SALINAN

BUPATI SITUBONDO
PROVINSI JAWA TIMUR

PERATURAN BUPATI SITUBONDO
NOMOR 18 TAHUN 2025

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN SITUBONDO

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI SITUBONDO,

Menimbang :

a. bahwa dalam rangka mengoptimalkan penyelenggaraan Sistem Pemerintahan Berbasis Elektronik yang dapat menjamin keamanan data dan informasi di lingkungan Pemerintah Daerah, perlu adanya pelaksanaan dan pengelolaan Sistem Keamanan Informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan data dan 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 Daerah Situbondo dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai manajemen keamanan informasi sistem pemerintahan berbasis elektronik;
c. bahwa sesuai ketentuan Pasal 41 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, Pemerintah Daerah harus menerapkan keamanan 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 di Lingkungan Pemerintah Kabupaten Situbondo;

Mengingat :

1. Pasal 18 Ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 12 Tahun 1950 tentang Pembentukan Daerah Kabupaten di Lingkungan Provinsi Jawa Timur (Berita Negara Republik Indonesia Tahun 1950 Nomor 41) sebagaimana telah diubah dengan Undang-Undang Nomor 2 Tahun 1965 tentang Perubahan Batas Wilayah Kotapraja Surabaya dan Dati II Surabaya (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 19, Tambahan Lembaran Negara Republik Indonesia Nomor 2730);
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 6856);
4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
5. 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 KABUPATEN SITUBONDO.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini, yang dimaksud dengan:
1. Daerah adalah Kabupaten Situbondo.
2. Pemerintah Daerah adalah Pemerintah Kabupaten Situbondo.
3. Bupati adalah Bupati Situbondo.
4. Dinas Komunikasi dan Informatika Kabupaten Situbondo yang selanjutnya disebut Dinas adalah perangkat daerah yang menyelenggarakan urusan di bidang Persandian.
5. 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.

6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
7. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
8. Keamanan Informasi adalah terjaganya kerahasiaan *(confidentiality),* keutuhan *(integrity),* ketersediaan (availability), keaslian, dan kenirsangkalan (*nonrepudiation*) Informasi.
9. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai pedoman kebijakan internal manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah.
(2) Pelaksanaan persandian untuk pengamanan informasi bertujuan untuk:
    a. menciptakan harmonisasi dalam melaksanakan Persandian untuk pengamanan informasi;
    b. meningkatkan komitmen, efektivitas, dan kinerja Pemerintah Daerah dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan Persandian untuk pengamanan informasi; dan
    c. memberikan pedoman dalam menetapkan pola hubungan komunikasi sandi antar Perangkat Daerah.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 3

Kebijakan internal manajemen keamanan informasi SPBE 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) Ruang lingkup manajemen keamanan informasi SPBE meliputi:
    a. data dan informasi SPBE;
    b. aplikasi SPBE; dan
    c. aset infrastruktur SPBE.
(2) Ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Daerah yang harus diamankan dalam SPBE.

Pasal 5

(1) Penanggung jawab manajemen keamanan informasi SPBE dijabat oleh Sekretaris Daerah.
(2) Sekretaris Daerah sebagai penanggung jawab merupakan ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE sesuai dengan peraturan perundang-undangan.
(3) Penanggung jawab sebagaimana dimaksud pada ayat (1) ditetapkan oleh Bupati.

Pasal 6

(1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen keamanan informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 5 ayat (2) menetapkan pelaksana teknis Keamanan SPBE.
(2) Pelaksana teknis Keamanan SPBE sebagai dimaksud pada ayat (1) terdiri atas:
    a. Ketua; dan
    b. Anggota.
(3) Ketua Tim sebagaimana dimaksud pada ayat (2) huruf a dijabat oleh Kepala Dinas.
(4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh pimpinan perangkat daerah 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 5 ayat (2) huruf b mempunyai tugas:
    a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada perangkat daerah 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 SPBE dan Infrastruktur SPBE.

Pasal 8

(1) Perencanaan manajemen keamanan informasi SPBE 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; 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 manajemen keamanan informasi SPBE 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 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 ada 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.

Pasal 12

Teknologi keamanan informasi sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.

Pasal 13

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 14

(1) Evaluasi kinerja manajemen keamanan informasi SPBE 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. mengidentifikasi, menganalisis, mengelola dan mengendalikan kerentanan pada layanan, aplikasi maupun infrastruktur SPBE;
   b. menganalisis efektivitas pelaksanaan Keamanan SPBE.
(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (3) huruf a dilakukan oleh pihak internal dan eksternal organisasi yang memiliki kompetensi berdasarkan kriteria dan standar tertentu sesuai peraturan perundang-undangan.
(5) Evaluasi kinerja sebagaimana dimaksud pada ayat (3) huruf b dilaksanakan dengan:
   a. mengidentifikasi dan menganalisis Indeks Keamanan Informasi; dan
   b. mendukung dan merealisasikan program audit Keamanan SPBE.
(6) Evaluasi kinerja sebagaimana dimaksud pada ayat (4) dan ayat (5) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.
(7) Perangkat Daerah menyampaikan laporan hasil evaluasi kepada penanggung jawab.

(8) Ketentuan lebih lanjut terkait teknis evaluasi dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah di lingkungan Pemerintah Daerah ditetapkan oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 15

(1) Perbaikan berkelanjutan 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.

BAB III
PENGENDALIAN TEKNIS KEAMANAN

Pasal 16

Untuk mendukung kebijakan internal manajemen keamanan informasi SPBE, dapat menerapkan pengendalian teknis keamanan yang meliputi:
a. manajemen risiko;
b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
c. pengelolaan pihak ketiga.

Pasal 17

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 16 huruf a dilakukan oleh setiap perangkat daerah.
(2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko dengan 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 dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 18

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 16 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 cangkupan aspek meliputi:
    a. keamanan perangkat teknologi informasi komunikasi;
    b. konfigurasi perangkat IT Security;
    c. keamanan jaringan;
    d. keamanan komunikasi;
    e. keamanan pusat data dan lingkungan pendukung;
    f. keamanan penyimpanan elektronik;
    g. keamanan perangkat *end point*;
    h. keamanan migrasi data;
    i. keamanan *remote working*;
    j. pengelolaan akses kontrol;
    k. pengelolaan aset;
    l. pengelolaan dan pengendalian kerentanan;
    m. pengendalian keamanan dari ancaman virus dan *malware*;
    n. persyaratan keamanan terkait manajemen proyek, pembangunan dan pengembangan aplikasi SPBE;
    o. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
    p. perlindungan data pribadi;
    q. pengendalian keamanan informasi terhadap pihak ketiga;
    r. penerapan kriptografi;
    s. kelangsungan bisnis (*business continuity*) atau layanan TIK;
    t. penanganan insiden keamanan informasi;
    u. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);
    v. audit internal keamanan SPBE; dan/atau
    w. aspek prosedur pengendalian keamanan informasi SPBE lainnya.
(3) Prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) ditetapkan dengan Keputusan Bupati atau surat edaran Sekretaris Daerah.

Pasal 19

(1) Setiap perangkat daerah bertanggungjawab atas pelaksanaan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 18 ayat (3).
(2) Setiap perangkat daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian keamanan informasi SPBE.

Pasal 20

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 16 huruf c dilakukan oleh setiap perangkat daerah.
(2) Perangkat daerah harus 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) Perangkat daerah harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
(4) Perangkat daerah harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerja sama dengan pihak ketiga.
(5) Perangkat daerah harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
PENDANAAN

Pasal 21

Pelaksanaan penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah bersumber dari Anggaran Pendapatan dan Belanja Daerah dan/atau sumber pendanaan lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB V
KETENTUAN PERALIHAN

Pasal 22

Pada saat Peraturan Bupati ini berlaku, kebijakan yang telah dilaksanakan di lingkungan Pemerintah Daerah dan Peraturan Bupati yang mengatur mengenai pelaksanaan Persandian untuk Pengamanan Informasi Pemerintah Daerah yang telah ditetapkan, dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan Peraturan Bupati ini.

BAB VI
KETENTUAN PENUTUP

Pasal 23

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Situbondo
Pada tanggal 21 Maret 2025
BUPATI SITUBONDO,

ttd.

YUSUF RIO WAHYU PRAYOGO

Diundangkan di Situbondo
Pada tanggal 21 Maret 2025
SEKRETARIS DAERAH
KABUPATEN SITUBONDO,

ttd.

WAWAN SETIAWAN

BERITA DAERAH KABUPATEN SITUBONDO TAHUN 2025 NOMOR 18

Salinan sesuai dengan Aslinya,
a.n. KEPALA BAGIAN HUKUM

BHIMA SUNARTO PUTRA, S.H.
Penata (III/c)
19850725 201503 1 001