SALINAN

BUPATI BANDUNG BARAT
PROVINSI JAWA BARAT

PERATURAN BUPATI BANDUNG BARAT

NOMOR 22 TAHUN 2025

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI BANDUNG BARAT,

Menimbang : a. bahwa informasi merupakan aset strategis dalam penyelenggaraan pemerintah berbasis elektronik sehingga perlu mewujudkan proses kerja yang efisien dan efektif serta meningkatkan kualitas pelayanan publik;

b. bahwa untuk menjamin keamanan dan melaksanakan manajemen keamanan informasi dalam rangka menjamin kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan sumber daya terkait data dan informasi, Infrastruktur sistem pemerintahan berbasis elektronik, dan Aplikasi sistem pemerintahan berbasis elektronik;

c. bahwa berdasarkan ketentuan Pasal 48 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi perlu melaksanakan manajemen keamanan informasi;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat : 1. Undang-Undang Nomor 12 Tahun 2007 tentang Pembentukan Kabupaten Bandung Barat di Provinsi Jawa Barat (Lembaran Negara Republik Indonesia Tahun 2007 Nomor 14, Tambahan Lembaran Negara Republik Indonesia Nomor 4688);

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 beberapa kali diubah, terakhir dengan Undang Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);
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 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);
4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185);
5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
6. 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);
7. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
8. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE (Berita Negara Republik Indonesia Tahun 2021 Nomor 541).
9. Peraturan Daerah Kabupaten Bandung Barat Nomor 4 Tahun 2019 tentang Penyelenggaraan Komunikasi, Informatika dan Statistik (Lembaran Daerah Kabupaten Bandung Barat Tahun 2019 Nomor 4, Tambahan Lembaran Daerah Kabupaten Bandung Barat Nomor 3);
10. Peraturan Bupati Kabupaten Bandung Barat Nomor 3 Tahun 2023 tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Bandung Barat Tahun 2023 Nomor 3);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK**.**

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah Kabupaten yang selanjutnya disebut Daerah adalah Daerah Kabupaten Bandung Barat.
2. Pemerintahan Daerah adalah penyelenggaraan urusan Pemerintahan oleh Pemerintah Daerah dan Dewan Perwakilan Rakyat Daerah menurut asas otonomi dan tugas pembantuan dengan prinsip otonomi seluas-luasnya dalam sistem dan prinsip Negara Kesatuan Republik Indonesia sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
3. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
4. Bupati adalah Bupati Bandung Barat.
5. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
6. Teknologi Informasi dan Komunikasi selanjutnya disebut TIK adalah terminologi yang mencakup seluruh peralatan teknis untuk memproses dan menyampaikan informasi.
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
8. Aplikasi adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan.
9. Infrastruktur 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.
10. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko.
11. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan informasi.
12. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja dari layanan Sistem Elektronik.

13. Manajemen risiko adalah aktivitas terkoordinasi untuk identifikasi, penilaian, dan penentuan prioritas risiko yang kemudian akan dikelola, dipantau, dan dikontrol untuk mengurangi dampak dan/ atau kemungkinan terjadinya risiko tersebut.
14. Audit Keamanan Informasi adalah Audit TIK cakupan keamanan informasi.
15. Tim Pelaksana Sistem Manajemen Keamanan Informasi yang selanjutnya disebut Tim SMKI adalah sekelompok orang yang bertanggung jawab untuk menyusun, mengkomunikasikan, memastikan, dan memantau pelaksanaan SMKI di Pemerintah Kabupaten Bandung Barat.
16. Keamanan jaringan adalah perlindungan sistem dan data dalam jaringan dari ancaman seperti *hacker, virus*, pencurian data, atau serangan siber.
17. Keamanan pusat data adalah perlindungan terhadap data, perangkat keras, dan sistem jaringan yang berada di dalam pusat data dari ancaman.
18. Keamanan perangkat endpoint adalah perlindungan terhadap perangkat pengguna yang terhubung ke jaringan organisasi, untuk mencegah akses tidak sah, serangan *malware*, pencurian data, atau eksploitasi sistem dari titik akhir tersebut.
19. Keamanan *remote working* adalah langkah-langkah dan kebijakan yang diterapkan untuk melindungi data, sistem, dan jaringan perusahaan saat karyawan menggunakan koneksi internet publik maupun pribadi.
20. Penerapan kriptografi adalah penggunaan teknik-teknik pengamanan data menggunakan algoritma matematika untuk memastikan kerahasiaan, integritas, dan keaslian informasi dalam berbagai sistem digital dan komunikasi.

Pasal 2

(1) Maksud Peraturan Bupati Bandung Barat ini adalah sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan Pemerintah Kabupaten Bandung Barat.

(2) Tujuan Peraturan Bupati adalah sebagai pedoman pengelolaan sistem manajemen keamanan informasi secara terpadu untuk memastikan terjaganya kerahasiaan, keutuhan dan ketersediaan.

(3) Pengelolaan sistem manajemen keamanan informasi sebagaimana di maksud pada ayat (2) meliputi:

a. infrastruktur;
b. komputer;
c. jaringan;
d. sistem;
e. informasi/aplikasi; dan
f. sumber daya manusia.

BAB II

KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 3

(1) Kebijakan Internal SMKI dilakukan dengan proses sebagai berikut:

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 (1) dapat menerapkan pengendalian teknis keamanan yang meliputi:

a. manajemen risiko;

b. penetapan prosedur pengendalian keamanan informasi SPBE; dan

c. pengelolaan pihak ketiga.

(3) Penetapan ruang lingkup sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf a meliputi:

a. Data dan Informasi SPBE;

b. Aplikasi SPBE; dan

c. Infrastruktur SPBE;

(4) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Kabupaten Bandung Barat yang harus diamankan.

Pasal 4

(1) Penanggung jawab sebagaimana dimaksud dalam pasal 3 ayat (1) huruf b, ditetapkan oleh Bupati.

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

(3) Sekretaris Daerah sebagaimana dimaksud pada ayat (1) juga melaksakan tugas sebagai koordinator SPBE.

Pasal 5

(1) Dalam melaksanakan tugas sebagai penanggung jawab SMKI, Koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) menetapkan Tim SMKI.

(2) Tim SMKI sebagaimana dimaksud pada ayat (1) terdiri atas:

a. ketua Tim SMKI; dan

b. anggota Tim SMKI.

(3) Ketua Tim SMKI sebagaimana dimaksud pada ayat (2) huruf a, dapat dijabat oleh Kepala perangkat daerah yang menyelenggarakan urusan pemerintahan di bidang Informasi dan komunikasi publik.

(4) Anggota Tim SMKI sebagaimana dimaksud pada ayat (2) huruf b, terdiri dari pimpinan perangkat Daerah yang memiliki, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Insfrastruktur SPBE.

Pasal 6

(1) Ketua Tim SMKI sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE meliputi:

a. menetapkan prosedur pengendalian keamanan informasi SPBE;

b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE;

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 dalam bentuk dokumen keberlangsungan bisnis dan perencanaan pemulihan; dan

f. melaporkan pelaksanaan manajemen keamanan informasi SPBE dan penerapan standar teknis dan prosedur Keamanan SPBE kepada koordinator SPBE.

(2) Anggota Tim SMKI 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 ketentuan peraturan perundang- undangan;

c. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen keberlangsungan bisnis dan perencanaan pemulihan; dan

d. berkoordinasi dengan ketua Tim SMKI terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 7

(1) Perencanaan sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf c, ditetapkan oleh ketua Tim SMKI 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 pada 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 pada Pasal 7 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 9

(1) Dukungan pengopersian 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

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 informasi sebagaimana dimaksud pada Pasal 9 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.

(5) Anggaran Keamanan SPBE sebagaimana dimaksud pada 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 3 ayat (1) huruf e dilakukan oleh kordinator SPBE.

(2) Evaluasi kinerja sebagaimana dimaksud ayat (1) dilakukan terhadap pelaksanaan manajemen keamanan informasi SPBE.

(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.

(5) Hasil evaluasi kinerja didokumentasikan digunakan sebagai bahan evaluasi kinerja keamanan informasi berikutnya.

Pasal 12

(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 informasi secara periodik.

c. tindak lanjut hasil audit Keamanan SPBE.

BAB III

PENGENDALIAN TEKNIS KEAMANAN

Pasal 13

(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 terdiri atas:

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 sebagaimana dimaksud dalam Pasal 3 ayat (2) huruf b, ditetapkan oleh Bupati.

(2) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1), digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE di Lingkungan Pemerintah Kabupaten dengan cangkupan aspek 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. keberlangsungan bisnis;

t. perencanaan pemulihan bencana terhadap layanan TIK;

u. audit internal keamanan SPBE; dan/atau

v. aspek prosedur pengendalian keamanan informasi SPBE lainnya.

Pasal 15

(1) Setiap Perangkat Daerah melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada 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 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 menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama dengan pihak ketiga.

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

(6) Pelaporan sebagaimana dimaksud pada ayat (5) disampaikan kepada Koordinator SPBE.

BAB VI

KETENTUAN PENUTUP

Pasal 17

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Bandung Barat.

Ditetapkan di Ngamprah
pada tanggal 15 Agustus 2025
BUPATI BANDUNG BARAT,

ttd.

JEJE RITCHIE ISMAIL

Diundangkan di Ngamprah
pada tanggal 15 Agustus 2025
SEKRETARIS DAERAH
KABUPATEN BANDUNG BARAT,

ttd.

ADE ZAKIR

BERITA DAERAH KABUPATEN BANDUNG BARAT TAHUN 2025 NOMOR 23