



SALINAN

WALI KOTA BANJAR
PROVINSI JAWA BARAT

PERATURAN WALI KOTA BANJAR
NOMOR 38 TAHUN 2023

TENTANG
MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA BANJAR,

- Menimbang : a. bahwa dalam rangka melindungi kerahasiaan, keutuhan dan ketersediaan aset informasi di Pemerintah Kota Banjar yang diselenggarakan berbasis elektronik dari berbagai ancaman keamanan informasi baik dari dalam maupun luar;
- b. bahwa untuk menjamin terjaganya keamanan informasi sistem pemerintahan berbasis elektronik perlu diselenggarakan manajemen keamanan informasi;
- c. untuk memberikan arah, landasan dan kepastian hukum kepada semua pihak yang terlibat dalam sistem pemerintahan berbasis elektronik, maka diperlukan pengaturan tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;
- d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu menetapkan Peraturan Wali Kota tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;
- Mengingat : 1. Undang-Undang Nomor 27 Tahun 2002 tentang Pembentukan Kota Banjar di Provinsi Jawa Barat (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 130 Tambahan Lembaran Negara Republik Indonesia Nomor 4244);
2. 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 6858);
3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Nomor 6400);
4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

5. 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);
6. 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);
7. Peraturan Wali Kota Nomor 18 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kota Banjar Tahun 2023 Nomor 18);

MEMUTUSKAN:

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

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:

1. Daerah Kota adalah Daerah Kota Banjar.
2. Pemerintah Daerah Kota adalah Wali Kota sebagai unsur penyelenggara pemerintah daerah yang memimpin pelaksanaan urusan pemerintah yang menjadi kewenangan daerah.
3. Wali Kota adalah Wali Kota Banjar.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Banjar.
5. Perangkat Daerah adalah unsur pembantu Wali Kota dan Dewan Perwakilan Rakyat Daerah dalam menyelenggarakan urusan pemerintahan yang menjadi kewenangan 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

Peraturan Wali Kota ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah.

BAB II KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu Umum

Pasal 3

- (1) 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.
- (2) 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.

Bagian Kedua Penetapan Ruang Lingkup

Pasal 4

- (1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 3 ayat (1) 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 Pemerintah Daerah yang harus diamankan dalam SPBE.

Bagian Ketiga
Penetapan Penanggung Jawab

Pasal 5

- (1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf b dilaksanakan oleh Wali Kota.
- (2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
- (3) Sekretaris Daerah sebagai penanggung jawab sebagaimana dimaksud pada ayat (1) merupakan ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan.

Pasal 6

- (1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen keamanan informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 5 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 Pemerintah Daerah.

Pasal 7

- (1) Ketua tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah, yang meliputi :
 - 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 Instansi Pusat atau koordinator SPBE Pemerintah Daerah Provinsi.
- (2) Anggota tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf b mempunyai tugas :

- a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada setiap Perangkat Daerah;
- 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

Bagian Keempat Perencanaan

Pasal 8

- (1) Perencanaan sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf c ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.
- (2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
 - a. program kerja Keamanan SPBE 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 ayat (2) huruf a, ditentukan sesuai dengan ketentuan peraturan perundang-undangan.
- (5) Target realisasi program kerja Keamanan SPBE pada ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 9

Edukasi kesadaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (3) huruf a dilaksanakan paling sedikit melalui kegiatan:

- a. sosialisasi; dan
- b. pelatihan.

Pasal 10

Penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 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 11

- (1) Peningkatan Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (3) huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan SPBE.
- (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 12

Penanganan insiden Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 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 13

Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (3) huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima Dukungan Pengoperasian

Pasal 14

- (1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf d dilakukan oleh koordinator SPBE.
- (2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
 - a. sumber daya manusia Keamanan SPBE; dan
 - b. anggaran keamanan SPBE.
- (3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen keamanan informasi SPBE diberikan alokasi sumber daya yang sesuai.

Pasal 15

- (1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan memiliki kompetensi:
 - a. keamanan TIK; dan
 - b. keamanan aplikasi.

- (2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus adanya dukungan kegiatan:
 - a. pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi dan TIK; dan/atau
 - b. bimbingan teknis mengenai standar teknis dan prosedur Keamanan SPBE.
- (3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia Keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan SPBE.
- (4) Teknologi keamanan informasi sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.
- (5) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Keenam Evaluasi Kinerja

Pasal 16

- (1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf e dilakukan oleh koordinator SPBE.
- (2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah.
- (3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
 - a. 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 Keenam Perbaikan Berkelanjutan Terhadap Keamanan Informasi

Pasal 17

- (1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf f dilakukan oleh pelaksana teknis Keamanan SPBE.
- (2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.

- (3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
 - a. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE;
 - b. memperbaiki pelaksanaan Keamanan SPBE secara periodik; dan
 - c. tindak lanjut hasil audit Keamanan SPBE.

Bagian Ketujuh Manajemen Risiko

Pasal 18

- (1) Manajemen risiko sebagaimana dimaksud dalam Pasal 3 ayat (2) huruf a dilakukan oleh setiap Perangkat Daerah.
- (2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko 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.

Bagian Kedelapan Penetapan Prosedur Pengendalian Keamanan Informasi SPBE

Pasal 19

- (1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 3 ayat (2) huruf b ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.
- (2) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah Kota 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;
 - t. perencanaan pemulihan bencana terhadap layanan TIK;
 - u. audit internal keamanan SPBE; dan/atau
 - v. aspek prosedur pengendalian keamanan informasi SPBE lainnya.
- (3) Ketentuan lebih lanjut mengenai penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) ditetapkan dengan Keputusan Wali Kota.

Pasal 20

- (1) Setiap Perangkat Daerah 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.

Bagian Kesembilan Pengelolaan Pihak Ketiga

Pasal 21

- (1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 3 ayat (2) huruf c dilakukan oleh setiap Perangkat Daerah.
- (2) Perangkat Daerah 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 memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
- (4) Perangkat Daerah harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerja sama dengan pihak ketiga.
- (5) Perangkat Daerah harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB III
KETENTUAN PENUTUP

Pasal 22

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 Banjar.

Ditetapkan di Banjar
pada tanggal 27 April 2023
WALI KOTA BANJAR,

ttd

ADE UU SUKAESIH

Diundangkan di Banjar
pada tanggal 27 April 2023
SEKRETARIS DAERAH KOTA BANJAR,

ttd

ADE SETIANA

BERITA DAERAH KOTA BANJAR TAHUN 2023 NOMOR 38

Salinan sesuai dengan aslinya,
KEPALA BAGIAN HUKUM,
SETDA
MASEP YANI TARUNA, SH.,M.AP
NIP.19710503 200604 1 010
BANJAR