



WALI KOTA PALEMBANG

PROVINSI SUMATERA SELATAN

PERATURAN WALI KOTA PALEMBANG

NOMOR 27 TAHUN 2023

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KOTA PALEMBANG

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA PALEMBANG,

- Menimbang : a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Kota Palembang, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;
- b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Wali Kota tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kota Palembang;

- Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 28 Tahun 1959 tentang Pembentukan Daerah Tingkat II Termasuk Kotapraja, Dalam Lingkungan Daerah Tingkat I Sumatera Selatan (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 73, Tambahan Lembaran Negara Republik Indonesia Nomor 1821);
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.....

5. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah, terakhir dengan 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);
6. 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 6400);
7. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
8. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Resiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
10. 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);
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 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);

MEMUTUSKAN:

Menetapkan:

PERATURAN WALI KOTA TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KOTA PALEMBANG.

BAB 1

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini, yang dimaksud dengan:

1. Kota adalah Kota Palembang.
2. Pemerintah Kota adalah Pemerintah Kota Palembang.
3. Wali Kota adalah Wali Kota Palembang.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Palembang.

5. Perangkat.....

5. Perangkat Daerah, yang selanjutnya disingkat PD adalah Perangkat Daerah yang ada di lingkungan Pemerintah Kota Palembang.
6. Sistem Pemerintahan Berbasis Elektronik, yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna Sistem Pemerintahan Berbasis Elektronik.
7. Teknologi Informasi dan Komunikasi, yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
8. 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.
9. Keamanan Sistem Pemerintahan Berbasis Elektronik mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, Infrastruktur Sistem Pemerintahan Berbasis Elektronik, dan Aplikasi Sistem Pemerintahan Berbasis Elektronik.
10. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan (*confidentiality*) atas informasi dan komunikasi secara Elektronik.
11. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas Informasi Elektronik.
12. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas Informasi Elektronik.
13. Aplikasi Sistem Pemerintahan Berbasis Elektronik adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan Sistem Pemerintahan Berbasis Elektronik.
14. Manajemen Keamanan Sistem Pemerintahan Berbasis Elektronik adalah serangkaian proses untuk mencapai penerapan keamanan Sistem Pemerintahan Berbasis Elektronik yang efektif, efisien, dan berkesinambungan, serta mendukung layanan Sistem Pemerintahan Berbasis Elektronik yang berkualitas.
15. Aplikasi Sistem Pemerintahan Berbasis Elektronik adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan Sistem Pemerintahan Berbasis Elektronik.
16. Infrastruktur Sistem Pemerintahan Berbasis Elektronik 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.

Pasal 2

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

(2) Kebijakan.....

- (2) Kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) meliputi:
 - a. penetapan ruang lingkup;
 - b. penetapan penanggung jawab;
 - c. perencanaan;
 - d. dukungan pengoperasian;
 - e. evaluasi kinerja; dan
 - f. perbaikan berkelanjutan terhadap keamanan informasi.
- (3) Ketentuan lain untuk mendukung kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) dapat menerapkan pengendalian teknis keamanan yang meliputi:
 - a. manajemen risiko;
 - b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
 - c. pengelolaan pihak ketiga.

BAB II KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 3

- (1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a, meliputi:
 - a. data dan informasi SPBE;
 - b. aplikasi SPBE; dan
 - c. infrastruktur SPBE.
- (2) Penetapan sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Kota yang harus diamankan dalam SPBE.

Pasal 4

- (1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b, dilaksanakan 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 yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 5

- (1) Tugas sebagaimana dimaksud dalam Pasal 4 ayat (3) sebagai penanggung jawab manajemen keamanan informasi SPBE, koordinator SPBE menetapkan pelaksana teknis Keamanan SPBE.
- (2) Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. ketua tim; dan
 - b. anggota tim.

(3) Ketua.....

- (3) Ketua tim sebagaimana dimaksud pada ayat (2) huruf a dapat dijabat oleh pimpinan PD yang membidangi urusan komunikasi dan informatika.
- (4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh pimpinan PD lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Kota.

Pasal 6

- (1) Ketua tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a, mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Kota yang meliputi:
 - a. menetapkan prosedur pengendalian keamanan informasi SPBE Pemerintah Kota;
 - b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di lingkungan Pemerintah Kota;
 - c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan;
 - d. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
 - e. memutuskan dan merancang langkah kelangsungan layanan TIK dan bentuk dokumen *business continuity* dan *disaster recovery plans*; dan
 - f. melaporkan pelaksanaan manajemen keamanan informasi SPBE pada koordinator SPBE.
- (2) Anggota tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b, mempunyai tugas:
 - a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada setiap PD;
 - b. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan;
 - c. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
 - d. melakukan koordinasi dengan ketua tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 7

- (1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (2) 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 8

- (1) Program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 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.

Pasal 9

- (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 maniasi 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 10

- (1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 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 SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b, harus tersedia sesuai dengan kebutuhan dan tingkat urgensi dari setiap PD.
- (5) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf c, disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 11

- (1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf e dilakukan oleh koordinator SPBE.
- (2) Evaluasi sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Kota.

(3) Kinerja.....

- (3) Kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan dengan:
 - a. menganalisis efektifitas pelaksanaan Keamanan SPBE; dan
 - 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 12

- (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;
 - b. memperbaiki pelaksanaan Keamanan SPBE secara periodik; dan
 - c. tindak lanjut hasil audit Keamanan SPBE.

BAB III PENGENDALIAN TEKNIS KEAMANAN

Pasal 13

- (1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf a, dilakukan oleh setiap PD.
- (2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko (*risk register*) dengan ketentuan substansi 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 14

- (1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (3) 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 Kota dengan cakupan aspek dapat meliputi:

a. keamanan.....

- 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 control;
 - 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 *Information Technology 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) Prosedur sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dengan Keputusan Wali Kota atau kebijakan teknis lainnya.

Pasal 15

- (1) Sebagaimana dimaksud dalam Pasal 14 ayat (3) dalam pelaksanaan penetapan prosedur setiap PD harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE.
- (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 16

- (1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf c, dilakukan oleh setiap PD.
- (2) PD 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) PD harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.

(4) PD.....

- (4) PD harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerja sama dengan pihak ketiga.
- (5) PD harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
KETENTUAN PENUTUP

Pasal 17

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 Palembang.

Ditetapkan di Palembang
pada tanggal 21 Agustus 2023
WALI KOTA PALEMBANG,



HARNOJOYO

Diundangkan di Palembang
pada tanggal 21 Agustus 2023
SEKRETARIS DAERAH KOTA PALEMBANG,



RATU DEWA
BERITA DAERAH KOTA PALEMBANG TAHUN 2023 NOMOR 27