



BUPATI SUMBAWA BARAT

PROVINSI NUSA TENGGRA BARAT

PERATURAN BUPATI SUMBAWA BARAT

NOMOR 25 TAHUN 2025

TENTANG

MANAJEMEN KEAMANAN INFORMASI

SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DI LINGKUNGAN PEMERINTAHAN KABUPATEN SUMBAWA BARAT

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI SUMBAWA BARAT,

- Menimbang : a. bahwa dalam rangka penyelenggaraan sistem pemerintahan berbasis elektronik yang aman, efektif, efisien, dan berkesinambungan serta berkualitas, perlu melakukan manajemen terhadap sistem pemerintahan berbasis elektronik;
- b. bahwa untuk memberikan landasan serta payung hukum terhadap penerapan manajemen sistem pemerintahan berbasis elektronik maka diperlukan suatu pengaturan;
- c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b perlu menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Sumbawa Barat;
- Mengingat : 1. Pasal 18 Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 30 Tahun 2003 tentang Pembentukan Kabupaten Sumbawa Barat di Provinsi Nusa Tenggara Barat (Lembaran Negara Republik Indonesia Tahun 2003 Nomor 145, Tambahan Lembaran Negara Republik Indonesia Nomor 4340);

✓ 4

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 beberapa kali 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);
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 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);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. 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);

8. 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);
9. Peraturan Bupati Sumbawa Barat Nomor 21 Tahun 2023 tentang Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Daerah (Berita Daerah Kabupaten Sumbawa Barat Tahun 2023 Nomor 23)

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN SUMBAWA BARAT.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam peraturan bupati ini, yang dimaksud dengan:

1. Daerah adalah Kabupaten Sumbawa Barat;
2. Bupati adalah Bupati Sumbawa Barat;
3. Pemerintah Daerah adalah Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonomi.
4. Sekretaris Daerah adalah Sekretaris Pemerintah Kabupaten Sumbawa Barat;
5. Perangkat Daerah yang selanjutnya disingkat SKPD adalah unsur pembantu kepala daerah dan Dewan Perwakilan Rakyat Daerah dalam menyelenggarakan urusan pemerintahan yang menjadi kewenangan daerah;
6. Dinas adalah Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan 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. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media;
9. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
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. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas Informasi elektronik.
13. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
14. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
15. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan system, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.

#### Pasal 2

- (1) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal manajemen Keamanan Informasi SPBE di Daerah.
- (2) Kebijakan internal manajemen Keamanan Informasi SPBE sebagaimana dimaksud ayat (1) meliputi :
  - a. penetapan ruang lingkup;
  - b. penetapan penanggung jawab;

YU

- 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 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 Bupati.
- (2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
- (3) Sekretaris Daerah sebagai penanggung jawab merupakan ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan peraturan perundang undangan.

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.

✓ M

- (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 Daerah.

#### Pasal 6

- (1) Ketua tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen Keamanan Informasi SPBE di Daerah yang meliputi:
  - a. menetapkan prosedur pengendalian Keamanan Informasi SPBE Daerah;
  - b. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE di 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. mengoordinasikan, memantau dan menerima laporan pengelolaan insiden Keamanan Informasi;
  - f. mendokumentasikan proses pengelolaan insiden Keamanan Informasi;
  - g. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen business continuity dan disaster recovery plans; dan
  - h. 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. mengoordinasikan, memantau dan mengelola insiden Keamanan Informasi di Perangkat Daerah masing-masing;
  - d. mengirim laporan pengelolaan insiden Keamanan Informasi kepada ketua tim;
  - e. mendokumentasikan proses pengelolaan insiden Keamanan Informasi di Perangkat Daerah masing-masing;
  - f. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *bussiness continuity* dan *disaster recovery plans*; dan
  - g. 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 dilakukan oleh 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 SPB 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.

#### Pasal 10

- (1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam pasal 9 ayat (2) huruf a, harus memiliki kompetensi:
  - a. keamanan infrastruktur 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 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 Daerah;
- (3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
  - a. menganalisa 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) tahun;
- (5). Laporan hasil evaluasi kinerja sebagaimana yang dimaksud pada ayat (1) dilaporkan kepada Bupati, Badan Siber dan Sandi Negara dan instansi terkait.

#### 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 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

#### SUMBER DAYA

#### 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 pada 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 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) ditetapkan oleh koordinator SPBE.

#### Pasal 15

- (1) Setiap Perangkat Daerah harus 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 2 ayat (3) huruf c dilakukan oleh setiap Perangkat Daerah;
- (2) Perangkat Daerah 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) Perangkat Daerah harus 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 kerjasama dengan pihak ketiga;
- (5) Perangkat Daerah harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek Keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV  
PENGHARGAAN

Pasal 17

- (1) Bupati memberikan penghargaan kepada Perangkat Daerah yang melaksanakan manajemen Keamanan Informasi SPBE dengan baik.
- (2) Penghargaan sebagaimana dimaksud pada ayat (1) didasarkan pada kriteria penilaian dalam bentuk pemeringkatan yang merupakan hasil dari :
  - a. monitoring dan evaluasi; dan
  - b. penilaian ahli.
- (3) Pemeringkatan sebagaimana dimaksud pada ayat (2) diberikan kategori predikat:
  - a. sangat baik;
  - b. baik;
  - c. cukup; dan
  - d. kurang baik.
- (4) Dinas menyusun kriteria penilaian dan bentuk penghargaan sebagaimana dimaksud pada ayat (2).
- (5) Dalam memberikan penghargaan sebagaimana dimaksud pada ayat (1) terlebih dahulu dilakukan penilaian oleh tenaga ahli.
- (6) Tenaga ahli sebagaimana dimaksud pada ayat (5) ditetapkan dengan keputusan Bupati.

BAB V  
PENDANAAN

Pasal 18

Pendanaan penyelenggaraan Manajemen Keamanan Informasi SPBE bersumber pada :

- a. anggaran pendapatan dan belanja daerah (APBD); dan
- b. Sumber pendanaan lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI  
KETENTUAN PENUTUP

Pasal 19

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Taliwang  
pada tanggal 10 September 2025

BUPATI SUMBAWA BARAT



Diundangkan di Taliwang  
pada tanggal 10 September 2025

SEKRETARIS DAERAH KABUPATEN SUMBAWA BARAT



BERITA DAERAH KABUPATEN SUMBAWA BARAT TAHUN 2025 NOMOR 25