



WALIKOTA DENPASAR
PROVINSI BALI

PERATURAN WALIKOTA DENPASAR
NOMOR 33 TAHUN 2025
TENTANG
MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN
PEMERINTAH KOTA DENPASAR

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALIKOTA DENPASAR,

- Menimbang :
- bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Kota Denpasar, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;
 - bahwa berdasarkan ketentuan Pasal 48 ayat (3) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, manajemen keamanan informasi dilaksanakan berdasarkan pedoman manajemen keamanan informasi sistem pemerintahan berbasis elektronik;
 - bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Walikota tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Denpasar.

- Mengingat :
- Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
 - Undang-Undang Nomor 1 Tahun 1992 tentang Pembentukan Kotamadya Daerah Tingkat II Denpasar (Lembaran Negara Republik Indonesia Tahun 1992 Nomor 9, Tambahan Lembaran Negara Republik Indonesia Nomor 3465);



3. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua Atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 143, Tambahan Lembaran Negara Republik Indonesia Nomor 6801);
4. 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 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);
5. Undang-Undang Nomor 15 Tahun 2023 tentang Provinsi Bali (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 62, Tambahan Lembaran Negara Republik Indonesia Nomor 6871);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Menteri dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah di ubah dengan Peraturan Menteri Dalam Negeri 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);

MEMUTUSKAN:

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

BAB I KETENTUAN UMUM

Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan:

1. Daerah adalah Kota Denpasar.
2. Pemerintah Daerah adalah Pemerintah Kota Denpasar.
3. Walikota adalah Walikota Denpasar.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Denpasar.
5. Perangkat Daerah adalah Perangkat Daerah di lingkungan Pemerintah Daerah.
6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
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 SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
10. Manajemen Keamanan Informasi SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
11. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi 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.

Pasal 2

- (1) Maksud ditetapkan Peraturannya Peraturan Walikota ini sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan Daerah.

- (2) Kebijakan internal Manajemen Keamanan Informasi SPBE sebagaimana dimaksud 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 SISTEM PEMERINTAHAN BERBASIS
ELEKTRONIK

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 ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Daerah yang harus diamankan dalam SPBE.

Pasal 4

- (1) Penetapan penanggung jawab sebagaimana dimaksud dalam pasal 2 ayat (2) huruf b dilaksanakan oleh Walikota.
- (2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
- (3) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE, Sekretaris Daerah sebagai penanggung jawab merupakan ketentuan yang tidak terpisahkan dari tugas disebut sebagai koordinator SPBE.

Pasal 5

- (1) 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 pimpinan Perangkat Daerah yang membidangi urusan komunikasi dan informatika.
- (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 Daerah.

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 Daerah yang meliputi:
 - a. menetapkan prosedur pengendalian Keamanan Informasi SPBE Daerah;
 - b. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE di lingkungan Daerah;
 - c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan Peraturan Perundang-undangan;
 - d. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
 - e. memutuskan dan merancang langkah kelangsungan layanan TIK dalam 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 Perangkat Daerah masing- masing;
 - b. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan Peraturan Perundang- undangan;
 - c. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
 - d. berkoordinasi 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.
- (2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud dalam pasal 7 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

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 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 10

- (1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam pasal 9 ayat (2) huruf a paling sedikit berjumlah 2 (dua) 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 kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.
- (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 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 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 Perangkat Daerah.
- (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 Daerah dengan cakupan aspek dapat 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 kepala Perangkat Daerah yang melaksanakan urusan pemerintahan di bidang komunikasi, informatika dan statistik.

Pasal 15

- (1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 14 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 16

- (1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf c dilakukan oleh setiap Perangkat Daerah.
- (2) Perangkat Daerah berkewajiban 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 berkewajiban memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
- (4) Perangkat Daerah berkewajiban menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek Keamanan Informasi dalam hubungan kerjasama dengan pihak ketiga.

- (5) Perangkat daerah berkewajiban membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
KETENTUAN PENUTUP

Pasal 17

Peraturan Walikota ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Denpasar
pada tanggal 2 September 2025

WALIKOTA DENPASAR,

ttd.

I GUSTI NGURAH JAYA NEGARA

Diundangkan di Denpasar
pada tanggal 2 September 2025

SEKRETARIS DAERAH KOTA DENPASAR,

ttd.

IDA BAGUS ALIT WIRADANA

BERITA DAERAH KOTA DENPASAR TAHUN 2025 NOMOR 33

