WALIKOTA BATAM

PERATURAN WALIKOTA BATAM

NOMOR TAHUN 2022

TENTANG

PENYELENGGARAAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KOTA BATAM

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALIKOTA BATAM,

Menimbang:

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

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Walikota tentang Penyelenggaraan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kota Batam;

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 Djawa Timur, Djawa Tengah, Djawa Barat, dan Daerah Istimewa Jogjakarta (Lembaran Negara Republik Indonesia Tahun 1955 Nomor 53, Tambahan Lembaran Negara Republik Indonesia Nomor 859);

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);

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 diubah 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 Menteri Komunikasi dan Informatika Nomor 41/PER/M.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional;
7. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi;
8. 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.

MEMUTUSKAN:

Menetapkan: PERATURAN WALIKOTA TENTANG PENYELENGGARAAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KOTA BATAM.

BAB 1

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan:

1. Sistem adalah suatu kesatuan yang terdiri komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran informasi, materi atau energi untuk mencapai suatu tujuan.
2. 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.
3. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
4. Keamanan Informasi SPBE adalah pengendalian keamanan yang terpadu dalam SPBE untuk terjaganya aspek kerahasiaan, integritas dan ketersediaan dari informasi.
5. Sistem Manajemen Keamanan Informasi SPBE yang selanjutnya di singkat SMKI SPBE adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
6. Teknologi Informasi dan Komunikasi, yang selanjutnya disingkat TIK adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, membuat laporan, menganalisis, memindahkan informasi dan/atau menyebarkan informasi antar media.
7. Komputer adalah alat untuk memproses data elektronik, mengetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan menyimpan.
8. Perangkat Lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian sistem elektronik.
9. Aset Informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
10. Aset Pengolahan Informasi adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi.
11. Penyimpanan Informasi adalah suatu proses menyimpan informasi dengan menggunakan media baik elektronik maupun non-elektronik.

12. *Data Center* atau Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
13. Walikota adalah Walikota Batam.
14. Daerah adalah Kota Batam.
15. Sekretaris Daerah adalah Sekretaris Daerah Kota Batam.
16. Perangkat Daerah adalah Perangkat Daerah di lingkungan Pemerintah Kota Batam.
17. Rencana Pemulihan Bencana atau *Disaster Recovery Plan* (DRP) adalah dokumen yang berisikan rencana tindak lanjut yang diperlukan guna pemulihan layanan SPBE setelah terdampak bencana.
18. Rencana Bisnis Berkelanjutan atau *Business Continuity Plan* (BCP) adalah dokumen yang berisikan rencana dan *framework* untuk menjamin bahwa proses bisnis dapat terus berlanjut dalam keadaan emergensi.

BAB II

MAKSUD, TUJUAN DAN RUANG LINGKUP

Pasal 2

(1) Maksud ditetapkannya Peraturan Walikota ini sebagai pedoman bagi Pemerintah Kota Batam dalam melaksanakan kebijakan, program dan kegiatan SMKI SPBE untuk pengamanan informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Batam.

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

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

Pasal 3

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

a. aset Informasi;

b. aset Pengolahan Informasi; dan

c. penyimpanan 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 situs *web*, layar komputer; dan
    3. informasi yang dikirimkan melalui jaringan telekomunikasi.

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.

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

PENANGGUNG JAWAB DAN PELAKSANA TEKNIS

Pasal 7

(1) Sekretaris Daerah adalah penanggung jawab pelaksanaan Sistem Manajemen Keamanan Informasi SPBE di Lingkungan Pemerintah Kota Batam.

(2) Penanggung jawab sebagaimana dimaksud dalam ayat (1) disebut dengan Koordinator.

(3) Koordinator secara berkala melaporkan pelaksanaan Sistem Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Kota Batam secara berkala kepada Walikota.

(4) Dalam melaksanakan tanggung jawabnya Koordinator dibantu oleh Pelaksana Teknis Keamanan Informasi SPBE.

(5) Pelaksana Teknis Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (4) terdiri atas:

a. Kepala Dinas Komunikasi dan Informatika sebagai pejabat pimpinan tinggi pratama;

b. Sekretaris Dewan / Direktur BUMD / Wakil Direktur RSUD / Sekretaris Perangkat Daerah / Kepala Bagian Sekretariat Daerah / Sekretaris Camat sebagai pejabat pimpinan tinggi atau pejabat administrator.

Pasal 8

(1) Pejabat pimpinan tinggi pratama mempunyai tugas:

a. menyusun dan membuat dokumen Rencana Bisnis Berkelanjutan atau *Business Continuity Plan* (BCP) dan Rencana Pemulihan Bencana atau *Disaster Recovery Planning* (DRP);

b. memastikan penerapan standar teknis dan prosedur Keamanan Informasi SPBE;

c. merumuskan, mengkoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Informasi SPBE; dan

d. melaporkan pelaksanaan manajemen keamanan informasi SPBE dan penerapan standar teknis dan prosedur Keamanan Informasi SPBE kepada Koordinator.

(2) Pejabat pimpinan tinggi atau pejabat administrator mempunyai tugas:

a. menerapkan standar teknis dan prosedur keamanan aplikasi di unit kerja masing-masing;

b. memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan Informasi SPBE yang telah ditetapkan;

c. memastikan keberlangsungan proses bisnis SPBE; dan

d. berkoordinasi dengan pejabat pimpinan tinggi pratama yang terkait dengan pelaksanaan dan perumusan program kerja serta anggaran Keamanan Informasi SPBE.

BAB IV

PERENCANAAN

Pasal 9

(1) Pelaksana Teknis Keamanan Informasi SPBE wajib menyusun rencana dan program peningkatan keamanan informasi untuk jangka pendek, menengah dan panjang.

(2) Penyusunan perencanaan dengan merumuskan:

a. Program kerja Keamanan Informasi SPBE yang disusun berdasarkan kategori risiko atau manajemen risiko Keamanan Informasi SPBE.

b. Target realisasi program kerja Keamanan Informasi SPBE.

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

a. identifikasi;

b. pengukuran;

c. pemantauan; dan

d. pengendalian atas risiko terkait penggunaan TIK.

(4) Manajemen risiko SPBE sebagaimana dimaksud pada ayat (3) mencakup:

a. pengadaan dan pengembangan sistem;

b. operasional TIK;

c. jaringan komunikasi;

d. penggunaan perangkat komputer;

e. pengendalian terhadap informasi; dan

f. penggunaan pihak ketiga sebagai penyedia jasa TIK.

(5) Penerapan manajemen risiko SPBE harus dilakukan secara terintegrasi pada setiap penggunaan operasional TIK terkait sistem yang digunakan.

Pasal 10

Perencanaan sebagaimana dimaksud dalam pasal 9 dibuat Pelaksana Teknik Keamanan Informasi SPBE dalam dokumen Kebijakan Keamanan Informasi SPBE Pimpinan Tinggi Pratama.

BAB V

DUKUNGAN PENGOPERASIAN

Pasal 11

(1) Pimpinan Perangkat Daerah menyediakan sumber daya yang dibutuhkan untuk membentuk, mengimplementasikan memelihara, dan meningkatkan penerapan SMKI SPBE secara berkesinambungan.

(2) Sumber daya sebagaimana dimaksud ayat 1 dapat berupa sumber daya manusia, peralatan dan perlengkapan.

Pasal 12

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

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

a. organisasi keamanan informasi SPBE;

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 SPBE;

l. kelangsungan usaha; dan

m. kepatuhan.

Pasal 13

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

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

(3) Setiap Perangkat Daerah penyelenggara TIK wajib mengidentifikasi dan memantau aktivitas operasional TIK untuk memastikan efektifitas, efisiensi, 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 TIK termasuk audit trail; dan

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

Pasal 14

(1) Setiap Perangkat Daerah penyelenggara TIK harus memastikan ketersediaan data dan sistem dalam rangka menjaga kelangsungan TIK 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 15

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

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

BAB VI

EVALUASI KINERJA

Pasal 16

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

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

a. kegiatan pemantauan secara terus menerus; dan

b. pelaksanaan fungsi pemeriksaan intern yang efektif dan menyeluruh.

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

(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.

BAB VII

PERBAIKAN BERKELANJUTAN

Pasal 17

(1) Pejabat Tinggi Pratama menyusun Rencana Bisnis Berkelanjutan atau *Business Continuity Plan* (BCP) serta melakukan pengujian Rencana Bisnis Berkelanjutan secara berkala;

(2) Pejabat Tinggi Pratama memastikan Layanan SPBE dapat berlangsung atau dipulihkan sesuai dengan batas waktu yang ditentukan; dan

(3) Pejabat Tinggi Pratama memastikan Rencana Bisnis Berkelanjutan atau *Business Continuity Plan* (BCP) dapat berfungsi sebagai Pusat Data kedua dalam mendukung proses bisnis.

Pasal 18

(1) Pejabat Tinggi Pratama menyusun Rencana Pemulihan Bencana atau *Disaster Recovery Plan* (DRP) serta melakukan pengujian Rencana Pemulihan Bencana secara berkala;

(2) Pejabat Tinggi Pratama memastikan Layanan SPBE dapat berlangsung atau dipulihkan sesuai dengan batas waktu yang ditentukan; dan

(3) Pejabat Tinggi Pratama memastikan Rencana Pemulihan Bencana atau *Disaster Recovery Plan* (DRP) dapat berfungsi sebagai Pusat Data kedua dalam mendukung proses bisnis.

Pasal 19

Peraturan Walikota ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Batam pada tanggal

Juni 2022

WALIKOTA BATAM,

Ttd

MUHAMMAD RUDI