WALI KOTA TANJUNGPINANG
PROVINSI KEPULAUAN RIAU

PERATURAN WALI KOTA TANJUNGPINANG
NOMOR 58 TAHUN 2023

TENTANG

PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA
WALI KOTA TANJUNGPINANG,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 39 ayat (5) Peraturan Wali Kota Nomor 8 Tahun 2022 tentang Pedoman Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik, perlu ditetapkan Peraturan Wali Kota tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 5 Tahun 2001 tentang Pembentukan Kota Tanjungpinang (Lembaran Negara Republik Indonesia Tahun 2001 Nomor 85, Tambahan Lembaran Negara Republik Indonesia Nomor 4112);
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 diubah beberapa kali, terakhir dengan Undang-Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan antara Pemerintah Pusat dan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6757);
6. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601).
7. Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia nomor 6856);
8. 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);
9. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
10. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);

11. 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);
12. 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):
13. 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);
14. 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 (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
15. Peraturan Daerah Kota Tanjungpinang Nomor 11 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Tanjungpinang (Lembaran Daerah Kota Tanjungpinang Tahun 2016 Nomor 11) sebagaimana telah diubah dengan Peraturan Daerah Kota Tanjungpinang Nomor 6 Tahun 2020 tentang Perubahan Kedua Atas Peraturan Daerah Kota Tanjungpinang Nomor 11 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Tanjungpinang (Lembaran Daerah Kota Tanjungpinang Tahun 2020 Nomor 44);
16. Peraturan Wali Kota Tanjungpinang Nomor 8 Tahun 2022 tentang Pedoman Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kota Tanjungpinang Tahun 2022 Nomor 402);

MEMUTUSKAN:

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

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:

1. Daerah adalah Kota Tanjungpinang.
2. Pemerintah Daerah adalah Pemerintah Kota Tanjungpinang.
3. Wali Kota adalah Wali Kota Tanjungpinang.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Tanjungpinang.
5. Perangkat Daerah adalah unsur pembantu kepala Daerah dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
6. Dinas adalah perangkat daerah yang menyelenggarakan urusan pemerintah daerah di bidang komunikasi, informatika, statistik dan persandian.
7. Komunikasi adalah penyampaian informasi dari satu pihak ke pihak yang lain melalui media perantara yang bersifat elektronik maupun non elektronik.
8. Informatika adalah pemanfaatan perangkat-perangkat berkemampuan komputasi dalam pengelolaan informasi, termasuk dalam pemrosesan, pengarsipan dan penyebaran informasi.
9. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
10. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
11. 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.

12. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
13. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan (*confidentiality*) atas informasi dan komunikasi secara Elektronik.
14. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas Informasi Elektronik.
15. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas Informasi Elektronik.
16. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
17. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
18. 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.
19. Pihak Ketiga adalah semua unsur di luar pengguna unit Teknologi Informasi dan Komunikasi Pemerintah Kota Tanjungpinang yang bukan bagian dari Pemerintah Kota Tanjungpinang seperti konsultan, penyedia jasa komunikasi, pemasok dan pemelihara perangkat pengolah informasi.

Pasal 2

(1) Maksud dari Peraturan Wali Kota ini adalah sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah.

(2) Tujuan dari Peraturan Wali Kota ini adalah sebagai panduan bagi seluruh Perangkat Daerah, unit kerja dan pegawai dalam pelaksanaan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Daerah.

(3) Ruang Lingkup Peraturan Wali Kota ini meliputi:
   a. kebijakan Internal Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik; dan
   b. pengendalian Teknis Keamanan.

BAB II

KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Pasal 3

(1) Kebijakan internal manajemen keamanan informasi SPBE meliputi:
   a. penetapan ruang lingkup;
   b. penetapan penanggung jawab;
   c. perencanaan;
   d. dukungan pengoperasian;
   e. evaluasi kinerja; dan
   f. perbaikan berkelanjutan terhadap keamanan informasi.

(2) Untuk mendukung kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) dapat menerapkan pengendalian teknis keamanan yang meliputi:
   a. manajemen risiko;
   b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
   c. pengelolaan pihak ketiga.

(3) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) huruf a meliputi:
   a. data dan informasi SPBE;
   b. aplikasi SPBE; dan
   c. infrastruktur SPBE.

(4) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (3) merupakan aset Pemerintah Daerah yang harus diamankan dalam SPBE.

Pasal 4

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf b dilaksanakan atau ditetapkan oleh Wali Kota.

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

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

Pasal 5

(1) Sekretaris Daerah 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. ketua tim; dan
    b. anggota tim.
(3) Ketua Tim sebagaimana dimaksud pada ayat (2) huruf a dapat dijabat oleh Kepala Dinas.
(4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh pimpinan perangkat daerah lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Daerah.
(5) Pelaksana Teknis Keamanan SPBE dan tugas sebagaimana dimaksud pada ayat (2) ditetapkan dengan Keputusan Sekretaris Daerah.

Pasal 6

(1) Perencanaan sebagaimana dimaksud dalam Pasal 3 ayat (1) 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 7

(1) Program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 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 dalam Pasal 6 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 8

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 3 ayat (1) 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 9

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 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 8 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.
(5) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 10

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 ayat (1) 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 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 11

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 3 ayat (1) 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 12

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 3 ayat (2) 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 13

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 3 ayat (2) huruf b ditetapkan oleh Ketua Tim pelaksana teknis Keamanan SPBE.

(2) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah dengan cakupan aspek 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.

(3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk keputusan Wali Kota.

Pasal 14

(1) Setiap perangkat daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 13 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 15

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

BAB IV

KETENTUAN PENUTUP

Pasal 16

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 Tanjungpinang.

Ditetapkan di Tanjungpinang
pada tanggal18 September 2023
WALI KOTA TANJUNGPINANG,

**ttd.**

RAHMA

Diundangkan di Tanjungpinang
pada tanggal 18 September 2023
SEKRETARIS DAERAH,

**ttd.**

ZULHIDAYAT

BERITA DAERAH KOTA TANJUNGPINANG TAHUN 2023 NOMOR 492

Salinan ini sesuai dengan aslinya,
KEPALA BAGIAN HUKUM

LIA ADHAYATNI, SH.,MH
Pembina
NIP. 19781109 200604 2 021