WALI KOTA TANJUNGPINANG
PROVINSI KEPULAUAN RIAU

PERATURAN WALI KOTA TANJUNGPINANG
NOMOR 57 TAHUN 2023

TENTANG

PEDOMAN PENYELENGGARAAN PERSANDIAN
UNTUK PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA TANJUNGPINANG,

Menimbang :

a. bahwa dalam rangka melindungi informasi di lingkungan Pemerintah Kota Tanjungpinang perlu dilakukan pengaturan sebagai upaya pengamanan melalui pelaksanaan persandian;

b. bahwa untuk melaksanakan ketentuan Pasal 4 ayat (1) Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Daerah, menyebutkan penyelenggaraan persandian untuk pengamanan informasi pemerintah daerah provinsi dan kabupaten/kota salah satunya dilaksanakan melalui penyusunan kebijakan pengamanan informasi;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Wali Kota tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi;

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar 1945 Negara Republik Indonesia;

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. Peraturan Pemerintah Nomor 12 Tahun 2017 tentang Pembinaan dan Pengawasan Penyelenggaraan Pemerintah Daerah (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 73, Tambahan Lembaran Negara Republik Indonesia Nomor 6041);
7. 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);
8. Peraturan Presiden Nomor 79 Tahun 2008 tentang Tunjangan Pengamanan Persandian;

9. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah diubah dengan Permendagri Nomor 120 Tahun 2018 tentang perubahan atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2018 Nomor 157);
10. Peraturan Menteri Pemberdayaan Aparatur Negara dan Reformasi Birokrasi Nomor 18 Tahun 2019 tentang Jabatan Fungsional Sandiman (Berita Negara Republik Indonesia Tahun 2019 Nomor 1010);
11. 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);
12. 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);

MEMUTUSKAN

Menetapkan: PERATURAN WALI KOTA TENTANG PEDOMAN PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

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. Perangkat Daerah adalah unsur pembantu Kepala Daerah dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
5. Dinas adalah perangkat daerah yang menyelenggarakan urusan pemerintah daerah di bidang komunikasi, informatika, statistik dan persandian.
6. Persandian adalah kegiatan di bidang pengamanan data/informasi yang dilaksanakan dengan menerapkan konsep, teori, seni dan ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terkait pada etika profesi sandi.
7. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.
8. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
9. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
10. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik.
11. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
12. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
13. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
14. Tunjangan Pengamanan Persandian yang selanjutnya di singkat TPP adalah tunjangan khusus yang diberikan kepada Pegawai Negeri yang diangkat dan ditugaskan secara penuh sesuai dengan ketentuan

peraturan perundang-undangan sebagai pengelola pengamanan persandian di lingkungan instansi pemerintah pusat dan daerah, sebagai bentuk kompensasi atas tanggung jawab dalam melaksanakan tugas di bidang penyelenggaraan pengamanan persandian.

Pasal 2

(1) Maksud dari Peraturan Wali Kota ini adalah sebagai pedoman bagi Pemerintah Daerah dalam melaksanakan kebijakan, program, dan kegiatan penyelenggaraan persandian untuk pengamanan informasi.
(2) Tujuan Pembentukan Peraturan Wali Kota ini adalah:
    a. menciptakan harmonisasi dalam pembagian urusan pemerintahan di bidang persandian;
    b. sebagai acuan tata cara penyelenggaraan persandian untuk pengamanan informasi di lingkungan Pemerintah Daerah; dan
    c. meningkatkan efektivitas pelaksanaan kebijakan, program dan kegiatan penyelenggaraan persandian untuk pengamanan Informasi.
(3) Ruang lingkup Peraturan Wali Kota ini meliputi:
    a. penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah;
    b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.
    c. Pemantauan, Evaluasi dan Pelaporan; dan
    d. Pembinaan dan Pengawasan Teknis.

BAB II

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI PEMERINTAH DAERAH

Bagian Kesatu

Umum

Pasal 3

Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dilaksanakan melalui:

a. penyusunan kebijakan Pengamanan Informasi;
b. pengelolaan sumber daya Keamanan Informasi;
c. pengamanan Sistem Elektronik dan pengamanan informasi nonelektronik; dan
d. penyediaan layanan Keamanan Informasi.

Bagian Kedua

Penyusunan Kebijakan Pengamanan Informasi

Pasal 4

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 3 huruf a dilakukan dengan:

a. menyusun rencana strategis pengamanan informasi;
b. menetapkan arsitektur Keamanan Informasi; dan
c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

Pasal 5

(1) Rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 4 huruf a ditetapkan oleh Wali Kota.
(2) Penyusunan rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.
(3) Rencana strategis sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. Tujuan, sasaran, program, kegiatan, dan target pelaksanaan Pengamanan Informasi setiap tahun untuk jangka waktu 5 (lima) tahun; dan
    b. peta rencana penyelenggaraan pengamanan informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun untuk jangka waktu 5 (lima) tahun.
(4) Rencana strategis Pengamanan Informasi yang telah disusun sebagimana dimaksud pada ayat (1) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah.
(5) Dalam melakukan penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.

Pasal 6

(1) Arsitektur keamanan informasi sebagaimana dimaksud dalam Pasal 4 huruf b ditetapkan oleh Wali Kota atas usulan Kepala Dinas.
(2) Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) memuat:
    a. infrastruktur teknologi informasi;
    b. desain keamanan perangkat teknologi informasi dan keamanan jaringan; dan
    c. aplikasi keamanan perangkat teknologi informasi dan keamanan jaringan.

(3) Arsitektur keamanan informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.

(4) Arsitektur Keamanan Informasi dilakukan evaluasi oleh Wali Kota pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu-waktu sesuai dengan kebutuhan.

(5) Dalam melakukan penyusunan Arsitektur Keamanan Informasi, Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.

Pasal 7

(1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 huruf c ditetapkan oleh Wali Kota atas usulan Kepala Dinas.

(2) Aturan mengenai tata kelola Keamanan Informasi terdiri atas:
   a. keamanan sumber daya teknologi informasi;
   b. keamanan akses kontrol;
   c. keamanan data dan informasi;
   d. keamanan sumber daya manusia;
   e. keamanan jaringan;
   f. keamanan surat elektronik;
   g. keamanan pusat data; dan/atau
   h. keamanan komunikasi.

(3) Dalam melakukan penyusunan aturan mengenai tata kelola Keamanan Informasi, Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.

Bagian Ketiga

Pengelolaan Sumber Daya Keamanan Informasi

Pasal 8

(1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 3 huruf b dilaksanakan oleh Dinas.

(2) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. pengelolaan aset keamanan teknologi informasi dan komunikasi;
   b. pengelolaan sumber daya manusia; dan
   c. manajemen pengetahuan.

Pasal 9

(1) Pengelolaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.

(2) Aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi, dan/atau memulihkan insiden Keamanan Informasi dalam Sistem Elektronik.

Pasal 10

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf b dilakukan oleh Dinas.

(2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses sebagai berikut:
   a. pengembangan kompetensi;
   b. pembinaan karir;
   c. pendayagunaan; dan
   d. pemberian tunjangan pengamanan persandian.

Pasal 11

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf a dilaksanakan dengan:
   a. melalui tugas belajar, pendidikan dan pelatihan, pembentukan dan penjenjangan fungsional, pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, *workshop*, seminar dan kegiatan lainnya yang terkait pengembangan kompetensi sumber daya manusia di bidang Keamanan Informasi;
   b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya, atau Pemerintah Daerah; dan
   c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi bidangnya.

(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf b dilaksanakan dengan:
   a. pembinaan jabatan fungsional di bidang Keamanan Informasi; dan

b. pengisian formasi jabatan pimpinan tinggi, jabatan administrator, dan jabatan pengawas sesuai dengan standar kompetensi yang ditetapkan.

(3) Pendayagunaan sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di bidang Keamanan lnformasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan.

(4) Pemberian tunjangan pengamanan persandian sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf d adalah pemberian tunjangan khusus kepada Aparatur Sipil Negara yang diangkat sebagai pengelola pengamanan persandian di lingkungan Pemerintah Daerah yang lingkup tugas dan tanggung jawabnya meliputi bidang pengamanan persandian sesuai dengan ketentuan Peraturan Perundang-undangan.

(5) Penetapan kriteria pemberian tunjangan pengamanan persandian ditetapkan Wali Kota atas usulan Kepala Dinas.

Pasal 12

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf c dilakukan oleh Dinas.

(2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait keamanan Informasi.

(3) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi.

(4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi.

(5) Dalam pelaksanaan manajemen pengetahuan, Pemerintah Daerah dapat melakukan koordinasi dan konsultasi dengan BSSN.

Bagian Keempat

Pengamanan Sistem Elektronik dan Pengamanan lnformasi Nonelektronik

Pasal 13

Pengamanan sistem elektronik dan pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 3 huruf c dilaksanakan oleh Dinas sesuai dengan ketentuan Peraturan Perundang-undangan.

Pasal 14

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 13 terdiri atas:

a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirsangkal terhadap data dan informasi;
b. penjaminan ketersediaan infrastruktur yang terdiri atas pusat data, jaringan intra pemerintah, dan sistem penghubung layanan penyelenggaraan pemerintahan berbasis elektronik; dan
c. penjaminan keutuhan, ketersediaan, dan keaslian aplikasi.

Pasal 15

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 13, Dinas melakukan:
    a. identifikasi;
    b. deteksi;
    c. proteksi; dan
    d. penanggulangan dan pemulihan.
(2) Identifikasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui kegiatan analisis kerawanan dan risiko terhadap Sistem Elektronik.
(3) Deteksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui kegiatan analisis untuk menentukan adanya ancaman atau kejadian insiden pada Sistem Elektronik.
(4) Proteksi sebagaimana dimaksud pada ayat (1) huruf c dilakukan melalui kegiatan mitigasi risiko dan penerapan perlindungan terhadap Sistem Elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintahan berbasis elektronik.
(5) Penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (1) huruf d dilakukan melalui kegiatan penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Pasal 16

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 14 Pemerintah Daerah wajib menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.
(2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh BSSN dan/atau lembaga penyelenggara Sertifikasi Elektronik dalam negeri yang telah diakui.
(3) Untuk mendapatkan Sertifikat elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 17

(1) Dalam mendukung penyelenggaran layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 16, Pemerintah Daerah dapat menyelenggarakan pusat operasi Pengamanan Informasi sesuai dengan standar yang ditetapkan oleh BSSN.
(2) Pusat operasi Pengamanan lnformasi sebagaimana dimaksud pada ayat (1) bertujuan untuk pengamanan Sistem Elektronik dengan melakukan proses pengawasan, penanggulangan, dan pemulihan atas insiden keamanan Sistem Elektronik dengan memperhatikan aspek personel, proses pelaksanaan, dan ketersediaan teknologi.

Pasal 18

(1) Pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 13 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.
(2) Pengamanan Informasi nonelektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai ketentuan peraturan perundang-undangan.

Pasal 19

(1) Dinas melaksanakan audit Keamanan Informasi di lingkup Pemerintah Daerah.
(2) Audit Keamanan Informasi meliputi audit keamanan Sistem Elektronik dan audit pelaksanaan sistem manajemen.
(3) Audit Keamanan lnformasi dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima

Penyediaan Layanan Keamanan Informasi

Pasal 20

(1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 3 huruf d dilaksanakan oleh Dinas.

(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:

a. wali kota dan wakil wali kota;
b. perangkat paerah;
c. aparatur sipil negara pada Pemerintah Daerah; dan
d. pihak lainnya.

Pasal 21

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 20 ayat (1) meliputi:

a. identifikasi kerentanan dan penilaian risiko terhadap Sistem Elektronik;
b. asistensi dan fasilitasi penguatan keamanan Sistem Elektronik;
c. penerapan Sertifikat Elektronik untuk melindungi Sistem Elektronik dan dokumen elektronik;
d. perlindungan Informasi melalui penyediaan perangkat teknologi Keamanan lnformasi dan jaring komunikasi sandi;
e. fasilitasi sertifikasi penerapan manajemen pengamanan Sistem Elektronik;
f. audit Keamanan Sistem Elektronik;
g. audit keamanan pelaksanaan sistem manajemen;
h. literasi Keamanan Informasi dalam rangka peningkatan kesadaran Keamanan Informasi dan pengukuran tingkat kesadaran Keamanan Informasi di lingkungan pemerintah daerah dan publik;
i. peningkatan kompetensi sumber daya manusia di bidang Keamanan lnformasi dan/atau persandian;
j. pengelolaan pusat operasi Pengamanan lnformasi;
k. penanganan insiden Keamanan Sistem Elektronik;
l. forensik digital;
m. perlindungan informasi pada kegiatan penting pemerintah daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
n. perlindungan Informasi pada aset/fasilitas penting milik atau yang akan digunakan pemerintah daerah melalui kegiatan kontra penginderaan;

o. konsultasi Keamanan Informasi bagi Pengguna Layanan; dan/atau
p. jenis Layanan Keamanan Informasi lainnya.

Pasal 22

(1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 21, Dinas melaksanakan manajemen Layanan Keamanan Informasi.
(2) Manajemen Layanan Keamanan lnformasi sebagaimana dimaksud pada ayat (1) bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan Keamanan Informasi kepada Pengguna Layanan.
(3) Manajemen Layanan Keamanan Informasi merupakan penanganan terhadap keluhan, gangguan, masalah, permintaan, dan/atau perubahan Layanan Keamanan Informasi dari Pengguna Layanan.
(4) Manajemen Layanan Keamanan lnformasi sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen Layanan Keamanan lnformasi.

BAB III

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Pasal 23

(1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf b ditetapkan oleh Wali Kota.
(2) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (1) bertujuan untuk menentukan jaring komunikasi sandi internal Pemerintah Daerah.
(3) Jaring komunikasi sandi internal Pemerintah Daerah sebagaimana dimaksud pada ayat (2) terdiri atas:
    a. jaring komunikasi sandi antar perangkat daerah;
    b. jaring komunikasi sandi internal perangkat daerah; dan
    c. jaring komunikasi sandi pimpinan daerah.
(4) Jaring komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh Perangkat Daerah.
(5) Jaring komunikasi sandi internal Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar Pengguna Layanan di lingkup internal Perangkat Daerah.

(6) Jaring komunikasi sandi Pimpinan Daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Wali Kota, Wakil Wali Kota, dan Kepala Perangkat Daerah.

Pasal 24

(1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 23 ayat (1) dilaksanakan melalui:
   a. identifikasi pola hubungan komunikasi sandi; dan
   b. analisis pola hubungan komunikasi sandi.
(2) ldentifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf a, dilakukan terhadap:
   a. pola hubungan komunikasi pimpinan dan pejabat struktural internal Pemerintah Daerah;
   b. alur informasi yang dikomunikasikan antar Perangkat Daerah dan internal Perangkat Daerah;
   c. teknologi informasi dan komunikasi;
   d. infrastruktur komunikasi; dan
   e. kompetensi personel.
(3) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2).
(4) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3) memuat:
   a. pengguna Layanan yang akan terhubung dalam jaring komunikasi sandi;
   b. topologi atau bentuk atau model keterhubungan jaring komunikasi sandi antar Pengguna Layanan;
   c. perangkat keamanan teknologi informasi dan komunikasi, dan infrastruktur komunikasi, serta fasilitas lainnya yang dibutuhkan; dan
   d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.
(5) Hasil analisis pola hubungan komunikasi sandi ditetapkan sebagai Pola Hubungan Komunikasi Sandi Antar Perangkat Daerah dalam bentuk Keputusan Wali Kota.
(6) Keputusan Wali Kota sebagaimana dimaksud pada ayat (5) paling sedikit memuat:

a. entitas Pengguna Layanan yang terhubung dalam jaring komunikasi sandi;
b. topologi atau bentuk atau model keterhubungan antar Pengguna Layanan;
c. sarana dan prasarana yang digunakan; dan
d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.

(7) Salinan Keputusan Wali Kota disampaikan oleh Wali Kota kepada Gubernur sebagai wakil Pemerintah Pusat dan ditembuskan kepada Kepala Lembaga Pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

Pasal 25

(1) Pola hubungan komunikasi sandi antar perangkat daerah yang telah ditetapkan sebagaimana dimaksud dalam Pasal 23 ayat (2), diimplementasikan dengan memanfaatkan perangkat dan/atau aplikasi yang telah diamankan dengan persandian.

(2) Perangkat dan/atau aplikasi yang telah diamankan dengan persandian sebagaimana dimaksud pada ayat (1), terdiri atas:
a. *Handphone* bersandi;
b. *Handytalky* bersandi;
c. Secure chat application;
d. Secure e-mail;
e. *File encryption*; dan
f. Perangkat dan/atau aplikasi yang telah diamankan dengan persandian lainnya.

BAB IV

PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 26

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.

(2) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas setiap 1 (satu) tahun sekali.

(3) Dinas menyampaikan laporan hasil pemantauan dan evaluasi kepada Wali Kota dan kepada Gubernur sebagai wakil Pemerintah Pusat.

Pasal 27

Pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB V

PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 28

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dilaksanakan oleh BSSN dan Gubernur sebagai wakil Pemerintah Pusat sesuai dengan kewenangannya.

Pasal 29

(1) Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar perangkat daerah dilakukan oleh Wali Kota.
(2) Pembinaan dan Pengawasan teknis sebagaimana dimaksud pada ayat (1) dilakukan Dinas sesuai dengan ketentuan peraturan perundang-undangan.
(3) Dinas menyampaikan Pembinaan dan Pengawasan teknis sebagaimana dimaksud pada ayat (2) disampaikan ke BSSN.

Pasal 30

(1) Dalam melaksanakan pembinaan dan pengawasan teknis sebagimana dimaksud dalam Pasal 28, Pemerintah Daerah sesuai dengan kewenangannya menyelenggarakan rapat koordinasi urusan Persandian.
(2) Rapat koordinasi sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam setahun.

BAB VI

PENDANAAN

Pasal 31

Pendanaan pelaksanaan penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat daerah bersumber dari:

a. Anggaran Pendapatan dan Belanja Daerah Kota; dan
b. Sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII

PENUTUP

Pasal 32

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 tanggal 18 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 491

Salinan ini sesuai dengan aslinya,
KEPALA BAGIAN HUKUM

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