



BUPATI MOROWALI
PROVINSI SULAWESI TENGAH

PERATURAN BUPATI MOROWALI
NOMOR 18. TAHUN 2025

TENTANG
MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MOROWALI,

- Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Kabupaten Morowali, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;
- b. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Morowali dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai manajemen keamanan informasi sistem pemerintahan berbasis elektronik;
- c. bahwa berdasarkan Peraturan Daerah Nomor 9 Tahun 2024 tentang Sistem Pemerintahan Berbasis Elektronik, terkait pentingnya kebijakan manajemen keamanan informasi perlu menyusun manajemen keamanan informasi sistem pemerintahan berbasis elektronik;
- d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

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 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 6858);

MEMUTUSKAN

Menetapkan : PERATURAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
2. Keamanan Informasi adalah suatu kondisi untuk melindungi aset yang dimiliki organisasi dari berbagai ancaman pihak internal maupun eksternal untuk menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, serta terjaganya aspek kerahasiaan, keutuhan dan ketersediaan dari informasi.
3. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
4. Manajemen Keamanan Informasi SPBE adalah serangkaian proses untuk mengamankan Sistem Pemerintahan Berbasis Elektronik (SPBE).

5. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
6. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
7. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan atas informasi dan komunikasi secara Elektronik.
8. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan atas Informasi Elektronik.
9. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan atas Informasi Elektronik.
10. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
11. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan system, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat Elektronik lainnya.
12. Daerah adalah Kabupaten Morowali
13. Bupati adalah Bupati Morowali
14. Sekretaris Daerah adalah Sekretaris Daerah Morowali.
15. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.

Pasal 2

- (1) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal Manajemen Keamanan Informasi SPBE di Daerah.
- (2) Kebijakan internal Manajemen Keamanan Informasi SPBE sebagaimana dimaksud ayat (1) meliputi :
 - a. penetapan ruang lingkup;
 - b. penetapan penanggung jawab;
 - c. perencanaan;
 - d. dukungan pengoperasian;
 - e. evaluasi kinerja; dan
 - f. perbaikan berkelanjutan terhadap Keamanan Informasi.
- (3) Ketentuan lain untuk mendukung kebijakan internal Manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) dapat menerapkan pengendalian teknis keamanan yang meliputi :
 - a. manajemen risiko;
 - b. penetapan prosedur pengendalian Keamanan Informasi SPBE; dan
 - c. pengelolaan pihak ketiga.

BAB II

KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 3

- (1) Penetapan ruang lingkup Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam pasal 2 ayat (2) huruf a meliputi:
 - a. data dan informasi SPBE;
 - b. Aplikasi SPBE; dan
 - c. Infrastruktur SPBE.
- (2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Daerah yang harus diamankan dalam SPBE.

Pasal 4

- (1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dilaksanakan oleh Bupati.
- (2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
- (3) Sekretaris daerah Kabupaten Morowali sebagai penanggung jawab merupakan ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan peraturan perundangundangan.

Pasal 5

- (1) Dalam melaksanakan tugas sebagai penanggung jawab Manajemen Keamanan Informasi SPBE, Koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) menetapkan pelaksana teknis Keamanan SPBE.
- (2) Pelaksana teknis Keamanan SPBE sebagai dimaksud pada ayat (1) terdiri atas:
 - a. Ketua Tim; dan
 - b. Anggota Tim.
- (3) Ketua Tim sebagaimana dimaksud pada ayat (2) huruf a dapat dijabat oleh Kepala PD yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.
- (4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh Kepala PD lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di Daerah.
- (5) Tim sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Bupati.

Pasal 6

- (1) Ketua Tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan Manajemen Keamanan Informasi SPBE di Daerah yang meliputi:
 - a. menetapkan prosedur pengendalian Keamanan Informasi SPBE;

- b. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE;
 - c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundangundangan;
 - d. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
 - e. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans*; dan
 - f. melaporkan pelaksanaan Manajemen Keamanan Informasi SPBE pada koordinator SPBE.
- (2) Anggota Tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b bertugas:
- a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian Keamanan Informasi SPBE pada PD;
 - b. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundangundangan;
 - c. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
 - d. berkoordinasi dengan Ketua Tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 7

- (1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf c ditetapkan oleh Ketua Tim pelaksana teknis Keamanan SPBE.
- (2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
 - a. program kerja Keamanan SPBE; dan
 - b. target realisasi program kerja Keamanan SPBE.

Pasal 8

- (1) Program kerja Keamanan SPBE sebagaimana dimaksud pada Pasal 7 ayat (2) huruf a minimal memuat:
 - a. edukasi kesadaran Keamanan SPBE;
 - b. penilaian kerentanan Keamanan SPBE;
 - c. peningkatan Keamanan SPBE;
 - d. penanganan insiden Keamanan SPBE; dan
 - e. audit Keamanan SPBE.
- (2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada Pasal 7 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 9

- (1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf d dilakukan oleh Koordinator SPBE.

- (2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
 - a. sumber daya manusia Keamanan SPBE;
 - b. teknologi Keamanan SPBE; dan
 - c. anggaran Keamanan SPBE.
- (3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan Manajemen Keamanan Informasi SPBE diberikan alokasi sumber daya yang sesuai.

Pasal 10

- (1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan syarat harus memiliki kompetensi:
 - a. keamanan TIK; dan
 - b. keamanan aplikasi.
- (2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus didukung dengan kegiatan:
 - a. pelatihan dan/atau sertifikasi kompetensi keamanan TIK dan keamanan aplikasi; dan/atau
 - b. bimbingan teknis mengenai standar teknis dan prosedur Keamanan SPBE.
- (3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia Keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan SPBE.

Pasal 11

Teknologi keamanan informasi sebagaimana dimaksud pada pasal 9 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.

Pasal 12

Anggaran Keamanan SPBE sebagaimana dimaksud pada pasal 9 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 13

- (1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf e dilakukan oleh Koordinator SPBE.
- (2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan Manajemen Keamanan Informasi SPBE di Daerah.
- (3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
 - a. menganalisis efektifitas pelaksanaan Keamanan SPBE; atau
 - b. mendukung dan merealisasikan program audit Keamanan SPBE.
- (4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 14

- (1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf f dilakukan oleh pelaksana teknis Keamanan SPBE.
- (2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.
- (3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
 - a. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE;
 - b. memperbaiki pelaksanaan Keamanan SPBE secara periodik; dan
 - c. tindak lanjut hasil audit Keamanan SPBE.

Pasal 15

- (1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf a dilakukan oleh setiap PD.
- (2) Manajemen risiko sebagaimana dimaksud pada ayat (1) minimal menyusun daftar risiko dengan ketentuan substansi meliputi:
 - a. inventarisasi aset SPBE;
 - b. identifikasi ancaman dan kerentanan keamanan terhadap aset SPBE;
 - c. penilaian risiko keamanan terhadap aset SPBE;
 - d. penentuan prioritas risiko;
 - e. analisa dampak jika terjadi risiko;
 - f. analisa kontrol keamanan yang bisa diterapkan; dan/atau
 - g. rekomendasi kontrol keamanan.
- (3) Prosedur pelaksanaan manajemen risiko mengacu sesuai dengan ketentuan peraturan perundangundangan.

Pasal 16

- (1) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf b ditetapkan oleh Ketua Tim pelaksana teknis Keamanan SPBE.
- (2) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah.
- (3) Implementasi Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (3), mencakup aspek yang dapat meliputi:
 - a. keamanan perangkat TIK;
 - b. keamanan jaringan;
 - c. keamanan pusat data;
 - d. keamanan perangkat *end point*;
 - e. keamanan *remote working*;
 - f. keamanan penyimpanan elektronik;
 - g. pengelolaan akses kontrol;

- h. pengendalian keamanan dari ancaman virus dan *malware*;
 - i. persyaratan keamanan terkait pembangunan dan pengembangan aplikasi SPBE;
 - j. pengelolaan aset;
 - k. keamanan migrasi data;
 - l. konfigurasi perangkat IT *Security*;
 - m. perlindungan data pribadi;
 - n. keamanan komunikasi;
 - o. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
 - p. pengendalian keamanan informasi terhadap pihak ketiga;
 - q. penerapan kriptografi;
 - r. penanganan insiden Keamanan Informasi;
 - s. kelangsungan bisnis atau layanan TIK;
 - t. perencanaan pemulihan bencana terhadap layanan TIK;
 - u. audit internal Keamanan SPBE; dan/atau
 - v. aspek prosedur pengendalian Keamanan Informasi SPBE lainnya.
- (4) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dengan Keputusan Bupati.

Pasal 17

- (1) Setiap PD harus melaksanakan ketentuan penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 14 ayat (4).
- (2) Setiap PD bertanggungjawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian Keamanan Informasi SPBE.

Pasal 18

- (1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf c dilakukan oleh setiap PD.
- (2) PD memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan.
- (3) PD harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
- (4) PD harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek Keamanan Informasi dalam hubungan kerjasama dengan pihak ketiga.
- (5) PD harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.
- (6) Laporan sebagaimana dimaksud pada ayat (5) disampaikan kepada Bupati.

BAB III
KETENTUAN PENUTUP

Pasal 19

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 24 Maret 2025
BUPATI MOROWALI,

ttd.

IKSAN

Diundangkan di Bungku
pada tanggal 24 Maret 2025

SEKRETARIS DAERAH KABUPATEN MOROWALI,

ttd.

YUSMAN MAHBUB

BERITA DAERAH KABUPATEN MOROWALI TAHUN 2025 NOMOR 021

Salinan sesuai dengan aslinya

KEPALA BAGIAN HUKUM

SEKRETARIAT DAERAH KABUPATEN MOROWALI,



BAHDIN BAID, S.H.,M.H

Pembina Tkt I,IV/b

NIP.19820602 200604 1 005