SALINAN

WALI KOTA KEDIRI
PROVINSI JAWA TIMUR

PERATURAN WALI KOTA KEDIRI
NOMOR 10 TAHUN 2026

TENTANG
MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA KEDIRI,

Menimbang :

a. 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;
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 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 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, Manajemen keamanan informasi SPBE perlu dilaksanakan oleh setiap Pemerintah Daerah berdasarkan pedoman yang telah ditetapkan;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Wali Kota 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 16 Tahun 1950 tentang Pembentukan Daerah-daerah Kota Besar dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, Jawa Barat dan dalam Daerah Istimewa Yogyakarta (Berita Negara Republik Indonesia Tahun 1950 Nomor 45) sebagaimana telah diubah dengan Undang-Undang Nomor 13 Tahun 1954 tentang Pengubahan Undang-Undang Nomor 16 dan Nomor 17 Tahun 1950 tentang Pembentukan Kota-Kota Besar dan Kota-Kota Kecil di Jawa (Lembaran Negara Republik Indonesia Tahun 1954 Nomor 40, Tambahan Lembaran Negara Republik Indonesia Nomor 551);

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 5587) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 9 Tahun 2015 (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
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 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
10. Peraturan Wali Kota Kediri Nomor 42 Tahun 2019 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kota Kediri Tahun 2020 Nomor 1) sebagaimana telah diubah beberapa kali terakhir dengan Peraturan Wali Kota Kediri Nomor 48 Tahun 2022 tentang Perubahan Kedua Atas Peraturan Wali Kota Nomor 42 Tahun 2019 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kota Kediri Tahun 2022 Nomor 48);

MEMUTUSKAN:

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

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:
1. Daerah adalah Kota Kediri.
2. Pemerintah Daerah adalah Pemerintah Kota Kediri.

3. Wali Kota adalah Wali Kota Kediri.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Kediri.
5. Perangkat Daerah adalah unsur pembantu Wali Kota dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
6. Dinas Komunikasi dan Informatika Kota Kediri yang selanjutnya disebut Dinas adalah Perangkat Daerah di lingkungan Pemerintah Kota Kediri yang menyelenggarakan urusan pemerintahan di bidang komunikasi, informatika, statistik, dan persandian.
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
8. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
9. 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.
10. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
11. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan atas informasi dan komunikasi secara Elektronik.
12. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan atas Informasi Elektronik.
13. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan atas Informasi Elektronik.
14. Manajemen Keamanan Informasi SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
15. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
16. 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.

Pasal 2

(1) Manajemen Keamanan Informasi SPBE dimaksudkan sebagai kebijakan internal untuk mewujudkan tata kelola perlindungan aset informasi yang terpadu dan sistematis guna menjamin kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan dalam penyelenggaraan pemerintahan berbasis elektronik.
(2) Kebijakan internal Manajemen Keamanan Informasi SPBE 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) 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.

(4) Keamanan Informasi SPBE mencakup penjaminan:
   a. kerahasiaan;
   b. keutuhan;
   c. ketersediaan;
   d. keaslian; dan
   e. kenirsangkalan sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.

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 Pemerintah Daerah yang harus diamankan dalam SPBE.

Pasal 4

(1) Penanggung jawab sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b ditetapkan oleh Wali Kota.
(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
(3) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan Informasi SPBE, Sekretaris Daerah disebut sebagai koordinator SPBE.
(4) Koordinator SPBE sebagaimana dimaksud pada ayat (3) wajib melaporkan kepada Wali Kota.

Pasal 5

(1) Dalam melaksanakan tugas sebagai penanggung jawab Manajemen Keamanan Informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) menetapkan tim pelaksana teknis Keamanan Informasi 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 pimpinan Dinas.
(4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh pimpinan Perangkat Daerah yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di Pemerintah Daerah.

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 Pemerintah Daerah;
   b. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE di Daerah;
   c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai ketentuan 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 keberlangsungan bisnis dan rencana pemulihan bencana; 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 Informasi SPBE yang telah ditetapkan sesuai ketentuan peraturan perundang-undangan;
c. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen keberlangsungan bisnis dan rencana pemulihan bencana; 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 Informasi SPBE.
(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
a. program kerja Keamanan Informasi SPBE; dan
b. target realisasi program kerja Keamanan Informasi SPBE.

Pasal 8

(1) Program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf a paling sedikit meliputi:
a. edukasi kesadaran Keamanan Informasi SPBE;
b. penilaian kerentanan Keamanan Informasi SPBE;
c. peningkatan Keamanan Informasi SPBE;
d. penanganan insiden Keamanan Informasi SPBE; dan
e. audit Keamanan Informasi SPBE.
(2) Target realisasi program kerja Keamanan Informasi SPBE sebagaimana dimaksud dalam 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 Informasi SPBE;
b. teknologi Keamanan Informasi SPBE; dan
c. anggaran Keamanan Informasi 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 Informasi SPBE sebagaimana dimaksud pada pasal 9 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 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 Informasi SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan Informasi SPBE.

(4) Teknologi keamanan informasi sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

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

Pasal 11

(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 efektivitas pelaksanaan Keamanan Informasi SPBE; atau
b. mendukung dan merealisasikan program audit Keamanan Informasi SPBE.

(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 12

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf f dilakukan oleh pelaksana teknis Keamanan Informasi 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 Informasi SPBE;
b. memperbaiki pelaksanaan Keamanan Informasi SPBE secara periodik; dan
c. tindak lanjut hasil audit Keamanan Informasi SPBE.

BAB III
PENGENDALIAN TEKNIS KEAMANAN

Pasal 13

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf a dilakukan oleh setiap Perangkat Daerah.

(2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit 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. analisis dampak jika terjadi risiko;
f. analisis kontrol keamanan yang bisa diterapkan; dan/atau
g. rekomendasi kontrol keamanan.

(3) Prosedur pelaksanaan manajemen risiko mengacu pada ketentuan peraturan perundang-undangan.

Pasal 14

(1) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada Pasal 2 ayat (3) huruf b ditetapkan oleh ketua tim pelaksana teknis Keamanan Informasi SPBE.
(2) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE di Daerah dengan cakupan aspek dapat meliputi:
    a. keamanan perangkat teknologi informasi komunikasi;
    b. keamanan jaringan;
    c. keamanan pusat data;
    d. keamanan perangkat akhir;
    e. keamanan bekerja jarak jauh;
    f. keamanan penyimpanan elektronik;
    g. pengelolaan akses kontrol;
    h. pengendalian keamanan dari ancaman virus dan perangkat lunak perusak;
    i. persyaratan keamanan terkait pembangunan dan pengembangan aplikasi SPBE;
    j. pengelolaan aset;
    k. keamanan migrasi data;
    l. konfigurasi perangkat Keamanan Informasi;
    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.
(3) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk Keputusan Wali Kota atau surat edaran Sekretaris Daerah atau kebijakan teknis lainnya.

Pasal 15

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada Pasal 14 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 16

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) 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 dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
KETENTUAN PENUTUP
Pasal 17

Peraturan Wali Kota ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Wali Kota ini dengan penempatannya dalam Berita Daerah Kota Kediri.

Ditetapkan di Kediri
pada tanggal 17 Maret 2026

WALI KOTA KEDIRI,

ttd.

VINANDA PRAMESWATI

Diundangkan di Kediri
pada tanggal 17 Maret 2026

Pj. SEKRETARIS DAERAH KOTA KEDIRI,

ttd.

MOCHAMAD FERRY DJATMIKO

BERITA DAERAH KOTA KEDIRI TAHUN 2026 NOMOR 10

Salinan sesuai dengan aslinya
a.n SEKRETARIS DAERAH KOTA KEDIRI
KEPALA BAGIAN HUKUM,

PEMERINTAH KOTA KEDIRI
SEKRETARIAT DAERAH

ANITA PUJI LESTARI, SH, MH.
Penata Tk. I
NIP. 19840804 201001 2 042