



BUPATI MOROWALI
PROVINSI SULAWESI TENGAH

PERATURAN BUPATI MOROWALI
NOMOR 28 TAHUN 2024

TENTANG
PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN
INFORMASI DI DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MOROWALI,

- Menimbang : a. bahwa dalam rangka melindungi informasi perlu dilakukan upaya pengamanan melalui penyelenggaraan persandian untuk pengamanan informasi di lingkungan pemerintah daerah;
- b. bahwa untuk mewujudkan pelaksanaan persandian secara aman dan mencegah penyalahgunaan informasi di daerah diperlukan suatu pedoman pelaksanaan;
- c. bahwa berdasarkan ketentuan Pasal 27 dan Pasal 28 Peraturan Daerah Nomor 14 Tahun 2022 tentang Penyelenggaraan Komunikasi, Informatika, Statistik dan Persandian, yang 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 Pelaksanaan Persandian untuk Pengamanan Informasi di Daerah;
- Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 51 Tahun 1999 tentang Pembentukan Kabupaten Buol, Kabupaten Morowali dan Kabupaten Banggai Kepulauan (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 179, Tambahan Lembaran Negara Republik Indonesia Nomor 3900) sebagaimana telah diubah dan disempurnakan dengan Undang-Undang Nomor 11 Tahun 2000 tentang Perubahan Undang-Undang Nomor 51 Tahun 1999 tentang Pembentukan Kabupaten Buol, Kabupaten Morowali dan Kabupaten Banggai Kepulauan Lembaran Negara Republik Indonesia Tahun 2000 Nomor 78, Tambahan Lembaran Negara Republik Indonesia Nomor 3966);

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 Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6865);

Menetapkan : PERATURAN BUPATI TENTANG PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI 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. Sandi adalah kode rahasia yang digunakan untuk mengakses sistem atau sebagai cara mengirim pesan rahasia.
3. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan dan kenirsangkalan informasi.
4. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
5. Arsitektur Keamanan Informasi adalah kerangka kerja untuk merencanakan dan menerapkan langkah-langkah keamanan atau perusahaan.
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. Pola Hubungan Komunikasi Sandi adalah keterhubungan antar pengguna persandian melalui jaringan komunikasi.
9. Rencana Pembangunan Jangka Menengah Daerah yang selanjutnya di singkat RPJMD adalah dokumen perencanaan pembangunan daerah yang dibuat untuk jangka waktu 5 tahun.
10. Rencana Kerja adalah suatu proses yang berorientasi pada hasil yang ingin dicapai selama kurun waktu satu tahun akan menjadi landasan operasional dalam melaksanakan tugas dan tanggung jawabnya dalam mencapai tujuan.
11. Rencana Strategis adalah dokumen perencanaan yang berisi strategi dan arahan untuk mencapai tujuan organisasi dalam jangka waktu tertentu.
12. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data serta otentifikasi data.

13. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan urusan Pemerintahan bidang Persandian dan yang memiliki manfaat.
14. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
15. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan dibidang keamanan siber dan persandian.
16. Otoritas Sertifikat Digital Badan Siber dan Sandi Negara yang selanjutnya disingkat OSD Badan Siber Sandi Negara adalah sistem elektronik yang berfungsi sebagai Layanan Sertifikat Elektronik di Badan Siber dan Sandi Negara.
17. Balai Sertifikasi Elektronik yang selanjutnya disebut BSrE merupakan unit pelaksana teknis penyelenggara OSD Badan Siber Sandi Negara yang berada di bawah dan bertanggung jawab kepada Kepala Badan Siber dan Sandi Negara.
18. Daerah adalah Kabupaten Morowali.
19. Pemerintahan Daerah adalah penyelenggara urusan pemerintah oleh pemerintah 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 Republik Indonesia Tahun 1945.
20. Pemerintah Daerah adalah Kepala Daerah sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan Pemerintah yang menjadi kewenangan daerah otonom.
21. Bupati adalah Bupati Morowali.
22. Sekretaris Daerah adalah Sekretaris Daerah kabupaten Morowali.
23. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Bupati dalam penyelenggaraan urusan Pemerintahan yang menjadi kewenangan daerah.
24. Dinas adalah Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Morowali.

Pasal 2

Maksud pembentukan Peraturan Bupati ini yakni sebagai pedoman bagi Pemerintah Daerah dalam melaksanakan kebijakan, program dan kegiatan pelaksanaan urusan pemerintahan bidang Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah.

Pasal 3

Peraturan Bupati ini bertujuan:

- a. menciptakan harmonisasi dalam melaksanakan urusan pemerintahan bidang Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah;
- b. meningkatkan komitmen, efektifitas, dan kinerja PD dalam melaksanakan program dan kegiatan pelaksanaan Persandian untuk Pengamanan Informasi; dan

- c. memberikan pedoman bagi Pemerintah Daerah dalam menetapkan Pola Hubungan Komunikasi Sandi antar PD.

BAB II

PENYELENGGARAAN

PERSANDIAN DAERAH

Bagian Kesatu

Umum

Pasal 4

Penyelenggaraan Persandian Daerah untuk Pengamanan Informasi di lingkungan Pemerintah Daerah, meliputi:

- a. penyusunan kebijakan Pengamanan Informasi;
- b. pengelolaan sumber daya Keamanan Informasi;
- c. pengamanan Sistem Elektronik dan Pengamanan Informasi nonelektronik;
- d. penyedia Layanan Keamanan Informasi;
- e. penyediaan kebutuhan penyelenggaraan Persandian untuk Pengamanan Informasi melalui identifikasi dan analisis pola hubungan komunikasi Persandian;
- f. penyelenggaraan operasional dukungan Persandian untuk Pengamanan Informasi;
- g. pemanfaatan layanan Sertifikat Elektronik;
- h. pengawasan dan evaluasi penyelenggaraan Pengamanan Informasi melalui Persandian di seluruh PD; dan
- i. koordinasi dan konsultasi penyelenggaraan Persandian untuk Pengamanan Informasi.

Pasal 5

Penyelenggaraan urusan pemerintahan bidang Persandian dilaksanakan oleh Bupati melalui Dinas.

Pasal 6

- (1) Bupati memimpin dan bertanggung jawab atas penyelenggaraan urusan Persandian yang menjadi kewenangan Daerah yang dilaksanakan sebagaimana dimaksud dalam Pasal 5.
- (2) Dinas melalui Bidang Teknologi Informasi, Persandian, dan Statistik bertanggung jawab atas kinerja pelaksanaan urusan pemerintahan bidang Persandian sesuai tugas dan fungsinya.

Pasal 7

- (1) Dinas menyusun perencanaan penyelenggaraan Persandian sesuai dengan tugas dan fungsinya.
- (2) Perencanaan penyelenggaraan Persandian sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam perencanaan pembangunan Daerah.
- (3) Perencanaan pembangunan Daerah sebagaimana dimaksud pada ayat (2) merupakan bagian integral dari sistem perencanaan pembangunan nasional dan dituangkan dalam dokumen Perencanaan Pembangunan Daerah.
- (4) Dokumen perencanaan pembangunan Daerah sebagaimana dimaksud pada ayat (3) berupa:
 - a. Rencana Pembangunan Jangka Panjang Daerah;

- b. Rencana Pembangunan Jangka Menengah Daerah; dan
- c. Rencana Kerja Pemerintah Daerah.

Pasal 8

- (1) Dalam rangka menjabarkan Rencana Pembangunan Jangka Menengah Daerah sebagaimana dimaksud dalam Pasal 7 ayat (4) huruf b, Dinas menyusun Rencana Strategis Dinas yang memuat tujuan, sasaran, program dan kegiatan penyelenggaraan Persandian untuk Keamanan Informasi di lingkungan Pemerintah Daerah.
- (2) Dalam rangka menjabarkan rencana kerja Pemerintah Daerah sebagaimana dimaksud dalam Pasal 7 ayat (4) huruf c, Dinas menyusun rencana kerja yang memuat program, kegiatan, lokasi dan kelompok sasaran berdasarkan layanan urusan pemerintah bidang Persandian, disertai indikator kinerja program dan kegiatan, serta penganggaran penyelenggaraan Persandian untuk Keamanan Informasi di Lingkungan pemerintah Daerah.

Bagian Kedua

Penyusunan Kebijakan Pengamanan Informasi

Pasal 9

Penyusunan Kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 4 huruf a, dilakukan dengan:

- a. menyusun Rencana Strategis Keamanan Informasi;
- b. menetapkan Arsitektur Keamanan Informasi; dan
- c. menetapkan aturan mengenai tata kelola Keamanan Informasi

Pasal 10

- (1) Rencana Strategis Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf a, disusun oleh Bupati melalui Dinas.
- (2) Dalam melakukan penyusunan Rencana Strategis sebagaimana dimaksud pada ayat (1), Bupati melalui Dinas dapat melakukan koordinasi dan konsultasi dengan BSSN dan/atau kementerian/lembaga lainnya.

Pasal 11

- (1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf b, ditetapkan oleh Bupati.
- (2) Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) memuat:
 - a. infrastruktur teknologi informasi; dan
 - b. desain keamanan perangkat teknologi informasi dan keamanan jaringan;
- (3) Dalam melakukan penyusunan Arsitektur Keamanan Informasi, Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN dan/atau kementerian/lembaga lainnya.
- (4) Arsitektur Keamanan Informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.

- (5) Bupati dapat melakukan evaluasi pelaksanaan Arsitektur Keamanan Informasi.

Pasal 12

- (1) Aturan mengenai tata kelola Keamanan Informasi dalam Pasal 9 huruf c ditetapkan oleh Bupati.
- (2) 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.
- (3) Dalam melakukan penyusunan aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN dan/atau kementerian/lembaga lainnya.

Bagian Ketiga Pengelolaan Sumber Daya Keamanan Informasi Pasal 13

- (1) Dinas harus melakukan pengelolaan sumber daya Keamanan Informasi.
- (2) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1), terdiri dari:
 - a. pengelolaan aset keamanan teknologi informasi dan komunikasi;
 - b. pengelolaan sumber daya manusia; dan
 - c. manajemen pengetahuan.

Pasal 14

- (1) Pengelolaan aset keamanan teknologi informasi dan komunikasi dilaksanakan oleh Pemerintah Daerah, melalui:
 - a. perencanaan kebutuhan;
 - b. pengadaan;
 - c. pemanfaatan dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan; dan
 - d. pengawasan dan pengendalian.
- (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 15

- (1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf b dilakukan oleh PD.
- (2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1), dapat dilakukan melalui serangkaian proses sebagai berikut:
 - a. pengembangan kompetensi;
 - b. pembinaan karir; dan
 - c. pendayagunaan.

- (3) Pengembangan kompetensi sebagaimana dimaksud pada ayat (2) huruf a dapat dilakukan, melalui:
 - 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; dan
 - c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi bidangnya.
- (4) Pembinaan karir sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan dengan ketentuan:
 - a. pembinaan jabatan fungsional di bidang keamanan informasi, dan
 - b. pengisian jabatan struktural sesuai standar kompetensi yang ditetapkan.
- (5) Pendayagunaan sebagaimana yang dimaksud pada ayat (2) huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di bidang keamanan Informasi dapat bekerja sesuai dengan standar kompetensi pegawai yang ditetapkan.

Pasal 16

- (1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 15 ayat (1), dilakukan melalui:
 - a. pendidikan dan pelatihan jabatan fungsional;
 - b. pendidikan dan pelatihan teknis sandi;
 - c. bimbingan teknis; dan
 - d. kegiatan pengembangan kompetensi lain yang terkait dengan Persandian dan teknologi informasi serta bidang ilmu lainnya yang dibutuhkan.
- (2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) merupakan pengembangan sumber daya manusia yang terkait dengan ilmu Persandian dan teknologi informasi serta bidang ilmu lainnya yang dibutuhkan.

Pasal 17

Sumber daya manusia yang sudah tidak melaksanakan tugas pada Dinas harus disesuaikan kewenangannya, yaitu:

- a. pencabutan atau pemutusan hak akses terhadap informasi dan fasilitas informasi yang diamankan; dan
- b. pelaksanaan prosedur pengamanan materiil Sandi melalui berita acara serah terima.

Pasal 18

- (1) Manajemen pengetahuan pada Pasal 13 ayat (2) huruf c dilakukan oleh Dinas 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) Dalam pelaksanaan manajemen pengetahuan, Pemerintah Daerah dapat melakukan koordinasi dan konsultasi kepada BSSN dan/atau kementerian/lembaga lainnya.

Bagian Keempat

Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Pasal 19

Pengamanan Sistem Elektronik dan Pengamanan Informasi nonelektronik sebagaimana dimaksud dalam Pasal 4 huruf c, dilaksanakan oleh Dinas sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 20

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 19, terdiri atas:

- a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirangkal 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 melalui kegiatan mitigasi risiko dan penerapan perlindungan terhadap Sistem Elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintahan berbasis elektronik.
- (5) Penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (1) huruf d, dilakukan dengan kegiatan penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Pasal 22

- (1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 19, PD 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 23

- (1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 22 ayat (1), Dinas pelaksana urusan pemerintahan bidang persandian 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 24

- (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 25

- (1) Dinas melaksanakan audit Keamanan Informasi di lingkup Pemerintah Daerah.
- (2) Perangkat Daerah Wajib mendukung dalam pelaksanaan kegiatan audit Keamanan Informasi di wilayah kerjanya.
- (3) Audit Keamanan Informasi meliputi audit keamanan Sistem Elektronik dan audit Sistem Manajemen.
- (4) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (3), dilaksanakan sesuai ketentuan peraturan perundang-undangan.

Bagian Kelima

Penyediaan Layanan Keamanan Informasi

Pasal 26

- (1) Penyedia Layanan Keamanan informasi sebagaimana dimaksud dalam Pasal 4 huruf d, dilaksanakan oleh Dinas.
- (2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1), disediakan untuk Pengguna Layanan yang terdiri atas:
 - a. Bupati dan Wakil Bupati;
 - b. PD;
 - c. aparatur sipil negara pada Pemerintah Daerah; dan
 - d. pihak lainnya

Pasal 27

Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 26 ayat (2), meliputi:

- a. identifikasi kerentanan dan penilaian risiko terhadap Sistem Elektronik;
- b. asistensi dan fasilitasi penguatan keamanan Sistem Elektronik;
- c. penerapan Sertifikasi 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 masyarakat;
- 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. 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 28

- (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 Layanan Keamanan Informasi.
- (3) Manajemen Keamanan Informasi sebagaimana dimaksud pada ayat (1), merupakan penanganan terhadap keluhan, gangguan, masalah, permintaan, dan/atau perubahan Layanan Keamanan Informasi dari Pengguna Layanan Keamanan Informasi.
- (4) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (3), dilaksanakan berdasarkan manajemen Layanan Keamanan Informasi.
- (5) Dalam melaksanakan Layanan Keamanan Informasi sebagaimana yang dimaksud pada ayat 1, Dinas berkoordinasi dan berkonsultasi kepada BSSN dan/atau kementerian/ lembaga lainnya.

BAB III

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI

Pasal 29

- (1) Penetapan Pola Hubungan Komunikasi Sandi antar PD ditetapkan oleh Bupati.
- (2) Penetapan Pola Hubungan Komunikasi Sandi antar PD sebagaimana dimaksud pada ayat (1), untuk menentukan jaring komunikasi internal Pemerintah Daerah.
- (3) Untuk jaring komunikasi sandi di lingkungan Pemerintah Daerah mengacu pada peraturan perundang-undangan.

Pasal 30

Penetapan Pola Hubungan Komunikasi Sandi sebagaimana dimaksud dalam Pasal 29, dilaksanakan melalui:

- a. identifikasi Pola Hubungan Komunikasi Sandi; dan
- b. analisis Pola Hubungan Komunikasi Sandi.

Pasal 31

Identifikasi Pola Hubungan Komunikasi Sandi sebagaimana dimaksud dalam Pasal 30 huruf (a), dilakukan terhadap:

- a. pola hubungan komunikasi pimpinan dan pejabat struktural internal Pemerintah Daerah;
- b. alur informasi yang dikomunikasikan antar PD dan Internal PD;
- c. teknologi informasi dan komunikasi;
- d. kompetensi personil; dan
- e. infrastruktur komunikasi.

Pasal 32

Analisis Pola Hubungan Komunikasi Sandi sebagaimana dimaksud dalam Pasal 30 huruf (b), dilakukan terhadap hasil identifikasi Pola Hubungan Komunikasi Sandi yang memuat:

- a. pengguna layanan yang akan terhubung dalam jaring komunikasi Sandi;
- b. topologi atau bentuk atau model keterhubungan jaring komunikasi sandi antar Pengguna Layanan Keamanan Informasi;
- c. perangkat keamanan teknologi informasi dan komunikasi, serta fasilitas lainnya yang dibutuhkan; dan
- d. tugas dan tanggung jawab pengelola dan Pengguna Layanan Keamanan Informasi.

Pasal 33

- (1) Hasil identifikasi Pola Hubungan Komunikasi Sandi pada Pasal 32 ditetapkan sebagai Pola Hubungan Komunikasi Sandi antar PD dengan Keputusan Bupati.
- (2) Keputusan Bupati sebagaimana dimaksud pada ayat (1), paling sedikit memuat:
 - a. entitas pengguna layanan yang terhubung dalam jaring komunikasi Sandi;
 - b. topologi atau bentuk atau model keterhubungan antar Pengguna Layanan Keamanan Informasi;
 - c. sarana dan prasarana yang digunakan; dan
 - d. tugas dan tanggung jawab pengelola dan Pengguna Layanan Keamanan Informasi.
- (3) Salinan Keputusan sebagaimana dimaksud pada ayat (2), disampaikan oleh Bupati kepada Gubernur dan ditembuskan kepada Kepala BSSN.

Bagian Ketujuh

OPERASIONAL DUKUNGAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Pasal 34

- (1) Operasional dukungan Persandian untuk Pengamanan Informasi merupakan kegiatan operasional yang tidak terkait dengan Kriptografi namun mendukung terciptanya Keamanan Informasi.

- (2) Operasional dukungan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) meliputi:
 - a. pengamanan gelombang frekuensi (*jamming*);
 - b. kontra penginderaan; dan
 - c. penilaian Keamanan Sistem Informasi.
- (3) Pelaksana kegiatan operasional dukungan Persandian untuk pengamanan informasi oleh aparatur sipil negara pada Dinas.
- (4) Pelaksanaan operasional dukungan Persandian untuk Pengamanan Informasi Pemerintah Daerah mengacu pada ketentuan peraturan perundang-undangan.

Pasal 35

- (1) Pengamanan gelombang frekuensi (*jamming*) sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf a, merupakan upaya pengamanan sinyal dari ancaman penyalahgunaan sinyal untuk kepentingan yang tidak bertanggung jawab dengan cara menutup/memutuskan frekuensi.
- (2) Pengamanan gelombang frekuensi (*jamming*) dilakukan berdasarkan hasil identifikasi pada kegiatan Pemerintah Daerah yang berpotensi timbulnya ancaman penyalahgunaan sinyal.

Pasal 36

- (1) Kontra penginderaan sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf b, merupakan upaya melakukan deteksi dari pengawasan oleh pihak yang tidak berwenang pada objek ruang tertentu.
- (2) Kontra penginderaan sebagaimana dimaksud pada ayat (1) dilakukan pada objek ruang milik Pemerintah Daerah yang dilakukan untuk melakukan komunikasi terkait informasi yang harus diamankan.
- (3) Pelaksanaan kontra penginderaan sebagaimana dimaksud pada ayat (2), dilakukan secara berkala.
- (4) Temuan hasil kontra penginderaan berupa barang yang diduga menjadi peralatan penginderaan (*surveillance*) dapat dikonsultasikan ke BSSN dan/atau Kementerian/lembaga lainnya.
- (5) Hasil pelaksanaan kontra penginderaan harus ditindaklanjuti oleh Pemerintah Daerah sebagai bahan evaluasi dan perbaikan penyelenggaraan Layanan Keamanan Informasi dan Persandian.

Pasal 37

- (1) Penilaian keamanan sistem informasi sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf (c), merupakan upaya untuk mengukur tingkat kerawanan dan keamanan dari sistem informasi di lingkungan Pemerintah Daerah.
- (2) Penilaian keamanan sistem informasi sebagaimana dimaksud pada ayat (1) dilakukan pada sistem informasi milik Pemerintah Daerah.
- (3) Pemerintah Daerah melaksanakan kegiatan penilaian keamanan sistem informasi berkoordinasi dengan BSSN dan/atau kementerian/lembaga lainnya.
- (4) Hasil pelaksanaan penilaian keamanan sistem informasi sebagaimana dimaksud pada ayat (3), harus ditindaklanjuti oleh Pemerintah Daerah sebagai bahan evaluasi dan perbaikan dalam penyelenggaraan

BAB V

LAYANAN SERTIFIKAT ELEKTRONIK

Pasal 38

- (1) Pemerintah Daerah dalam penyelenggaraan Layanan Keamanan Informasi dan Persandian perlu menggunakan Jaringan Intra pemerintah.
- (2) Penggunaan Jaringan Intra pemerintah sebagaimana dimaksud pada ayat (1), bertujuan untuk menjaga keamanan dalam pengiriman data dan informasi antar Instansi Pusat dan/atau Pemerintah Daerah.

Pasal 39

- (1) Layanan Sertifikat Elektronik di lingkungan Pemerintah Daerah bertujuan untuk menjamin keutuhan, otentikasi dan nirangkal dokumen elektronik.
- (2) Layanan Sertifikat Elektronik dapat dimanfaatkan oleh Pemerintah Daerah jika memenuhi persyaratan dan telah diberikan kewenang oleh BSR E BSSN sesuai ketentuan peraturan perundang-undangan.
- (3) Setiap aparatur sipil negara Pemerintah Daerah dapat memiliki Sertifikat Elektronik yang dapat digunakan selama melaksanakan tugas kedinasan.
- (4) Kepemilikan Sertifikat Elektronik sebagaimana dimaksud pada ayat (3), difasilitasi oleh Dinas.
- (5) Tugas kedinasan sebagaimana dimaksud pada ayat (3) meliputi:
 - a. pengiriman dan pembuatan surat elektronik (email);
 - b. pembuatan dokumen persuratan elektronik; dan/atau
 - c. pembuatan dokumen elektronik lainnya yang menggunakan aplikasi dan sistem elektronik.
- (6) Aplikasi dan Sistem Elektronik yang dimiliki oleh Pemerintah Daerah harus memanfaatkan layanan Sertifikat Elektronik dalam rangka Pengamanan Informasi.

Pasal 40

- (1) Proses pemanfaatan Layanan Sertifikat Elektronik dilakukan melalui:
 - a. pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaharuan dan pencabutan Sertifikat Elektronik;
 - b. pengembangan aplikasi pendukung penggunaan Sertifikat Elektronik;
 - c. fasilitasi kegiatan sosialisasi dan bimbingan teknis terkait Sertifikat Elektronik; dan
 - d. pengawasan dan evaluasi penggunaan Sertifikat Elektronik.
- (2) Pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaharuan dan pencabutan Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) huruf a meliputi:
 - a. menangani verifikasi identitas berdasarkan identitas resmi, keanggotaan pada instansi dan rekomendasi dari instansi;
 - b. menyetujui/menolak permintaan pendaftaran Sertifikat Elektronik;
 - c. menindaklanjuti permintaan Sertifikat Elektronik kepada BSR E;
 - d. menyampaikan Sertifikat Elektronik kepada pemohon; dan
 - e. melakukan pengarsipan berkas pendaftaran Sertifikat Elektronik dalam bentuk *hardcopy* dan *softcopy*.

BAB VI
PEMANTAUAN, EVALUASI DAN PELAPORAN

Pasal 41

- (1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan Pola Hubungan Komunikasi Sandi antar PD.
- (2) Dinas melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1), setiap 1 (satu) tahun sekali.
- (3) Laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (2), disampaikan kepada Bupati dan Gubernur.
- (4) Pemantauan, evaluasi dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan Pola Hubungan Komunikasi Sandi antar PD dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII
KETENTUAN PENUTUP

Pasal 42

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Bungku
pada tanggal 5 Agustus 2024
Pj. BUPATI MOROWALI,

ttd.

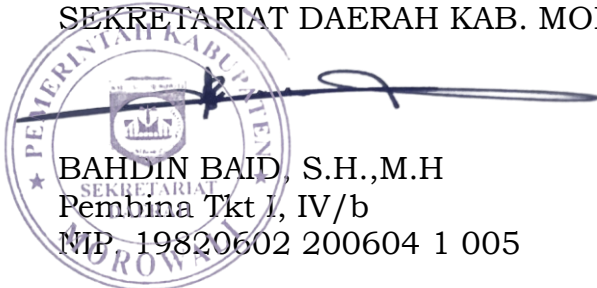
YUSMAN MAHBUB

Diundangkan di Bungku
pada tanggal 5 Agustus 2024
Plh. SEKRETARIS DAERAH KABUPATEN MOROWALI,
ttd.

HUSBAN LAONU

BERITA DAERAH KOTA MOROWALI TAHUN 2024 NOMOR 028

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM
SEKRETARIAT DAERAH KAB. MOROWALI


BAHDIN BAID, S.H., M.H
Pembina Tkt I, IV/b
NP 19820602 200604 1 005