WALIKOTA BLITAR

PROVINSI JAWA TIMUR

PERATURAN WALIKOTA BLITAR

NOMOR 26 TAHUN 2023

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALIKOTA BLITAR,

Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Kota Blitar, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;

b. bahwa berdasarkan ketentuan Pasal 2 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 Sistem Pemerintahan Berbasis Elektronik dilaksanakan oleh setiap Instansi Pusat dan Pemerintah Daerah;

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 Kota Blitar 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 Walikota Blitar tentang 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 17 Tahun 1950 tentang Pembentukan Daerah Kota Kecil dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah dan Jawa Barat sebagaimana telah diubah dengan Undang-Undang Nomor 13 Tahun 1954 tentang Pengubahan Undang-Undang Nomor 16 dan Nomor 17 Tahun 1950 (Republik Indonesia Dahulu) 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 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5597), sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);

4. Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 238, Tambahan Lembaran Negara Republik Indonesia Nomor 6841);

5. Peraturan Pemerintah Nomor 48 Tahun 1982 tentang Perubahan Batas Wilayah Kotamadya Daerah Tingkat II Blitar (Lembaran Negara Republik Indonesia Tahun 1982 Nomor 75, Tambahan Lembaran Negara Republik Indonesia Nomor 3243);

6. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan lnformasi 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 WALIKOTA TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan:

1. Daerah adalah Kota Blitar.
2. Pemerintah Daerah adalah Pemerintah Kota Blitar.
3. Walikota adalah Walikota Blitar.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Blitar.
5. Perangkat Daerah adalah dalah unsur pembantu Walikota 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.
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, keutuhan dan ketersediaan dari informasi.
9. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan *(nonrepudiation)* sumber daya terkait data dan informasi, Infrastruktur SPBE dan Aplikasi SPBE.
10. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasian *(confidentiality)* atas informasi dan komunikasi secara Elektronik.

11. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan *(integrity)* atas Informasi Elektronik.
12. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan *(availability)* atas Informasi Elektronik.
13. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
14. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
15. 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 *integrase/* penghubung, dan perangkat Elektronik lainnya.
16. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik.
17. Pihak Ketiga adalah pihak-pihak selain Pemerintah Daerah.
18. *Service Level Agreement* selanjutnya disingkat SLA adalah kontrak yang berisi ketetapan pencapaian sasaran tingkat layanan yang telah disetujui oleh pihak-pihak yang terikat perjanjian yang mencakup hak dan kewajiban yang harus dipenuhi oleh masing-masing pihak.

Pasal 2

(1) Peraturan Walikota ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah.

(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) 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. lnfrastruktur SPBE.

(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset pemerintah daerah yang harus diamankan dalam SPBE.

Pasal 4

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dilaksanakan oleh Walikota.

(2) Penanggungjawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.

(3) Sekretaris Daerah sebagaimana dimaksud pada ayat (2) sebagai penanggungjawab merupakan ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan.

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. pengarah;

b. ketua tim; dan

c. anggota tim.

(3) Pengarah tim sebagaimana dimaksud pada ayat (2) huruf a dijabat oleh Asisten yang membidangi urusan administrasi pembangunan.

(4) Ketua tim sebagaimana dimaksud pada ayat (2) huruf b dijabat oleh Kepala Perangkat Daerah yang membidangi urusan komunikasi dan informatika.

(5) Anggota tim sebagaimana dimaksud pada ayat (2) huruf c terdiri dari seluruh Kepala Perangkat Daerah yang bertanggungjawab atas kepemilikan aset daerah yang berada di Perangkat Daerah, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Daerah.

Pasal 6

(1) Pelaksana Teknis Keamanan SPBE sebagaimana dimaksud dalam Pasal 5 ayat (2) dalam melaksanakan tugasnya dapat dibantu oleh Tim Operasional Keamanan SPBE.

(2) Susunan Pelaksana Tim Operasional Keamanan SPBE sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Sekretaris Daerah.

Pasal 7

Ketua tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah 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 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.

Pasal 8

Anggota tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf c mempunyai tugas:

a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada perangkat daerah yang dipimpinnya;

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 9

(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 10

(1) Program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 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 pada Pasal 9 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 11

(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 12

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 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 SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan SPBE.

(4) Teknologi keamanan informasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

(5) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 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 lingkungan.

(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.

BAB III

PENGENDALIAN TEKNIS KEAMANAN

Pasal 15

(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 *(risk register)* dengan ketentuan subtansi 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 2 ayat (3) huruf b disusun oleh ketua tim pelaksana teknis Keamanan SPBE.

(2) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen keamanan.

(3) 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 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.

(4) Prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) ditetapkan dengan Keputusan Walikota.

Pasal 17

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 15 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 18

(1) Untuk penanggulangan kejadian insidentil yang bersifat mendesak berupa insiden siber yang mengancam keamanan SPBE di Lingkup Pemerintah Daerah, dapat dibentuk Tim Tanggap Insiden Komputer atau *Computer Security Incident Response Team* (CSIRT).

(2) Ketua Tim sebagaimana dimaksud pada ayat (1) secara dijabat oleh Kepala Perangkat Daerah yang membidangi urusan komunikasi dan informatika.

(3) Susunan Tim sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Walikota.

Pasal 19

(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 kerjasama 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

KETENTUAN PENUTUP

Pasal 20

Peraturan Walikota ini berlaku pada tanggal diundangkan.

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

Ditetapkan di Blitar
pada tanggal 6 April 2023
WALIKOTA BLITAR,

ttd.

SANTOSO

Diundangkan di Blitar
Pada tanggal 6 April 2023
SEKRETARIS DAERAH KOTA BLITAR,

ttd.

PRIYO SUHARTONO

BERITA DAERAH KOTA BLITAR TAHUN 2023 NOMOR 26

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

IKA HADI WIJAYA, S.H.,M.H.
NIP. 19791210 200604 1 008