



BUPATI MAMUJU TENGAH
PROVINSI SULAWESI BARAT

PERATURAN BUPATI MAMUJU TENGAH
NOMOR 6 TAHUN 2025

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MAMUJU TENGAH,

- Menimbang:
- a. bahwa setiap orang berhak untuk berkomunikasi dan memperoleh Informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, dan menyimpan Informasi dengan menggunakan segala jenis saluran yang tersedia;
 - b. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Daerah, perlu melaksanakan Manajemen Keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;
 - c. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Daerah dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai 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 4 Tahun 2013 tentang Pembentukan Kabupaten Mamuju Tengah di Provinsi Sulawesi Barat (Lembaran Negara Republik Indonesia Tahun 2013 Nomor 19, Tambahan Lembaran Negara Republik Indonesia Nomor 5397);
 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 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 MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Mamuju Tengah.
2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Mamuju Tengah.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Mamuju Tengah
5. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
6. Sistem Pemerintah Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi komunikasi untuk memberikan layanan kepada pengguna SPBE.
7. Teknologi informasi dan komunikasi selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan dan pemindahan informasi antar media.
8. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan (*confidentiality*) atas informasi dan komunikasi secara Elektronik.
9. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas Informasi Elektronik.
10. Ketersediaan adalah sesuai dengan konsep tentang ketersediaan (*availability*) atas informasi Elektronik.
11. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
12. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas dan fungsi layanan SPBE.
13. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integritas/penghubung, dan perangkat Elektronik lainnya.

Pasal 2

Peraturan Bupati ini dimaksudkan sebagai kebijakan internal Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah.

BAB II KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 3

Kebijakan internal Manajemen Keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 meliputi:

- a. penetapan ruang lingkup;
- b. penetapan penanggung jawab;
- c. perencanaan;
- d. dukungan pengoperasian;
- e. evaluasi kinerja; dan
- f. perbaikan berkelanjutan terhadap keamanan informasi.

Pasal 4

- (1) Penetapan ruang lingkup Manajemen Keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 3 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 Pemerintah Daerah yang harus diamankan dalam SPBE.

Pasal 5

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

Pasal 6

- (1) Dalam melaksanakan tugas sebagai penanggung jawab Manajemen Keamanan informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 5 ayat (3) menetapkan pelaksanaan teknis keamanan SPBE.
- (2) Pelaksanaan teknis keamanan SPBE sebagaimana 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 pimpinan PD yang membidangi urusan komunikasi dan informatika.
- (4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh pimpinan PD lainnya yang memiliki,

membawahi, membangun, memelihara, dan/atau mengembangkan aplikasi SPBE dan/atau infrastruktur SPBE dilingkungan Pemerintah Daerah.

Pasal 7

- (1) Ketua tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan Manajemen Keamanan informasi SPBE dilingkungan Pemerintah Daerah yang meliputi:
 - a. menetapkan prosedur pengendalian keamanan informasi SPBE Pemerintah Daerah;
 - b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE dilingkungan Pemerintah Daerah;
 - c. memastikan penerapan keamanan Aplikasi SPBE dan infrastruktur SPBE sesuai dengan standar teknis dan prosedur keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan;
 - d. merumuskan, mengkoordinasikan, 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 6 ayat (2) huruf b mempunyai tugas:
 - a. mengkoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada PD masing-masing;
 - b. memastikan penerapan keamanan Aplikasi SPBE dan infrastruktur SPBE sesuai dengan standar teknis dan prosedur keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan;
 - 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 dan Infrastruktur SPBE.

Pasal 8

- (1) Perencanaan sebagaimana dimaksud dalam Pasal 3 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 9

- (1) Program kerja keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf a paling sedikit meliputi:
 - a. edukasi kesadaran keamanan SPBE;
 - b. penilaian kerentanan keamanan SPBE;

- c. peningkatan keamanan SPBE;
 - d. penanganan insiden keamanan SPBE;
 - e. audit keamanan SPBE.
- (2) Target realisasi program kerja keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 10

- (1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 3 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) Koordinasi SPBE melalui dukungan pengoperasian memastikan pelaksanaan Manajemen Keamanan informasi SPBE diberikan alokasi sumber daya yang sesuai.

Pasal 11

- (1) Sumber daya manusia keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:
- a. keamanan TIK; dan
 - b. keamanan aplikasi.
- (2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1) paling sedikit harus adanya dukungan kegiatan:
- a. pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi TIK; 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.
- (4) Teknologi keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap PD.
- (5) Anggaran keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 12

- (1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 huruf e dilakukan oleh koordinator SPBE.
- (2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan Manajemen Keamanan informasi SPBE di lingkungan Pemerintah Daerah.
- (3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:

- a. menganalisis efektifitas pelaksanaan keamanan SPBE; dan/atau
 - b. mendukung dan merealisasikan program audit keamanan.
- (4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 13

- (1) Perbaikan berkelanjutan terhadap keamanan informasi sebagaimana dimaksud dalam Pasal 3 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. tindaklanjuti hasil audit keamanan SPBE.

BAB III

PENGENDALIAN TEKNIS KEAMANAN

Pasal 14

Selain kebijakan internal Manajemen Keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 3 dapat menerapkan pengendalian teknis keamanan meliputi:

- a. manajemen risiko;
- b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
- c. pengelolaan pihak ketiga.

Pasal 15

- (1) Manajemen risiko sebagaimana dimaksud dalam Pasal 14 huruf a dilakukan oleh setiap PD.
- (2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko (*risk register*) 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 perundang-undangan.

Pasal 16

- (1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 14 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 dilingkungan pemerintah Kabupaten Mamuju Tengah dengan cakupan aspek dapat meliputi:
 - a. keamanan perangkat teknologi informasi komunikasi;
 - 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 (*business continuity*);
 - t. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);
 - u. audit internal keamanan SPBE; dan/atau
 - v. aspek prosedur pengendalian keamanan informasi SPBE lainnya.
- (3) 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 16.
- (2) Setiap PD bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan pedoman pada prosedur pengendalian keamanan informasi SPBE.

Pasal 18

- (1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 14 huruf c dilakukan oleh setiap perangkat daerah.
- (2) PD harus memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar 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 (*service level agreement*/SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.
- (6) Memastikan tersedianya perjanjian kerahasiaan dengan pihak ketiga terkait pekerjaan Pembangunan dan atau pengembangan Aplikasi dan Infrastruktur SPBE.

BAB IV

KETENTUAN PENUTUP

Pasal 19

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahui, memerintahkan pengundangan Peraturan Bupati dengan penempatannya dalam serta Pemerintah Kabupaten Mamuju Tengah.

Ditetapkan di Tobadak
pada tanggal 26 Maret 2025
BUPATI MAMUJU TENGAH,

ttd

ARSAL ARAS

Diundangkan di Tobadak
Pada tanggal 25 Maret 2025
Pj.SEKRETARIS DAERAH KABUPATEN MAMUJU TENGAH,

ttd

LITHA FEBRIANI

BERITA DAERAH KABUPATEN MAMUJU TENGAH TAHUN 2025 NOMOR 6

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,



LUKMAN,S.Sos
NIP.19690604 200112 1 007