WALI KOTA PROBOLINGGO

PROVINSI JAWA TIMUR

SALINAN

PERATURAN WALI KOTA PROBOLINGGO
NOMOR 32 TAHUN 2022
TENTANG
MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK
DI LINGKUNGAN PEMERINTAH KOTA PROBOLINGGO

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA PROBOLINGGO

Menimbang :

a. bahwa untuk melaksanakan ketentuan Pasal 48 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik juncto 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 serta dalam rangka melaksanakan optimalisasi penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Probolinggo sehingga dapat mendukung terwujudnya tata kelola pemerintahan yang baik dan bersih, maka diperlukan Manajemen Keamanan Informasi;
b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Wali Kota tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Probolinggo;

Mengingat :

1. 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);

2. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234), sebagaimana telah diubah dengan Undang-Undang Nomor 15 Tahun 2019 (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 183, Tambahan Lembaran Negara Republik Indonesia Nomor 6398);
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 beberapa kali terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua atas Undang-Undang Nomor 23 Tahun 2014 (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
4. Peraturan Menteri Dalam Negeri Nomor 3 Tahun 2017 tentang Pedoman Pengelolaan Pelayanan Informasi dan Dokumentasi di Lingkungan Kementerian Dalam Negeri dan Pemerintahan Daerah (Berita Negara Republik Indonesia Tahun 2017 Nomor 157);
5. Peraturan Pemerintah Nomor 12 Tahun 2019 tentang Pengelolaan Keuangan Daerah (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 42, Tambahan Lembaran Negara Republik Indonesia Nomor 6322);
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 Menteri Komunikasi dan Informatika Nomor 10 Tahun 2015 tentang Tata Cara Pendaftaran Sistem Elektronik Instansi Penyelenggara Negara (Berita Negara Republik Indonesia Tahun 2015 Nomor 321);

8. 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);
9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
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;
11. Peraturan Daerah Kota Probolinggo Nomor 2 Tahun 2017 tentang Pembentukan Produk Hukum Daerah (Lembaran Daerah Kota Probolinggo Tahun 2017 Nomor 2, Tambahan Lembaran Daerah Kota Probolinggo Nomor 28);
12. Peraturan Daerah Kota Probolinggo Nomor 7 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kota Probolinggo Tahun 2016 Nomor 7, Tambahan Lembaran Daerah Kota Probolinggo Nomor 24) sebagaimana telah diubah dengan Peraturan Daerah Kota Probolinggo Nomor 5 Tahun 2019 tentang Perubahan Atas Peraturan Daerah Kota Probolinggo Nomor 7 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kota Probolinggo Tahun 2019 Nomor 5);

MEMUTUSKAN

Menetapkan : PERATURAN WALI KOTA TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KOTA PROBOLINGGO.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan :

1. Daerah adalah Kota Probolinggo.
2. Wali Kota adalah Walikota Probolinggo.
3. Pemerintah Daerah adalah Pemerintah Kota Probolinggo.

4. Perangkat Daerah adalah Perangkat Daerah di lingkungan Pemerintah Kota Probolinggo.
5. Dinas adalah Dinas Komunikasi dan Informatika Kota Probolinggo.
6. Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik yang berdiri sendiri atau dalam jaringan.
7. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
8. Informasi Elektronik adalah satu atau sekumpulan data elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *Electronic Data Interchange* (EDI), surat elektronik (*electronic mail*), telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
9. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) informasi.
10. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja dari layanan Sistem Elektronik.
11. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan Teknologi Informasi dan Komunikasi untuk memberikan layanan kepada Pengguna SPBE.
12. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, pengelolaan dan penyampaian atau pemindahan informasi antar sarana/media.

BAB II
MAKSUD DAN TUJUAN
Pasal 2

Peraturan Wali Kota ini dimaksudkan sebagai acuan bagi Pemerintah Daerah dalam menyelenggarakan proses Keamanan Informasi, yang meliputi :

a. perencanaan dan Program Kerja;
b. dukungan Pelaksanaan;
c. evaluasi Kinerja dan Perbaikan Berkelanjutan; dan
d. standar Pelaksanaan.

Pasal 3

Peraturan Wali Kota ini bertujuan untuk :

a. meningkatkan efektifitas dan efisiensi pelaksanaan program dan kegiatan di bidang Keamanan Informasi Elektronik;

b. sebagai acuan dalam penyusunan Standar Operasional Prosedur di bidang Keamanan Informasi Elektronik; dan
c. menciptakan harmonisasi dalam penyelenggaraan Keamanan Informasi Elektronik.

BAB III

AZAS PELAKSANAAN

Pasal 4

Sistem Keamanan Informasi Elektronik di lingkungan Pemerintah Daerah dilaksanakan berdasarkan azas-azas :

a. manfaat;
b. efektif;
c. efisien;
d. integrasi; dan
e. profesionalitas.

BAB IV

PERENCANAAN DAN PROGRAM KERJA

Pasal 5

Perencanaan Keamanan Informasi SPBE dilakukan dengan merumuskan :

a. program kerja keamanan SPBE yang disusun berdasarkan kategori Risiko Keamanan Informasi SPBE; dan
b. target realisasi program kerja Keamanan Informasi SPBE.

Pasal 6

Program Kerja Keamanan Informasi SPBE sebagaimana dimaksud dalam pasal 5 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.

Pasal 7

Edukasi Kesadaran Keamanan Informasi SPBE sebagaimana dimaksud dalam pasal 6 huruf a, dilaksanakan paling sedikit melalui kegiatan :

a. sosialisasi; dan
b. pelatihan.

Pasal 8

Penilaian Kerentanan Keamanan Informasi SPBE sebagaimana dimaksud dalam pasal 6 huruf b, dilaksanakan paling sedikit melalui :

a. inventarisasi seluruh aset SPBE, meliputi data dan informasi, aplikasi dan infrastruktur;
b. identifikasi kerentanan dan ancamanan terhadap aset SPBE; dan
c. pengukuran tingkat Risiko Keamanan Informasi SPBE.

Pasal 9

Peningkatan Keamanan Informasi SPBE sebagaimana dimaksud dalam pasal 6 huruf c, dilaksanakan berdasarkan hasil dari penilaian Kerentanan Informasi SPBE serta paling sedikit melalui :

a. penerapan standar teknis dan prosedur Keamanan Informasi SPBE; dan
b. pengujian fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 10

Penanganan Insiden Keamanan Informasi SPBE sebagaimana diamaksud dalam pasal 6 huruf d, dilaksanakan paling sedikit melalui :

a. identifikasi sumber serangan;
b. analisa informasi yang berkaitan dengan insiden selanjutnya;
c. penentuan prioritas penanganan insiden berdasarkan tingkat dampak yang terjadi;
d. pendokumentasian bukti insiden yang terjadi; dan
e. mitigasi atau mengurangi dampak resiko Keamanan Informasi SPBE.

Pasal 11

Audit Keamanan Informasi SPBE sebagaimana dimaksud dalam pasal 6 huruf e dilakukan sesuai dengan peraturan perundang-perundangan yang berlaku.

BAB V

DUKUNGAN PELAKSANAAN

Pasal 12

Dukungan terhadap pelaksanaan Manajemen Keamanan Informasi SPBE dilakukan dengan meningkatkan kapasitas terhadap :

a. Sumber Daya Manusia Keamanan Informasi SPBE; dan
b. anggaran Keamanan Informasi SPBE.

Pasal 13

(1) Sumber Daya Manusia Keamanan Informasi SPBE sebagaimana dimaksud dalam pasal 12 huruf a, paling sedikit harus memiliki kompetensi :

a. keamanan Infrastruktur Teknologi, informasi dan Komunikasi; dan
b. keamanan Aplikasi SPBE.

(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), dapat dilakukan melalui kegiatan :
a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur Teknologi, Informasi dan Komunikasi; dan
b. bimbingan teknis mengenai Kemananan Informasi SPBE.

Pasal 14

Anggaran Keamanan Informasi SPBE sebagaimana dimaksud dalam pasal 12 huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan peraturan perundang-perundangan.

BAB VI

EVALUASI KINERJA

Pasal 15

(1) Evaluasi kinerja dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun terhadap pelaksanaan Keamanan Informasi SPBE;

(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan dengan :
a. mengidentifikasi area proses yang memiliki Risiko tinggi terhadap keberhasilan pelaksanaan Keamanan Informasi SPBE;
b. menetapkan indikator kinerja pada setiap area proses;
c. memformulasi pelaksanaan Keamanan Informasi SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
d. menganalisa efektifitas pelaksanaan Keamanan Informasi SPBE; dan
e. mendukung serta merealisasikan program Audit Keamanan Informasi SPBE.

(3) Tindak lanjut dari hasil evaluasi kinerja adalah Perbaikan Berkelanjutan, yang dilakukan dengan :
a. mengatasi permasalahan dalam pelaksanaan Keamananan Informasi SPBE; dan
b. memperbaiki pelaksanaan Keamanan Informasi SPBE secara periodik.

BAB VII

STANDAR TEKNIS KEAMANAN INFORMASI SPBE

Pasal 16

Pemerintah Daerah harus menerapkan Keamanan Informasi SPBE yang memenuhi standar teknis Keamanan Informasi SPBE.

Pasal 17

Standar teknis Keamanan Informasi SPBE sebagaimana dimaksud dalam pasal 16 diterapkan untuk :

a. keamanan data dan informasi SPBE;
b. keamanan Aplikasi SPBE;
c. keamanan sistem penghubung layanan SPBE; dan
d. keamanan jaringan intra SPBE.

Pasal 18

Standar teknis keamanan data dan informasi SPBE sebagaimana dimaksud dalam pasal 17 huruf a, terdiri atas terpenuhinya aspek :

a. kerahasiaan;
b. keaslian;
c. keutuhan;
d. kenirsangkalan; dan
e. ketersediaan.

Pasal 19

(1) Standar teknis Keamanan Aplikasi SPBE sebagaimana dimaksud dalam pasal 17 huruf b, diterapkan pada :
    a. aplikasi berbasis web, yaitu aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet; dan
    b. aplikasi berbasis *mobile*, yaitu aplikasi yang dalam pengoperasiannya dapat berjalan di perangkat bergerak dan memiliki sistem operasi yang mendukung Perangkat Lunak secara *standalone*.
(2) Standar teknis Keamanan Aplikasi SPBE sebagaimana dimaksud pada ayat (1) harus dilakukan pengujian keamanan setiap periode tertentu yang dilakukan, dengan :
    a. mengidentifikasi persyaratan minimum keamanan yang belum diterapkan ;
    b. memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan;
    c. melakukan pemindaian otomatis dan/atau pengujian penetrasi sistem;
    d. mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan Aplikasi SPBE; dan
    e. menganalisa kerentanan.
(3) Standar teknis keamanan aplikasi berbasis web sebagaimana dimaksud pada ayat (1) huruf a, terdiri atas terpenuhinya fungsi :
    a. autentikasi;
    b. manajemen sesi;
    c. persyaratan kontrol Akses;

d. validasi input;
e. kriptografi pada verifikasi statis;
f. penanganan *error* dan pencatatan log;
g. proteksi data;
h. keamanan komunikasi;
i. pengendalian kode berbahaya;
j. logika bisnis;
k. file;
l. keamanan API dan web *service*; dan
m. keamanan konfigurasi.

(4) Standar teknis keamanan Aplikasi Berbasis *Mobile* sebagaimana dimaksud pada ayat (1) huruf b, terdiri atas terpenuhinya fungsi :
a. penyimpanan Data dan Persyaratan Privasi ;
b. kriptografi;
c. autentikasi dan manajemen Sesi;
d. komunikasi jaringan;
e. interaksi *platform*;
f. kualitas kode dan pengaturan *build*; dan
g. ketahanan.

Pasal 20

Standar teknis keamanan sistem penghubung layanan SPBE sebagaimana dimaksud dalam pasal 17 huruf c, terdiri atas terpenuhinya fungsi :
a. keamanan Interoperabilitas Data dan Informasi;
b. kontrol Sistem Integrasi;
c. kontrol Perangkat Integrator;
d. keamanan API dan *Web Service*; dan
e. keamanan Migrasi Data.

Pasal 21

Standar teknis keamanan jaringan Intra sebagaimana dimaksud dalam pasal 17 huruf d, terdiri atas terpenuhinya fungsi :
a. aspek Administrasi Keamanan Jaringan Intra;
b. kontrol Akses dan Autentifikasi;
c. persyaratan Perangkat dan Aplikasi Keamanan Jaringan Intra;
d. kontrol Keamanan *Gateaway*;
e. kontrol Keamanan *Acces Point* pada Jaringan Nirkabel; dan
f. kontrol Konfigurasi *Acces Point* pada Jaringan Nirkabel.

BAB VI

KETENTUAN LAIN – LAIN

Pasal 22

Standar Operasional Prosedur yang belum diatur dalam Peraturan ini akan ditetapkan oleh Kepala Dinas sesuai ketentuan peraturan perundang-undangan.

BAB VII

KETENTUAN PENUTUP

Pasal 23

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 Probolinggo.

Ditetapkan di Probolinggo
pada tanggal 6 April 2022
WALI KOTA PROBOLINGGO,

Ttd,

HADI ZAINAL ABIDIN

Diundangkan di Probolinggo
pada tanggal 6 April 2022
SEKRETARIS DAERAH KOTA PROBOLINGGO,

Ttd,

NINIK IRA WIBAWATI

BERITA DAERAH KOTA PROBOLINGGO TAHUN 2022 NOMOR 32

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

DENNY BAGUS ERWANTO, S.H., M.H
NIP. 19780608 200903 1 004