



BUPATI GOWA
PROVINSI SULAWESI SELATAN

PERATURAN BUPATI GOWA
NOMOR 30 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS
ELEKTRONIK DI LINGKUNGAN PEMERINTAH DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA
BUPATI GOWA,

- Menimbang :
- a. bahwa dalam rangka memanfaatkan sistem pemerintahan berbasis elektronik agar dapat memberikan manfaat bagi perkembangan perekonomian daerah dan kemanfaatan umum, perlu disusun manajemen keamanan informasi;
 - b. bahwa dalam rangka penyelenggaraan pemerintah 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 sistem manajemen keamanan informasi Sistem Pemerintah 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 di Lingkungan Pemerintah Daerah;

- Mengingat :
1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
 2. Undang-Undang Nomor 29 Tahun 1959 tentang Pembentukan Daerah Tingkat II di Sulawesi (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 74, Tambahan Lembaran Negara Republik Indonesia Nomor 1822);

3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
4. 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);
5. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5586) sebagaimana telah diubah beberapa kali 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);
6. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
7. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2018 Nomor 182);
8. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
9. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
10. Peraturan Badan Siber Dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH DAERAH.

BAB I KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Gowa.
2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin Pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Gowa.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Gowa.
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 Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE secara terintegrasi.
7. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
8. 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, integritas dan ketersediaan dari informasi.
9. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
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 sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.

12. Teknologi Informasi dan Komunikasi yang selanjutnya disebut TIK adalah teknologi yang digunakan untuk mengumpulkan, menyimpan, mengirim, dan memanipulasi informasi.

BAB II MAKSUD DAN TUJUAN

Pasal 2

- (1) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal manajemen Keamanan Informasi di lingkungan Pemerintah Daerah.
- (2) Kebijakan internal manajemen Keamanan Informasi sebagaimana dimaksud pada 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) Kebijakan lain untuk mendukung kebijakan internal manajemen keamanan informasi 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 III RUANG LINGKUP

Pasal 3

Ruang lingkup peraturan Bupati ini meliputi:

- a. kebijakan internal manajemen keamanan informasi; dan
- b. pengendalian teknis keamanan.

BAB IV KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI

Pasal 4

- (1) Penetapan ruang lingkup sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a meliputi aset:
- a. data dan Informasi;
 - 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 2 ayat (2) huruf b dilaksanakan oleh Bupati.
- (2) 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 ketentuan 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 pelaksana teknis keamanan SPBE .
- (2) Pelaksana 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 di lingkungan Pemerintah Daerah.

Pasal 7

- (1) Ketua tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah yang meliputi:
 - a. menetapkan prosedur pengendalian Keamanan Informasi SPBE Pemerintah Daerah;
 - b. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE di lingkungan 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, 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 6 ayat (2) huruf b mempunyai tugas:
- a. mengoordinasikan 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 ketentuan 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 SPBE dan Infrastruktur SPBE.

Pasal 8

- (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 9

- (1) Program kerja keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf a paling rendah meliputi:
- 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 dalam Pasal 8 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 10

- (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 11

- (1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf a minimal 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), minimal harus adanya dukungan kegiatan:
 - a. pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi dan 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 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 lingkungan Pemerintah 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 minimal 1 (satu) kali dalam 1 (satu) tahun.

Pasal 13

- (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 tidak 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.

BAB V PENGENDALIAN TEKNIS KEAMANAN

Pasal 14

- (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 perundang-undangan.

Pasal 15

- (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 dengan cakupan aspek 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 (*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) Ketentuan lebih lanjut mengenai penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) ditetapkan dengan Keputusan Bupati.

Pasal 16

- (1) Setiap PD harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 15 ayat (3).
- (2) Setiap PD bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian keamanan informasi SPBE.

Pasal 17

- (1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf c dilakukan oleh setiap PD.
- (2) PD harus memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dikukan 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 berserta kode sumbernya.

- (4) PD harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama 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.

BAB VI
KETENTUAN PENUTUP

Pasal 18

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Sungguminasa
pada tanggal 10 Oktober 2024



BUPATI GOWA,

NONAN BURICHTA ICHSAN YL

Diundangkan di Sungguminasa
pada tanggal 10 Oktober 2024



SEKRETARIS DAERAH KABUPATEN GOWA,

BERITA DAERAH KABUPATEN GOWA TAHUN 2024 NOMOR 30