) Dalam melakukan penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) Kepala Daerah dapat melakukan koordinasi dan konsultasi kepada BSSN.

(6) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (5) Bupati dapat menunjuk Kepala Dinas.

Pasal 8

(1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 huruf b ditetapkan oleh Bupati.

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

(3) Dalam melakukan penyusunan Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) Bupati dapat melakukan koordinasi dan konsultasi kepada BSSN.

(4) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (3) Bupati dapat menunjuk Kepala Dinas.

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

(6) Bupati melakukan evaluasi terhadap Arsitektur Keamanan Informasi pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu waktu sesuai dengan kebutuhan.

Pasal 9

(1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 huruf c ditetapkan oleh Bupati.

(2) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) paling sedikit terdiri atas:
   a. Keamanan sumberdaya teknologi informasi;
   b. Keamanan fisik dan akses kontrol;
   c. Keamanan data dan informasi;
   d. Keamanan sumber daya manusia;
   e. Keamanan jaringan dan telekomunikasi;
   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) Bupati dapat melakukan koordinasi dan konsultasi kepada BSSN.

(4) Dalam melakukan koordinasi dan konsultasi

sebagaimana dimaksud pada ayat (3) Bupati dapat menunjuk Kepala Dinas.

Bagian Ketiga

Pengelolaan Sumber Daya Keamanan Informasi

Pasal 10

(1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf b dilaksanakan oleh Dinas.

(2) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1)terdiri atas:
   a. Pengelolaan asset keamanan teknologi informasi dan komunikasi;
   b. Pengelolaan sumber daya manusia; dan
   c. Manajemen pengetahuan.

Pasal 11

(1) Pengelolaan asset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap asset 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 Dinas.

(2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses sebagai berikut:
   a. Perencanaan kebutuhan;
   b. Pengembangan kompetensi;
   c. Pembinaan karir;
   d. Pendayagunaan; dan

e. Pemberian Tunjangan Pengamanan Persandian/Kompensasi

Pasal 13

Perencanaan kebutuhan sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf a disusun dengan ketentuan:

(1) Memperhatikan kebutuhan jumlah dan kompetensi sesuai dengan hasil analisis beban kerja dan analisis formasi jabatan;
(2) Memperhatikan standard kompetensi sesuai dengan yang ditetapkan oleh Kementerian/Lembaga penyelenggara Urusan Pemerintahan bidang Kepegawaian; dan
(3) Mengusulkan kebutuhan sumber daya manusia kepada perangkat daerah penyelenggara Urusan Pemerintahan bidang Kepegawaian.

Pasal 14

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf b 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 yang terakreditasi, atau pemerintah daerah lainnya;
    c. Memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi bidangnya.
(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf c dilaksanakan dengan ketentuan:
    a. Pembinaan jabatan fungsional dibidang Keamanan Informasi; dan
    b. Pengisian formasi jabatan pimpinan tinggi, jabatan administrator, jabatan pengawas dan/atau jabatan fungsional sesuai dengan standard kompetensi yang ditetapkan.
(3) Pendayagunaan sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf d dilaksanakan agar seluruh sumber daya manusia yang bertugas dibidang Keamanan

Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standard kompetensi kerja pegawai yang ditetapkan.

Pasal14

(1) Pemberian tunjangan / kompensasi sebagaimana dimaksud pada Pasal 12 ayat (2) huruf e berupa:
   a. Pemberian tunjangan; dan
   b. Pengusulan pemberian tanda penghargaan bidang Persandian.
(2) Tunjangan sebagaimana dimaksud pada ayat (1) meliputi tunjangan pengamanan Persandian dan tunjangan jabatan fungsional Sandiman.
(3) Kompensasi sebagaimana dimaksud pada ayat (1) diberikan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal15

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf c dilakukan oleh Perangkat Daerah.
(2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusanterkait 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, *Pemerintah Daerah* berkoordinasi dan dapat melakukan konsultasi dengan BSSN.
(6) Ketentuan lebih lanjut mengenai pedoman manajemen pengetahuan Keamanan Informasi pemerintah daerah diatur dengan Peraturan Bupati.

Bagian Keempat

Pengamanan Sistem Elektronik dan
Pengamanan Informasi Nonelektronik

Pasal16

Pengamanan Sistem Elektronik dan pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf c dilaksanakan oleh Perangkat Daerah sesuai dengan ketentuan peraturan perundang-undangan.

Paragraf 1

Pengamanan Sistem Elektronik

Pasal 17

Pelaksanaan pengamanan Sistem Pemerintahan Berbasis Elektronik dan pengamanan informasi nonelektronik sebagaimana dimaksud dalamPasal 16 mencakup perlindungan informasi yang meliputi:

a. Penentuan tingkat klasifikasi informasi di perangkat daerah lingkup Pemerintah Daerah;
b. Penyelenggaraan Jaring Komunikasi Sandi atau penerapan Jaring privat maya (*virtual private network*) untuk pengiriman informasi dalam system pemerintahan berbasis elektronik di perangkat daerah.

Pasal 18

(1) Tingkat klasifikasi informasi di perangkat derah lingkup Pemerintah Daerah meliputi:
    a. Rahasia/yang dikecualikan;
    b. Terbatas/internal; dan
    c. Biasa/terbuka/publik.
(2) Penentuan tingkat klasifikasi informasi dilakukan oleh Pemilik Informasi atau pejabat yang berwenang.
(3) Informasi yang klasifikasinya telah disahka nsebagaimana dimaksud pada ayat (1) harus diberitahukan kepada Pejabat Pengelola Informasi dan Dokumentasi (PPID) Pembantu dan Utama untuk dikelola sesuai dengan peraturan perundang-undangan.
(4) Informasi yang klasifikasinya telah disahkan sebagaimana dimaksud pada ayat (1) harus diperlakukan sama sesuai dengan tingkat klasifikasinya oleh perangkat daerah lainnya.

Pasal19

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 16 terdiri atas:

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

Pasal 20

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalamPasal 16 Perangkat Daerah 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, implementasi metode enkripsi, 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 21

(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 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 atasinsiden keamanan Sistem Elektronik dengan memperhatikan aspek personel, proses pelaksanaan, dan ketersediaan teknologi.

Paragraf 2

Pengamanan Informasi Nonelektronik

Pasal 23

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

(2) Pemrosesan informasi nonelektronik meliputi keamanan pembuatan dan pemberian label tingkat klasifikasi.

(3) Pengiriman informasi nonelektronik yang berisiinformasi dengan tingkat klasifikasi informasi sebagaimana dimaksud pada pasal 18 ayat (1) huruf a dan b harus dibuatkan tanda bukti pengiriman tersendiri dan dicatat di buku ekspedisi atau agenda khusus.

(4) Penyimpanan informasi nonelektronik yang berisiinformasi dengan tingkat klasifikasi informasi sebagaimana dimaksud pada pasal 18 ayat (1) huruf a dan b harus diterapkan pengamanan fisik berlapis.

(5) Pemusnahan informasi nonelektronik dilaksanakan

sesuai dengan ketentuan peraturanperundang-undangan.

(6) 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 system manajemen.

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

Bagian Kelima

Penyediaan Layanan Keamanan Informasi

Pasal 25

(1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) hurufd dilaksanakan oleh Perangkat Daerah.

(2) Layanan Keamanan Informasi sebagaimana dimaksud pad aayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:

a. Bupati danWakil Bupati;
b. Perangkat Daerah;
c. Pegawai atau aparatur sipil Negara pada pemerintah daerah; 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 Jaring komunikasi sandi;

e. Fasilitasi sertifikasi penerapan manajemen pengamanan Sistem Elektronik;
f. Audit Keamanan Sistem Elektronik;
g. Audit keamanan pelaksanaan system manajemen atau penyelenggaraan Persandian sebagai Pengamanan Informasi;
h. Literasi Keamanan Informasi dalam rangka peningkatan kesadaran Keamanan Informasi dan pengukuran tingkat kesadaran Keamanan Informasi dilingkungan pemerintah daerah dan Publik;
i. Peningkatan kompetensi sumber daya manusia dibidang Keamanan Informasi dan/atau persandian;
j. Pengelolaan pusat operasi Pengamanan Informasi;
k. Penanganan insiden Keamanan Sistem Elektronik;
l. Forensic 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 Informasise bagaimana dimaksud dalamPasal 22 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 manajeme nLayanan Keamanan Informasi.

BAB III

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Pasal 28

(1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah sebagaimana dimaksudd alam Pasal 4 huruf b ditetapkan Bupati.
(2) Penetapan pola hubungan komunikasi sandi antar perangkat daerah sebagaimana dimaksud pada ayat (1) untuk menentukan Jaring komunikasis andi 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 dilingkup 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.
(7) Jaring komunikasi sandi dalam pelaksanaan pola hubungan komunikasi sandi dapat dilakukan kerjasama dengan Kementerian/Lembaga yang menyelenggarakan tugas pemerintahan di bidang Persandian dan Keamanan Informasi serta antar Pemerintah Daerah Provinsi/Kabupaten/Kota.
(8) Penyelenggaraan operasionalisasi Jaring komunikasi sandi dapat berkoordinasi dengan BSSN.

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, fungsional internal pemerintah daerah;
   b. Alurinformasi yang dikomunikasikan antar perangkat daerah dan internal perangkat daerah;
   c. Teknologi informasi dan komunikasi;
   d. Infrastruktur komunikasi; dan
   e. Kompetensi personil.

(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 Jaring komunikasi sandi;
   b. Topologi atau bentuk atau model keterhubungan Jaring komunikasi sandi antar pengguna layanan;
   c. Perangkat keamanan teknologi Informasi dan komunikasi, dan infrastruktur komunikasi, sertafasilitas lainnya yang dibutuhkan; dan
   d. Tugas dan tanggungjawab pengelola dan pengguna layanan.

(5) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (5) ditetapkan dengan keputusan Bupati sebagai pola hubungan komunikasi sandi antar perangkat daerah.

(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 (6) disampaikan kepada Gubernur sebagai wakil Pemerintah Pusat dan ditembuskan kepada Kepala BSSN.

BAB IV

PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 30

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi pemerintah daerah dan penetapan pola hubungan komunikasi sandi antar perangkat daerah.
(2) Dinas melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali.
(3) Dinas menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) kepada Bupati dan Gubernur sebagai wakil Pemerintah Pusat.

Pasal 31

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 32

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 dan ketentuan peraturan perundang-undangan.

Pasal 33

(1) Dalam melaksanakan pembinaan dan pengawasan teknis sebagaimana dimaksud dalam Pasal 32 BSSN dan pemerintah daerah provinsi sesuai dengan kewenangannya menyelenggarakan rapat koordinasi urusan Persandian.
(2) Rapat koordinasi sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam setahun.
(3) Dinas berkewajiban untuk mengikuti rapat koordinasi sebagaimana dimaksud pada ayat (1) dan ayat (2).

BAB VI

PENDANAAN

Pasal 34

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 dan/atau
b. Sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII

KETENTUAN PENUTUP

Pasal 35

Peraturan ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Masamba
pada tanggal, 18 Januari 2022

BUPATI LUWU UTARA,

ttd

INDAH PUTRI INDRIANI

Diundangkan di Masamba
pada tanggal, 18 Januari 2022

SEKRETARIS DAERAH KABUPATEN LUWU UTARA,

ttd

ARMIADI

BERITA DAERAH KABUPATEN LUWU UTARA TAHUN 2022 NOMOR 9