



BUPATI BANYUMAS  
PROVINSI JAWA TENGAH

PERATURAN BUPATI BANYUMAS  
NOMOR 8 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI  
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK  
DI LINGKUNGAN PEMERINTAH KABUPATEN BANYUMAS

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI BANYUMAS,

- Menimbang : a. bahwa setiap orang berhak untuk berkomunikasi dan memperoleh Informasi untuk mengembangkan pribadi dan lingkungan sosialnya, serta berhak untuk mencari, memperoleh, memiliki, dan menyimpan Informasi dengan menggunakan segala jenis saluran yang tersedia;
- b. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Kabupaten Banyumas, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;
- c. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Banyumas dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai manajemen keamanan informasi sistem pemerintahan berbasis elektronik;
- 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 di Lingkungan Pemerintah Kabupaten Banyumas;
- Mengingat : 1. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten dalam Lingkungan Propinsi Djawa Tengah (Berita Negara Republik Indonesia Tahun 1950 Nomor 42);

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 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 6841, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

#### MEMUTUSKAN:

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

#### BAB I

#### KETENTUAN UMUM

#### Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
2. Daerah adalah Kabupaten Banyumas.
3. Bupati adalah Bupati Banyumas.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Banyumas.
5. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan 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. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.
8. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisa, dan/atau menyebarkan Informasi.
9. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
10. 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.
11. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
12. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan Keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
13. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan (*confidentiality*) atas Informasi dan Komunikasi secara elektronik.
14. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas informasi elektronik.
15. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas informasi elektronik.
16. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan SPBE.

17. 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) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan Pemerintah 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 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) Ruang lingkup yang ditetapkan pada ayat (1) merupakan aset Pemerintah 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 ketentuan peraturan perundang-undangan.

#### Pasal 5

- (1) Koordinator SPBE dalam melaksanakan tugas 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 dan/atau Infrastruktur SPBE di lingkungan Pemerintah 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 Pemerintah Daerah;
  - b. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE di lingkungan Pemerintah Daerah;
  - c. memastikan penerapan keamanan Aplikasi dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan;
  - d. merumuskan, mengkoordinasikan, 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. mengkoordinasikan dan/atau memastikan penerapan prosedur pengendalian Keamanan Informasi pada Perangkat Daerah masing-masing;
  - b. memastikan penerapan keamanan Aplikasi 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. berkoordinasi dengan ketua tim terkait penerapan keamanan Aplikasi 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 5 (lima) orang dengan ketentuan harus memiliki kompetensi:
  - a. keamanan infrastruktur Teknologi Informasi dan Komunikasi; dan
  - b. keamanan aplikasi.
- (2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus ada dukungan kegiatan:
  - a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur Teknologi Informasi dan Komunikasi dan keamanan aplikasi; dan
  - 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 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 dapat 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 diatur 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 Bupati.
- (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 meliputi:
- a. keamanan perangkat Teknologi Informasi dan 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 keamanan teknologi Informasi (*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) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk Keputusan Bupati.

#### 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 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 kerja sama dengan pihak ketiga.
- (5) Perangkat Daerah harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan (*service level agreement/SLA*) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

### BAB IV

### 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 Banyumas.

Ditetapkan di Purwokerto  
pada tanggal 1 April 2024

Pj. BUPATI BANYUMAS,

ttd

HANUNG CAHYO SAPUTRO

Diundangkan di Purwokerto  
pada tanggal 1 April 2024

Pj. SEKRETARIS DAERAH  
KABUPATEN BANYUMAS,

ttd

JUNAIDI

BERITA DAERAH KABUPATEN BANYUMAS TAHUN 2024  
NOMOR 9

Salinan sesuai dengan aslinya

KEPALA BAGIAN HUKUM  
SETDA KABUPATEN BANYUMAS,



Ditandatangani secara  
elektronik oleh :

ARIF ROHMAN, S.H., M.H.

Pembina

NIP. 197505312009031002