SALINAN

BUPATI BANJARNEGARA
PROVINSI JAWA TENGAH

PERATURAN BUPATI BANJARNEGARA
NOMOR 6 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAH BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI BANJARNEGARA,

Menimbang :

a. bahwa dalam rangka memanfaatkan sistem pemerintahan berbasis elektronik agar dapat memberikan manfaat bagi perkembangan perekonomian daerah dan kemanfaatan umum, perlu disusun manajemen kemananan informasi;
b. bahwa dalam rangka penyelenggaraan pemerintah secara elektronik yang aman di lingkungan Pemerintah Kabupaten Banjarnegara, 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 Banjarnegara dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai sistem manajemen keamanan informasi Sistem Pemerintah 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 Pemerintah Berbasis Elektronik;

Mengingat :

1. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten Dalam Lingkungan Provinsi Jawa Tengah;

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 diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
3. 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);
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 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);
5. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
6. Peraturan Menteri Komunikasi Dan Informatika Nomor 41/PER/ME.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi Dan Komunikasi Nasional (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 4843);
7. Peraturan Menteri Komunikasi Dan Informasi Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);

MEMUTUSKAN :

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

BAB 1
KETENTUAN UMUM

Bagian Kesatu
Pengertian

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:
1. Daerah adalah Kabupaten Banjarnegara.
2. Bupati adalah Bupati Banjarnegara.
3. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Banjarnegara
4. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
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. 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 terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi.
9. 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.
10. Manajemen Risiko adalah pendekatan sistematis yang meliputih proses, pengukuran, struktur dan budaya untuk menetukan Tindakan terbaik terkait Risiko.
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 integrase/penghubung, dan perangkat Elektronik lainnya.
13. Pihak ketiga adalah pembuat, pengembang, pengelola Aplikasi dan Infrastruktur SPBE.

Bagian Kedua
Maksud dan Tujuan

Pasal 2

(1) Maksud Peraturan Bupati ini adalah sebagai pedoman bagi Pemerintah Daerah dalam melaksanakan kebijakan, program, dan kegiatan SMKI untuk pengamanan Sistem Informasi.
(2) Tujuan Peraturan Bupati ini adalah sebagai pedoman pengelolaan SMKI secara terpadu untuk memastikan terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).

(3) Pengelolaan SMKI sebagaimana dimaksud pada ayat (2) meliputi infrastruktur komputer, jaringan, sistem informasi/aplikasi, dan sumber daya manusia.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 3

(1) Kebijakan internal SMKI meliputi :
   a. penetapan ruang lingkup;
   b. penetapan penanggung jawab;
   c. perencanaan;
   d. dukungan pengoprasian;
   e. evaluasi kinerja;
   f. perbaikan berkelanjutan terhadap keamanan informasi.
(2) Ketentuan lain untuk mendukung kebijakan internal SMKI sebagaimana dimaksud pada ayat (1) dapat menerapkan pengendalian teknis keamanan yang meliputi :
   a. manajemen risiko;
   b. penetapan prosedur pengendalian keamanan informasi; dan
   c. pengelolaan pihak ketiga.
(3) Penetapan ruang lingkup SMKI sebagaimana dimaksud pada ayat (2) huruf a meliputi :
   a. data dan informasi SPBE;
   b. aplikasi SPBE;
   c. infrastruktur SPBE; dan
   d. kebijakan keamanan informasi SPBE.
(4) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Daerah yang harus diamankan.

Pasal 4

(1) Bupati menetapkan penanggung jawab sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf b.
(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
(3) Sekretaris Daerah sebagaimana dimaksud pada ayat (2) merupakan koordinator SPBE.

Pasal 5

(1) Dalam melaksanakan tugas sebagai penanggung jawab dan koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (2) dan ayat (3), Sekretaris Daerah 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 adalah Kepala Perangkat Daerah yang menyelenggarakan urusan pemerintahan bidang Komunikasi dan Informatika, bidang Persandian, dan bidang Statistik.
(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.

Pasal 6

(1) Ketua tim 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 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) Ketua tim pelaksana teknis Keamanan SPBE menetapkan Perencanaan sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf c.
(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 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
    b. keamanan aplikasi dan TIK; dan/atau
    c. 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) Koordinator SPBE melakukan evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf e.
(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen keamanan informasi SPBE.
(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) Pelaksana teknis Keamanan SPBE melakukan perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf f.
(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) Setiap kepala perangkat daerah melakukan manajemen risiko sebagaimana dimaksud dalam Pasal 3 ayat (2) huruf a.
(2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko (*risk register*) dengan ketentuan subtansi 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 sesuai dengan ketentuan peraturan perundang- undangan.

Pasal 14

(1) Ketua tim pelaksana teknis Keamanan SPBE menetapkan prosedur pengendalian keamanan informasi sebagaimana dimaksud dalam Pasal 3 ayat (2) huruf b.
(2) Penetapan prosedur pengendalian keamanan informasi sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE 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. 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 sebagaimana dimaksud pada ayat (2) ditetapkan dalam bentuk :
a. Keputusan Bupati;
b. surat edaran Sekretaris Daerah; atau
c. kebijakan teknis lainnya.

Pasal 15

(1) Setiap perangkat daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi 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 3 ayat (2) huruf c dapat dilakukan oleh 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 (*Service Level Agreement*/SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
PEMBIAYAAN

Pasal 17

(1) Pelaksanaan Manajemen Keamanan Informasi SPBE dibiayai dari Anggaran Pendapatan dan Belanja Daerah.
(2) Selain pembiayaan sebagaimana dimaksud pada ayat (1), Pelaksanaan Manajemen Keamanan Informasi SPBE dapat dibiayai dari sumber pendapatan lain yang sah dan tidak mengikat.

BAB V
KETENTUAN PENUTUP

Pasal 18

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Pemerintah Kabupaten Banjarnegara.

Ditetapkan di Banjarnegara
pada tanggal 18-1-2024

Pj. BUPATI BANJARNEGARA,

Cap ttd,

TRI HARSO WIDIRAHMANTO

Diundangkan di Banjarnegara
pada tanggal 18-1-2024

SEKRETARIS DAERAH KABUPATEN BANJARNEGARA,

Cap ttd,

INDARTO

BERITA DAERAH KABUPATEN BANJARNEGARA TAHUN 2024 NOMOR 6

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

Syahbudin Usmoyo, SH
Pembina Tk. I
NIP. 19740223 199803 1 006