WALI KOTA PADANG

PROVINSI SUMATERA BARAT

PERATURAN WALI KOTA PADANG

NOMOR 27 TAHUN 2022

TENTANG

PENYELENGGARAAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA PADANG,

Menimbang :

a. bahwa dalam rangka menjamin keamanan informasi sistem pemerintahan berbasi elektronik, perlu dilakukan pengendalian keamanan secara terpadu;
b. bahwa agar keamanan informasi sebagaimana dimaksud pada huruf a dapat diterapkan sesuai manajemen dan standar perlu diatur dalam bentuk Peraturan Wali Kota;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b, perlu menetapkan Peraturan Wali Kota tentang Penyelenggaraan Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

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 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);

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 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
4. Peraturan Pemerintah Nomor 17 Tahun 1980 tentang Perubahan Batas Wilayah Kotamadya Daerah Tingkat II Padang (Lembaran Negara Republik Indonesia Tahun 1980 Nomor 25, Tambahan Lembaran Negara Republik Indonesia Nomor 3864);
5. 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);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Daerah Kota Padang Nomor 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Padang (Lembaran Daerah Kota Padang Tahun 2016 Nomor 6, Tambahan Lembaran Daerah Kota Padang Nomor 87) sebagaimana diubah dengan Peraturan Daerah Kota Padang Nomor 3 Tahun 2020 tentang Perubahan Atas Peraturan Daerah Kota Padang Nomor 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Padang (Lembaran Daerah Kota Padang Tahun 2020 Nomor 3, Tambahan Lembaran Daerah Kota Padang Nomor 118);

8. Peraturan Wali Kota Padang Nomor 76 Tahun 2019 tentang Pengelolaan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Tahun 2019 Nomor 76);

MEMUTUSKAN:

Menetapkan : PERATURAN WALI KOTA TENTANG PENYELENGGARAAN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:

1. Wali Kota adalah Wali Kota Padang.
2. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
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. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
5. Instansi Pusat adalah kementerian, lembaga pemerintah nonkementerian, kesekretariatan lembaga negara, kesekretariatan lembaga nonstruktural, dan lembaga pemerintah lainnya.
6. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
7. Dinas adalah satuan kerja perangkat daerah yang melaksanakan urusan pemerintahan dibidang komunikasi dan informatika.
8. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
9. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
10. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
11. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.

12. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
13. Antarmuka Pemrograman Aplikasi (*Application Programming Interface)* yang selanjutnya disingkat API adalah sekumpulan perintah, fungsi, serta protokol yang mengintegrasikan dua bagian dari aplikasi atau dengan aplikasi yang berbeda secara bersamaan.
14. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.

BAB II
MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Bagian Kesatu
Umum

Pasal 2

(1) Manajemen keamanan informasi bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi.
(2) Manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) dilaksanakan melalui serangkaian proses manajemen keamanan informasi yang meliputi:
    a. penetapan ruang lingkup;
    b. penetapan penanggung jawab;
    c. perencanaan;
    d. dukungan pengoperasian;
    e. evaluasi kinerja; dan
    f. perbaikan berkelanjutan.

Bagian Kedua
Penetapan Ruang Lingkup

Pasal 3

(1) Penetapan ruang lingkup sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a dilakukan oleh Wali Kota.
(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) dilakukan dengan mendefinisikan:

a. isu internal keamanan informasi SPBE dalam organisasi; dan

b. isu eksternal keamanan informasi SPBE.

(3) Isu internal keamanan informasi SPBE dalam organisasi sebagaimana dimaksud pada ayat (2) huruf a didefinisikan berdasarkan area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE.

(4) Area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE sebagaimana dimaksud pada ayat (3) paling sedikit meliputi :

a. data dan informasi SPBE;

b. aplikasi SPBE;

c. aset Infrastruktur SPBE; dan

d. kebijakan keamanan informasi SPBE yang telah dimiliki.

(5) Isu eksternal keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) huruf b didefinisikan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Ketiga
Penetapan Penanggung Jawab

Pasal 4

(1) Wali Kota menetapkan penanggung jawab SPBE sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b sebagai Koordinator SPBE.

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

Pasal 5

(1) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (2) menetapkan pelaksana teknis Keamanan SPBE.

(2) Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:

a. Kepala Dinas; dan

b. Kepala Bidang Statistik Sektoral dan Persandian Daerah.

Pasal 6

(1) Kepala Dinas sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a mempunyai tugas:

a. memastikan penerapan standar teknis dan prosedur Keamanan SPBE;

b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE; dan

c. melaporkan pelaksanaan manajemen keamanan informasi SPBE dan penerapan standar teknis dan prosedur Keamanan SPBE kepada koordinator SPBE Pemerintah Daerah Kota Padang.

(2) Kepala Bidang Statistik Sektoral dan Persandian Daerah sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf b 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 SPBE yang telah ditetapkan;

c. memastikan keberlangsungan proses bisnis SPBE; dan

d. berkoordinasi dengan pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi pada Pemerintah Daerah Kota Padang terkait perumusan program kerja dan anggaran Keamanan SPBE.

Bagian Keempat
Perencanaan

Pasal 7

(1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf c dilakukan oleh pelaksana teknis Keamanan SPBE.

(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:

a. program kerja Keamanan SPBE yang disusun berdasarkan kategori risiko Keamanan SPBE; dan

b. target realisasi program kerja Keamanan SPBE.

(3) Program kerja Keamanan SPBE sebagaimana dimaksud pada 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.

(4) Kategori risiko Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a ditentukan sesuai dengan ketentuan peraturan perundang-undangan.

(5) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b ditetapkan berdasarkan kebutuhan Pemerintah Daerah.

Pasal 8

Edukasi kesadaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf a dilaksanakan paling sedikit melalui kegiatan:

a. sosialisasi; dan
b. pelatihan.

Pasal 9

Penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf b dilaksanakan paling sedikit melalui:

a. menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur;
b. mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
c. mengukur tingkat risiko Keamanan SPBE.

Pasal 10

(1) Peningkatan Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam Pasal 10.
(2) Peningkatan Keamanan SPBE dilaksanakan paling sedikit melalui:
    a. menerapkan standar teknis dan prosedur Keamanan SPBE; dan
    b. menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 11

Penanganan insiden Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf d dilaksanakan paling sedikit melalui:

a. mengidentifikasi sumber serangan;
b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
d. mendokumentasi bukti insiden yang terjadi; dan
e. memitigasi atau mengurangi dampak risiko Keamanan SPBE.

Pasal 12

Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima

Dukungan Pengoperasian

Pasal 13

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 ayat (2) 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; dan

b. anggaran Keamanan SPBE.

(3) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a paling sedikit harus memiliki kompetensi:

a. keamanan infrastruktur teknologi, informasi dan komunikasi; dan

b. keamanan aplikasi.

(4) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (3), Pemerintah Daerah paling sedikit melakukan kegiatan:

a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi, informasi dan komunikasi dan keamanan aplikasi; dan

b. bimbingan teknis mengenai standar Keamanan SPBE.

(5) Anggaran Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Keenam

Evaluasi Kinerja

Pasal 14

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf e dilakukan oleh koordinator SPBE.

(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan Keamanan SPBE dengan melaksanakan :

a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE;

b. menetapkan indikator kinerja pada setiap area proses;

c. memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;

d. menganalisis efektifitas pelaksanaan Keamanan SPBE; dan

e. 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.

Bagian Ketujuh

Perbaikan Berkelanjutan

Pasal 15

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 2 ayat (2) 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; dan
    b. memperbaiki pelaksanaan Keamanan SPBE secara periodik.

BAB III

STANDAR TEKNIS DAN PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Bagian Kesatu

Umum

Pasal 16

Standar teknis dan prosedur Keamanan SPBE diterapkan untuk:
a. keamanan data dan informasi;
b. keamanan Aplikasi SPBE;
c. keamanan Sistem Penghubung Layanan; dan
d. keamanan Jaringan Intra.

Bagian Kedua

Keamanan data dan informasi

Pasal 17

Standar teknis keamanan data dan informasi sebagaimana dimaksud dalam Pasal 16 huruf a terdiri atas terpenuhinya aspek:
a. kerahasiaan;
b. keaslian;
c. keutuhan;
d. kenirsangkalan; dan

e. ketersediaan.

Pasal 18

Terpenuhinya aspek kerahasiaan sebagaimana dimaksud dalam Pasal 17 huruf a dilakukan dengan prosedur:

a. menetapkan klasifikasi informasi;
b. menerapkan enkripsi dengan sistem kriptografi; dan
b. menerapkan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan.

Pasal 19

Terpenuhinya aspek keaslian sebagaimana dimaksud dalam Pasal 17 huruf b dilakukan dengan prosedur:

a. menyediakan mekanisme verifikasi;
b. menyediakan mekanisme validasi; dan
c. menerapkan sistem *hash function.*

Pasal 20

Terpenuhinya aspek keutuhan sebagaimana dimaksud dalam Pasal 17 huruf c dilakukan dengan prosedur:

a. menerapkan pendeteksian modifikasi; dan
b. menerapkan tanda tangan elektronik tersertifikasi.

Pasal 21

Terpenuhinya aspek kenirsangkalan sebagaimana dimaksud dalam Pasal 17 huruf d dilakukan dengan prosedur:

a. menerapkan tanda tangan elektronik tersertifikasi; dan
b. penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.

Pasal 22

Terpenuhinya aspek ketersediaan sebagaimana dimaksud dalam Pasal 17 huruf e dilakukan dengan prosedur :

a. menerapkan sistem pencadangan secara berkala;
b. membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses; dan
c. menerapkan sistem pemulihan.

Bagian Ketiga

Keamanan Aplikasi SPBE

Pasal 23

(1) Standar teknis dan prosedur keamanan Aplikasi SPBE sebagaimana dimaksud dalam Pasal 16 huruf b diterapkan pada:
   a. aplikasi berbasis web; dan
   b. aplikasi berbasis *mobile*.
(2) Aplikasi berbasis web sebagaimana dimaksud pada ayat (1) huruf a merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet.
(3) Aplikasi berbasis *mobile* sebagaimana dimaksud pada ayat (1) huruf b merupakan aplikasi yang dalam pengoperasiannya dapat berjalan diperangkat bergerak, dan memiliki sistem operasi yang mendukung perangkat lunak secara *standalone*.
(4) 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. menganalisis kerentanan.

Pasal 24

Standar teknis keamanan aplikasi berbasis web sebagaimana dimaksud dalam Pasal 23 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 eror 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.

Pasal 25

(1) Terpenuhinya fungsi autentikasi sebagaimana dimaksud dalam Pasal 24 huruf a dilakukan dengan prosedur:

a. menggunakan manajemen kata sandi untuk proses autentikasi;

b. menerapkan verifikasi kata sandi pada sisi server;

c. mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;

d. mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;

e. mengatur mekanisme pemulihan kata sandi;

f. menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan

g. menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.

(2) Terpenuhinya fungsi manajemen sesi sebagaimana dimaksud dalam Pasal 24 huruf b dilakukan dengan prosedur:

a. menggunakan pengendali sesi untuk proses manajemen sesi;

b. menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;

c. mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;

d. mengatur kondisi dan jangka waktu habis sesi;

e. validasi dan pencantuman *session id*;

f. pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan

g. pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna.

(3) Terpenuhinya fungsi persyaratan kontrol akses sebagaimana dimaksud dalam Pasal 24 huruf c dilakukan dengan prosedur:

a. menetapkan otorisasi pengguna untuk membatasi kontrol akses;

b. mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi;

c. mengatur antarmuka pada sisi administrator; dan

b. mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan.

(4) Terpenuhinya fungsi validasi input sebagaimana dimaksud dalam Pasal 24 huruf d dilakukan dengan prosedur:

a. menerapkan fungsi validasi input pada sisi server;

b. menerapkan mekanisme penolakan input jika terjadi kesalahan validasi;
c. memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi input;
d. melakukan validasi positif pada seluruh input;
e. melakukan filter terhadap data yang tidak dipercaya;
f. menggunakan fitur kode dinamis;
g. melakukan pelindungan terhadap akses yang mengandung konten skrip; dan
h. melakukan pelindungan dari serangan injeksi basis data.

(5) Terpenuhinya fungsi kriptografi pada verifikasi statis sebagaimana dimaksud dalam Pasal 24 huruf e dilakukan dengan prosedur:
a. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang- undangan;
b. melakukan autentikasi data yang dienkripsi;
c. menerapkan manajemen kunci kriptografi; dan
d. membuat angka acak yang menggunakan generator angka acak kriptografi.

(6) Terpenuhinya fungsi penanganan eror dan pencatatan log sebagaimana dimaksud dalam Pasal 24 huruf f dilakukan dengan prosedur:
a. mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;
b. menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;
c. tidak mencantumkan informasi yang dikecualikan dalam pencatatan log;
d. mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
e. mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah;
f. melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log; dan
g. melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

(7) Terpenuhinya fungsi proteksi data sebagaimana dimaksud dalam Pasal 24 huruf g dilakukan dengan prosedur:
a. melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
b. melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;

c. melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
d. melakukan penentuan jumlah parameter;
e. memastikan data disimpan dengan aman;
f. menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna; dan
g. membersihkan memori setelah tidak diperlukan.

(8) Terpenuhinya fungsi keamanan komunikasi sebagaimana dimaksud dalam Pasal 24 huruf h dilakukan dengan prosedur:
a. menggunakan komunikasi terenkripsi;
b. mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna;
c. mengatur jenis algoritma yang digunakan dan alat pengujiannya; dan
d. mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.

(9) Terpenuhinya fungsi pengendalian kode berbahaya sebagaimana dimaksud dalam Pasal 24 huruf i dilakukan dengan prosedur:
a. menggunakan analisis kode dalam kontrol kode berbahaya;
b. memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan;
c. mengatur izin terkait fitur atau sensor terkait privasi;
d. mengatur pelindungan integritas; dan
e. mengatur mekanisme fitur pembaruan.

(10) Terpenuhinya fungsi logika bisnis sebagaimana dimaksud dalam Pasal 24 huruf j dilakukan dengan prosedur:
a. memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis;
b. memastikan logika bisnis memiliki batasan dan validasi;
c. memonitor aktivitas yang tidak biasa;
d. membantu dalam kontrol antiotomatisasi; dan
e. memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.

(11) Terpenuhinya fungsi *file* sebagaimana dimaksud dalam Pasal 24 huruf k dilakukan dengan prosedur:
a. mengatur jumlah *file* untuk setiap pengguna dan kuota ukuran *file* yang diunggah;
b. melakukan validasi *file* sesuai dengan tipe konten yang diharapkan;
c. melakukan pelindungan terhadap metadata input dan metadata *file*;

d. melakukan pemindaian *file* yang diperoleh dari sumber yang tidak dipercaya; dan

e. melakukan konfigurasi server untuk mengunduh *file* sesuai ekstensi yang ditentukan.

(12) Terpenuhinya fungsi keamanan API dan *web service* sebagaimana dimaksud dalam Pasal 24 huruf l dilakukan dengan prosedur:

a. melakukan konfigurasi layanan web;

b. memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;

c. membuat keputusan otorisasi;

d. menampilkan metode RESTful *hypertext transfer protocol* apabila input pengguna dinyatakan valid;

e. menggunakan validasi skema dan verifikasi sebelum menerima input;

f. menggunakan metode pelindungan layanan berbasis web; dan

g. menerapkan kontrol antiotomatisasi.

(13) Terpenuhinya fungsi keamanan konfigurasi sebagaimana dimaksud dalam Pasal 24 huruf m dilakukan dengan prosedur:

a. mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan;

b. mendokumentasi, menyalin konfigurasi, dan semua dependensi;

c. menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;

d. memvalidasi integritas aset jika aset aplikasi diakses secara eksternal; dan

e. menggunakan respons aplikasi dan konten yang aman.

Pasal 26

Standar teknis keamanan aplikasi berbasis mobile sebagaimana dimaksud dalam Pasal 23 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 27

(1) Terpenuhinya fungsi penyimpanan data dan persyaratan privasi sebagaimana dimaksud dalam Pasal 26 huruf a dilakukan dengan prosedur:
   a. menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem;
   b. membatasi pertukaran data dan informasi yang dikecualikan dengan *third party;*
   c. menonaktifkan *cache keyboard* pada saat memasukkan data dan informasi yang dikecualikan;
   d. melindungi informasi yang dikecualikan saat terjadi *inter process communication;* dan
   e. melindungi data dan informasi yang dikecualikan yang dimasukkan melalui antarmuka pengguna.

(2) Terpenuhinya fungsi kriptografi sebagaimana dimaksud dalam Pasal 26 huruf b dilakukan dengan prosedur:
   a. menghindari penggunaan kriptografi simetrik dengan *hardcoded key;*
   b. mengimplementasikan metode kriptografi yang sudah teruji sesuai kebutuhan;
   c. menghindari penggunaan protokol kriptografi atau algoritme kriptografi yang obsolet;
   d. menghindari penggunaan kunci kriptografi yang sama; dan
   e. menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.

(3) Terpenuhinya fungsi autentikasi dan manajemen sesi sebagaimana dimaksud dalam Pasal 26 huruf c dilakukan dengan prosedur:
   a. menerapkan autentikasi pada *remote endpoint* terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh;
   b. menggunakan *session identifier* yang acak tanpa perlu mengirimkan kredensial pengguna apabila menggunakan *stateful* manajemen sesi;
   c. memastikan server menyediakan token yang telah ditandatangani menggunakan algoritme yang aman apabila menggunakan autentikasi *stateless* berbasis token;
   d. memastikan *remote endpoint* memutus sesi yang ada saat pengguna *log out*;
   e. menerapkan pengaturan sandi pada *remote endpoint*;
   f. membatasi jumlah percobaan *log in* pada *remote endpoint*;
   g. menentukan masa berlaku sesi dan masa kedaluwarsa token pada *remote endpoint*; dan
   h. melakukan otorisasi pada *remote endpoint.*

(4) Terpenuhinya fungsi komunikasi jaringan sebagaimana dimaksud dalam Pasal 26 huruf d dilakukan dengan prosedur:
   a. menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolet secara konsisten; dan
   b. memverifikasi sertifikat *remote endpoint.*

(5) Terpenuhinya fungsi interaksi platform sebagaimana dimaksud dalam Pasal 26 huruf e dilakukan dengan prosedur:
   a. memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan;
   b. melakukan validasi terhadap seluruh input dari sumber eksternal dan pengguna;
   c. menghindari pengiriman fungsionalitas sensitif melalui skema *custom uniform resource locator* dan fasilitas *inter process communication*;
   d. menghindari penggunaan *JavaScript* dalam *WebView*;
   e. menggunakan protokol *hypertext transfer protocol secure* pada *WebView*; dan
   f. mengimplementasikan penggunaan serialisasi API yang aman.

(6) Terpenuhinya fungsi kualitas kode dan pengaturan *build* sebagaimana dimaksud dalam Pasal 26 huruf f dilakukan dengan prosedur:
   a. menandatangani aplikasi dengan sertifikat yang valid;
   b. memastikan aplikasi dalam mode rilis;
   c. menghapus simbol *debugging* dari *native binary*;
   d. menghapus kode *debugging* dan kode bantuan pengembang;
   e. mengidentifikasi kelemahan seluruh komponen *third party*;
   f. menentukan mekanisme penanganan eror;
   g. mengelola memori secara aman; dan
   h. mengaktifkan fitur keamanan yang tersedia.

(7) Terpenuhinya fungsi ketahanan sebagaimana dimaksud dalam Pasal 26 huruf g dilakukan dengan prosedur:
   a. mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah;
   b. mendeteksi dan merespons *debugger*;
   c. mencegah *executable file* melakukan perubahan pada sumber daya perangkat;
   d. mendeteksi dan merespons keberadaan perangkat *reverse engineering*;
   e. mencegah aplikasi berjalan dalam emulator;
   f. mendeteksi perubahan kode dan data di ruang memori;

g. menerapkan fungsi *device binding* dengan menggunakan *property* unik pada perangkat;
h. melindungi seluruh *file* dan *library* pada aplikasi; dan
i. menerapkan metode *obfuscation.*

Bagian Keempat
Keamanan Sistem Penghubung Layanan

Pasal 28

Standar teknis keamanan Sistem Penghubung Layanan sebagaimana dimaksud dalam Pasal 16 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 29

(1) Terpenuhinya fungsi keamanan interoperabilitas data dan informasi sebagaimana dimaksud dalam Pasal 28 huruf a dilakukan dengan prosedur:
a. menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik;
b. menerapkan sistem enkripsi data;
c. memastikan data dan informasi selalu dapat diakses sesuai otoritasnya; dan
d. menerapkan sistem *hash function* pada *file.*

(2) Terpenuhinya fungsi kontrol sistem integrasi sebagaimana dimaksud dalam Pasal 28 huruf b dilakukan dengan prosedur:
a. menerapkan protokol *secure socket layer* atau protokol *transport layer security* versi terkini pada sesi pengiriman data dan informasi;
b. menerapkan *internet protocol security* untuk mengamankan transmisi data dalam jaringan berbasis *transmission control protocol/internet protocol;*
c. menerapkan sistem anti *distributed denial of service;*
d. menerapkan autentikasi untuk memverifikasi identitas eksternal antar Layanan SPBE yang terhubung;
e. menerapkan manajemen keamanan sesi;
f. menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan;
g. menerapkan validasi input;

h. menerapkan kriptografi pada verifikasi statis;
i. menerapkan sertifikat elektronik pada *web authentication*;
j. menerapkan penanganan eror dan pencatatan *log*;
k. menerapkan proteksi data dan jalur komunikasi;
l. menerapkan pendeteksi virus untuk memeriksa beberapa konten *file*;
m. menetapkan perjanjian tingkat layanan dengan standar paling rendah 95% (sembilan puluh lima per seratus); dan
n. memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.

(3) Terpenuhinya fungsi kontrol perangkat integrator sebagaimana dimaksud dalam Pasal 28 huruf c dilakukan dengan prosedur:
a. menggunakan sistem operasi dan perangkat lunak dengan *security patches* terkini;
b. menggunakan anti virus dan anti-*spyware* terkini;
c. mengaktifkan fitur keamanan pada peramban web;
b. menerapkan *firewall* dan *host-based intrusion detection systems*;
c. mencegah instalasi perangkat lunak yang belum terverifikasi;
d. mencegah akses terhadap situs yang tidak sah; dan
e. mengaktifkan sistem *recovery* dan *restore* pada perangkat integrator.

(4) Terpenuhinya fungsi keamanan API dan *web service* sebagaimana dimaksud dalam Pasal 28 huruf d dilakukan dengan prosedur:
a. menerapkan protokol *secure socket layer* atau protokol *transport layer security* diantara pengirim dan penerima API;
b. menerapkan protokol *open authorization* versi terkini untuk menjembatani interaksi antara *resource owner*, *resource server* dan/atau *third party*;
c. menampilkan metode RESTful *hypertext transfer protocol* apabila input pengguna dinyatakan valid;
d. melindungi layanan web RESTful yang menggunakan *cookie* dari *cross-site request forgery*; dan
e. memvalidasi parameter yang masuk oleh penerima API untuk memastikan data yang diterima valid dan tidak menyebabkan kerusakan.

(5) Terpenuhinya fungsi keamanan migrasi data sebagaimana dimaksud dalam Pasal 28 huruf e dilakukan dengan prosedur:
a. memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem;
b. memastikan aplikasi yang menggunakan sistem basis data lama tetap dipertahankan sampai sistem pendukung basis data baru dapat berjalan atau berfungsi dengan normal;
c. mendokumentasikan format sistem basis data lama secara rinci;

d. melakukan pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data;
e. menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan data; dan
f. melakukan validasi data ketika proses migrasi data selesai.

Bagian Kelima

Keamanan Jaringan Intra

Pasal 30

(1) Standar teknis keamanan Jaringan Intra sebagaimana dimaksud dalam Pasal 16 huruf d diterapkan pada:
a. Jaringan Intra pemerintah; dan
b. Jaringan Intra Instansi Pusat dan Pemerintah Daerah.

(2) Standar teknis keamanan Jaringan Intra sebagaimana dimaksud pada ayat (1) terdiri atas terpenuhinya:
a. aspek administrasi keamanan Jaringan Intra;
b. kontrol akses dan autentikasi;
c. persyaratan perangkat dan aplikasi keamanan Jaringan Intra;
d. kontrol keamanan *gateway*;
e. kontrol keamanan *access point* pada jaringan nirkabel; dan
f. kontrol konfigurasi *access point* pada jaringan nirkabel.

Pasal 31

(1) Terpenuhinya aspek administrasi keamanan Jaringan Intra sebagaimana dimaksud dalam Pasal 30 ayat (2) huruf a dilakukan dengan prosedur:
a. menyusun dan mengevaluasi dokumen arsitektur Jaringan Intra;
b. mengidentifikasi seluruh aset infrastruktur jaringan;
c. menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra; dan
d. membuat laporan pengawasan keamanan jaringan secara periodik.

(2) Terpenuhinya kontrol akses dan autentikasi sebagaimana dimaksud dalam Pasal 30 ayat (2) huruf b dilakukan dengan prosedur:
a. menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah;
b. menggunakan autentikasi untuk mengakses Jaringan Intra;
c. menerapkan pembatasan akses dalam Jaringan Intra;
d. mematikan atau membatasi *protocol, port,* dan layanan yang tidak digunakan;

e. menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya;
f. menerapkan fungsi *honeypot* untuk menganalisis celah keamanan berdasarkan jenis serangan;
g. menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;
h. memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan/atau mengubah konfigurasi sistem dalam Jaringan Intra;
i. menerapkan *secure endpoints*;
j. memblokir layanan yang tidak dikenal;
k. menerapkan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses Jaringan Intra; dan
l. menerapkan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.

(3) Terpenuhinya persyaratan perangkat dan aplikasi keamanan Jaringan Intra sebagaimana dimaksud dalam Pasal 30 ayat (2) huruf c dilakukan dengan prosedur:
a. menggunakan perangkat *security information and event management* untuk *network logging* dan *monitoring;*
b. menerapkan sistem deteksi dini kerentanan keamanan perangkat jaringan;
c. menggunakan perangkat *firewall*;
d. menggunakan perangkat *intrusion detection systems* dan *intrusion prevention systems;*
e. menerapkan *virtual private network* terenkripsi untuk penggunaan akses jarak jauh secara terbatas;
f. menerapkan kontrol *update patching* pada infrastruktur Jaringan Intra dan sistem komputer;
g. menggunakan perangkat *web application firewall*;
h. menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;
i. memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisasi celah peretas;
j. mengunduh perangkat lunak melalui *enterprise software distribution system*; dan
k. menerapkan sertifikat elektronik.

(4) Terpenuhinya kontrol keamanan *gateway* sebagaimana dimaksud dalam Pasal 30 ayat (2) huruf d dilakukan dengan prosedur:

a. menerapkan *content filtering*;
b. b.menerapkan *inspection packet filtering* untuk memeriksa *packet* yang masuk pada Jaringan Intra;
c. menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*;
d. memastikan perangkat *gateway* yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik;
e. melaksanakan manajemen *traffic gateway*; dan
f. memastikan *port* tidak dibuka secara *default.*

(5) Terpenuhinya kontrol keamanan *access point* pada jaringan nirkabel sebagaimana dimaksud dalam Pasal 30 ayat (2) huruf e dilakukan dengan prosedur:

a. menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini;
b. menerapkan *media access control* pada *address filtering*;
c. menerapkan *dedicated service set identifier;*
d. menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan;
e. menerapkan pembatasan terkait penambahan perangkat nirkabel yang dipasang secara tidak sah;
f. menerapkan manajemen *vulnerability* secara berkala dan berkelanjutan; dan
g. melakukan *patching firmware* secara rutin.

(6) Terpenuhinya kontrol konfigurasi *access point* pada jaringan nirkabel sebagaimana dimaksud dalam Pasal 30 ayat (2) huruf f dilakukan dengan prosedur:

a. menggunakan kata sandi yang kuat;
b. menggunakan protokol model *authentication authorization* dan *accounting* pada perangkat infrastruktur jaringan untuk *management user* atau otentikasi *administrator access point*;
c. memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan;
d. mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel; dan
e. menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

BAB IV

KETENTUAN PENUTUP

Pasal 33

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 Padang.

Ditetapkan di Padang
pada tanggal 20 Juni 2022
WALI KOTA PADANG,

HENDRI SEPTA

Diundangkan di Padang
pada tanggal 20 Juni 2022
SEKRETARIS DAERAH KOTA PADANG

ANDREE HARMADI ALGAMAR

BERITA DAERAH KOTA PADANG TAHUN 2022 NOMOR 27