SALINAN

WALIKOTA JAMBI

PROVINSI JAMBI

PERATURAN WALIKOTA JAMBI

NOMOR 22 TAHUN 2022

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAHAN KOTA JAMBI

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALIKOTA JAMBI,

Menimbang :

a. bahwa dalam rangka melindungi kerahasiaan, keutuhan dan ketersediaan aset informasi di Pemerintah Kota Jambi yang diselenggarakan berbasis elektronik dari berbagai ancaman keamanan informasi baik dari dalam maupun luar, perlu melakukan pengelolaan keamanan informasi;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a, perlu menetapkan Peraturan Walikota Jambi tentang Sistem Manajemen Keamanan Informasi Pemerintahan Kota Jambi.

Mengingat :

1. Undang – Undang Nomor 9 Tahun 1956 tentang Pembentukan Daerah Otonom Kota Besar Dalam Lingkungan Daerah Propinsi Sumatera Tengah (Lembaran Negara Republik Indonesia Tahun 1956 Nomor 20);

2. Undang – Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154 Tambahan Lembaran Negara Republik Indonesia Nomor 3881);

3. Undang – Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112 Tambahan Lembaran Negara Republik Indonesia Nomor 5038);

4. Undang-Undang Republik Indonesia Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 6, Tambahan Lembaran Negara Republik Indonesia Nomor 5494);

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 di ubah 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);
6. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
7. Peraturan Daerah Kota Jambi Nomor 14 Tahun 2016 tentang Pembentukan dan Sususan Perangkat Daerah (Lembaran Daerah Kota Jambi Tahun 2016 Nomor 14);
8. Peraturan Walikota Jambi Nomor 10 Tahun 2017 tentang Pemanfaatan Teknologi Informasi dan Komunikasi (BeritaDaerah Kota Jambi Tahun 2017 Nomor 10);

MEMUTUSKAN :

Menetapkan : PERATURAN WALIKOTA TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAHAN KOTA JAMBI

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan:

1. Daerah adalah Kota Jambi.
2. Walikota adalah Walikota Jambi.
3. Sekretaris Daerah adalah Sekretaris Daerah Kota Jambi.
4. Perangkat Daerah adalah unsur Pembantu Walikota dalam Penyelenggaraan Pemerintahan yang terdiri dari Sekretariat Daerah, Staf Ahli Walikota, Sekretariat DPRD, Inspektorat, Dinas Daerah, Badan Perencanaan Pembangunan Daerah, Badan Pengelolaan Keuangan dan Aset Daerah, Badan Kepegawaian Pendidikan dan Pelatihan, Lembaga Teknis Daerah, Kecamatan/Kelurahan dan Lembaga Lain.
5. Sistem adalah suatu kesatuan yang terdiri komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran informasi, materi atau energi untuk mencapai suatu tujuan.

6. Informasi adalah keterangan, pernyataan, gagasan, dan tanda tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non elektronik.
7. Keamanan Informasi adalah suatu kondisi dimana terjaganya aspek kerahasiaan, integritas dan ketersediaan dari informasi.
8. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko.
9. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
10. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
11. Komputer adalah alat untuk memproses data elektronik, mengetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan menyimpan.
12. Perangkat Lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian sistem elektronik.
13. Aset Informasi adalah unit informasi yang dapat dipahami dibagi, dilindungi dan dimanfaatkan secara efektif.
14. Aset Pengolahan Informasi adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi.
15. Penyimpanan Informasi adalah suatu proses menyimpan informasi dengan menggunakan media baik elektronik maupun non-elektronik.
16. *Data Center* adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti sistem komunikasi data dan penyimpanan data.

Pasal 2

(1) Maksud ditetapkannya Peraturan Walikota ini adalah sebagai pedoman pengelolaan SMKI secara terpadu untuk memastikan terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).

(2) Pengelolaan SMKI sebagaimana dimaksud pada ayat (1) meliputi infrastruktur komputer, jaringan, system informasi/aplikasi, dan sumber daya manusia.

BAB II

RUANG LINGKUP

Pasal 3

Ruang lingkup pengamanan informasi yang diatur dalam Peraturan Walikota ini meliputi:

a. aset informasi;

b. aset pengolahan informasi; dan

c. penyimpanan informasi.

Bagian Kesatu

Aset Informasi

Pasal 4

Aset Informasi sebagaimana dimaksud dalam Pasal 3 huruf a meliputi informasi yang tercetak, tertulis, dan tersimpan dalam bentuk

a. fisik, seperti:
    1. kertas;
    2. papan tulis;
    3. spanduk; dan
    4. buku atau dokumen.
b. elektronik, seperti:
    1. *database* dan *file* di dalam komputer;
    2. informasi yang ditampilkan pada *website*, layar komputer; dan
    3. informasi yang dikirimkan melalui jaringan telekomunikasi.

Bagian Kedua

Aset Pengolahan Informasi

Pasal 5

Aset Pengolahan Informasi sebagaimana dimaksud dalam Pasal 3 huruf b berupa:

a. peralatan mekanik yang digerakkan dengan tangan secara manual; dan

b. peralatan elektronik yang bekerja secara elektronik penuh.

Bagian Ketiga

Penyimpanan Informasi

Pasal 6

Penyimpanan Informasi sebagaimana dimaksud dalam Pasal 3 huruf c menggunakan media:

a. elektronik, meliputi antara lain:

1. *server*,
2. *hard disk*,
3. *flash disk*,
4. kartu memori, dan lain-lain.

b. non-elektronik, meliputi antara lain:

1. lemari,
2. rak,
3. laci,
4. *filling cabinet*, dan lain-lain.

BAB III

KOORDINATOR KEAMANAN TEKNOLOGI INFORMASI

Pasal 7

(1) Untuk melakukan pengamanan informasi sebagaimana dimaksud dalam Pasal 3, setiap Perangkat Daerah memiliki Koordinator Keamanan Teknologi Informasi.

(2) Koordinator Keamanan Teknologi Informasi sebagaimana dimaksud pada ayat (1) bertanggungjawab memastikan Teknologi Informasi yang digunakan mendukung proses tata kelola pemerintahan dan pencapaian tujuan organisasi.

(3) Koordinator Keamanan Teknologi Informasi sebagaimana dimaksud pada ayat (2) memiliki wewenang:

a. menyusun prosedur penyelenggaraan Keamanan Informasi yang diterapkansecara efektif baik bagi Perangkat Daerah maupun pengguna; dan

b. melakukan evaluasi kinerja penyelenggaraan Teknologi Informasi.

(4) Koordinator Keamanan Informasi sebagaimana dimaksud pada ayat (3) dijabat oleh Pejabat struktural yang membawahi penyelenggaraan Teknologi Informasi.

BAB IV

MANAJEMEN RISIKO

Pasal 8

(1) Setiap Perangkat Daerah penyelenggara Teknologi Informasi wajib melakukan proses manajemen risiko dalam menerapkan SMKI.

(2) Proses manajemen risiko sebagaimana dimaksud pada ayat (1) meliputi:

a. identifikasi;

b. pengukuran;

c. pemantauan; dan

d. pengendalian atas risiko terkait penggunaan Teknologi Informasi.

(3) Manajemen risiko sebagaimana dimaksud pada ayat (2) mencakup:

a. pengembangan sistem;

b. operasional Teknologi Informasi;

c. jaringan komunikasi;

d. penggunaan perangkat komputer;

e. pengendalian terhadap informasi; dan

f. penggunaan pihak ketiga sebagai penyedia jasa Teknologi Informasi.

(4) Penerapan manajemen risiko harus dilakukan secara terintegrasi pada setiap penggunaan operasional Teknologi Informasi terkait sistem yang digunakan.

BAB V

SUMBER DAYA

Pasal 9

Pimpinan Perangkat Daerah menyediakan sumber daya yang dibutuhkan untuk membentuk mengimplemteasikan, memelihara dan meningkatkan penerapan SMKI secara berkesinambungan.

BAB VI

STANDAR DAN PROSEDUR PENGENDALIAN

Pasal 10

(1) Setiap Perangkat Daerah harus menyusun standar dan prosedur pengendalian kegiatan teknologi informasi yang memenuhi prasyarat keamanan informasi dan untuk mengimplementasikan tindakan dalam mengelola risiko.

(2) Prasyarat keamanan informasi sebagaimana dimaksud pada ayat (1) meliputi aspek sebagai berikut:

a. organisasi keamanan informasi;

b. keamanan sumber daya manusia;

c. pengelolaan aset;

d. pengendalian akses;

e. kriptografi;

f. keamanan fisik dan lingkungan;

g. keamanan operasional;

h. keamanan komunikasi;

i. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;

j. hubungan kerja dengan pemasok (*supplier*);

k. penanganan insiden keamanan informasi;

l. kelangsungan usaha; dan

m. kepatuhan.

Pasal 11

(1) Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional Teknologi Informasi yang stabil dan aman.

(2) Penyelenggaraan pemrosesan transaksi pada operasional teknologi informasi harus memenuhi prinsip kehati-hatian.

(3) Setiap Perangkat Daerah penyelenggara teknologi informasi wajib mengidentifikasi dan memantau aktivitas operasional Teknologi Informasi untuk memastikan efektifitas, efesiensi, dan keamanan dari aktivitas tersebut antara lain dengan:

a. menerapkan perimeter fisik dan lingkungan di area kerja dan *Data Center*;

b. mengendalikan hak akses secara memadai sesuai kewenangan yang ditetapkan;

c. menerapkan pengendalian terhadap informasi yang diproses;

d. memastikan ketersediaan dan kecukupan kapasitas layanan jaringan komunikasi baik yang dikelola secara internal maupun oleh pihak lain penyedia jasa;

e. melakukan pemantauan kegiatan operasional Teknologi Informasi termasuk *audit trail*; dan

f. melakukan pemantauan terhadap aplikasi yang digunakan oleh Perangkat Daerah maupun pengguna.

BAB VII

MEKANISME PENYELENGGARAAN

Pasal 12

(1) Setiap Perangkat Daerah penyelenggara tekonologi informasi harus memastikan ketersediaan data dan sistem dalam rangka menjaga kelangsungan teknologi informasi melalui penyelenggaraan fasilitas *Data Center* baik dikelola oleh internal maupun oleh pihak penyedia jasa.

(2) Setiap aktivitas pada fasilitas di *Data Center* harus dapat terpantau guna menghindari kesalahan proses pada sistem dan memperhatikan aspek perlindungan terhadap data yang diproses dan lingkungan fisik.

Pasal 13

(1) Perangkat Daerah harus menerapkan prinsip pengendalian terhadap aktivitas Teknologi Informasi melalui proses evaluasi dan monitoring secara berkala.

(2) Setiap Perangkat Daerah wajib melakukan kegiatan pemantauan dan tindakan koreksi penyimpangan terhadap kendali keamanan informasi yang meliputi:

a. kegiatan pemantauan secara terus menerus; dan

b. pelaksanaan fungsi pemeriksaan intern yang efektif dan menyeluruh.

(3) Perangkat Daerah Penyelenggara Teknologi Informasi berdasarkan hasil *audit*, umpan balik, maupun evaluasi terhadap pengendalian keamanan informasi yang dilakukan, meningkatkan efektivitas sistem manajemen keamanan informasi secara berkesinambungan melalui perbaikan terhadap akibat penyimpangan kegiatan teknologi informasi.

(4) Hasil dari tindakan perbaikan dan peningkatan sebagaimana dimaksud pada ayat (3) harus dilaporkan kepada Kepala Perangkat Daerah dan didokumentasikan sebagai bagian dari proses *lesson learned* bagi Perangkat Daerah.

Pasal 14

(1) Apabila terjadi kebocoran informasi pada instansi terkait yang berdampak sangat luas, maka Pemerintah Kota Jambi dapat menunjuk auditor independen untuk melakukan investigasi yang diperlukan.

(2) Perangkat Daerah Penyelenggara Teknologi Informasi wajib menyediakan akses kepada auditor independen sebagaimana dimaksud pada ayat (1) untuk melakukan Pemeriksaan seluruh aspek terkait penyelenggaraan Teknologi Informasi.

BAB VIII

KETENTUAN PENUTUP

Pasal 15

Peraturan Walikota ini mulai berlaku pada tanggal diundangkan.

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

Dietapkan di Jambi

Pada Tanggal, 23 September 2022

WALIKOTA JAMBI

ttd

SYARIF FASHA

Diundangkan di Jambi

Pada Tanggal, 23 September 2022

SEKRETARIS DAERAH KOTA JAMBI

ttd

A. RIDWAN

Salinan Sesuai Dengan Aslinya
Plt. KEPALA BAGIAN HUKUM
SETDA KOTA JAMBI

ttd

SAHAT MARULI TUA, SH
Penata Tk.I
NIP. 19680203 199402 1 002

BERITA DAERAH KOTA JAMBI TAHUN 2022 NOMOR 22