SALINAN

PERATURAN BUPATI BREBES

NOMOR 98 TAHUN 2024

TENTANG

PEDOMAN MANAJEMEN KEAMANAN INFORMASI

SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI BREBES,

Menimbang : a. bahwa untuk menjamin keberlangsungan sistem pemerintahan berbasis elektronik dengan meminimalkan dampak resiko keamanan elektronik, perlu manajemen keamanan informasi dalam mencapai penerapan keamanan sistem pemerintahan berbasis elektronik yang efektif, efisien, dan berkesinambungan, serta mendukung layanan;

b. bahwa Manajemen Keamanan Informasi dilakukan melalui serangkaian proses yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap keamanan informasi dalam sistem pemerintahan berbasis elektronik;

c. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur sistem pemerintahan berbasis elektronik 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 Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat : 1. Pasal 18 Ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten dalam Lingkungan Propinsi Jawa Tengah (Berita Negara Republik Indonesia Tahun 1950 Nomor 42);

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 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);

4. Undang-Undang Nomor 11 Tahun 2023 tentang Provinsi Jawa Tengah (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 6867);

MEMUTUSKAN:

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

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Brebes.
2. Bupati adalah Bupati Brebes.
3. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
4. Perangkat Daerah adalah unsur pembantu Bupati dalam penyelenggaraan pemerintah daerah yang terdiri sekretariat daerah, sekretariat DPRD, dinas daerah, Lembaga teknis daerah, kecamatan, dan kelurahan.
5. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
6. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
7. 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.
8. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan *(nonrepudiation)* sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
9. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE

yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.

10. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
11. 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.
12. Rencana Bisnis Berkelanjutan (*Business Continuity Plan)* adalah strategi preventif dan kuratif dalam menjamin keberlangsungan layanan SPBE.
13. Tim Pelaksana Teknis Keamanan SPBE adalah Tim yang bertugas dalam melaksanakan keamanan SPBE di lingkungan Pemerintah Kabupaten Brebes.
14. Tim Tanggap Insiden Keamanan Komputer Pemerintah *(Government Computer Security Incident Response Team)* yang selanjutnya disingkat GCSIRT adalah Tim yang bertugas melaksanakan penanganan insiden Keamanan Informasi di lingkungan Pemerintah Daerah.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai pedoman 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) Guna mendukung kebijakan internal Manajemen Keamanan Informasi SPBE sebagaimana dimaksud

pada ayat (2) dapat menerapkan Tata Kelola Keamanan Informasi yang meliputi:

a. prosedur pengendalian Keamanan Informasi SPBE;
b. manajemen risiko; dan
c. pengelolaan pihak ketiga.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN 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 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) Dalam melaksanakan tugas sebagai penanggung jawab, sekretaris disebut sebagai koordinator SPBE.

Pasal 5

(1) Dalam melaksanakan tugas sebagai penanggung jawab Manajemen Keamanan Informasi SPBE, 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 dijabat oleh Kepala Perangkat Daerah yang membidangi urusan pemerintahan bidang Komunikasi dan Informatika.

(4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh Kepala Perangkat Daerah lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE 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. merumuskan prosedur pengendalian Keamanan Informasi SPBE Pemerintah Daerah;
b. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE di lingkungan Pemerintah Daerah;
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, mengkoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE; dan
e. melaporkan pelaksanaan manajemen Keamanan Informasi SPBE kepada 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 SPBE pada setiap 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 Rencana Bisinis Berkelanjutan *(Business Continuity Plan)* dan Rencana Pemulihan Bencana (*Disaster Recovery Plan)*; dan
d. 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 ditetapkan oleh Ketua Tim Pelaksana Teknis Keamanan SPBE.
(2) Perencanaan sebagaimana dimaksud pada ayat (1) berupa penyusunan:
    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 pada 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 memadai.

Pasal 10

(1) Sumber Daya Manusia Keamanan SPBE sebagaimana dimaksud pada pasal 9 ayat (2) huruf a paling sedikit berjumlah 10 (sepuluh) orang yang memiliki kompetensi:
   a. keamanan infrastruktur teknologi, informasi dan komunikasi; dan
   b. keamanan aplikasi.

(2) Untuk memenuhi kompetensi Sumber Daya Manusia Keamanan SPBE sebagaimana dimaksud pada ayat (1), mensyaratkan:
   a. mengikuti pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi dan infrastruktur;
   b. mengikuti bimbingan teknis mengenai standar teknis dan prosedur Keamanan SPBE; dan/atau
   c. memiliki pengalaman kerja.

(3) Teknologi Keamanan SPBE sebagaimana dimaksud pada pasal 9 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

(4) 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 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. 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 kualitatif 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.

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. menindaklanjuti hasil audit Keamanan SPBE.

BAB III
TATA KELOLA KEAMANAN INFORMASI

Pasal 13

(1) Prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf a dirumuskan oleh Tim Pelaksana Teknis Keamanan SPBE.

(2) Rumusan prosedur pengendalian Kemanan Informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan Manajemen Keamanan nformasi SPBE di lingkungan Pemerintah Daerah meliputi aspek :

a. keamanan perangkat teknologi informasi komunikasi;
b. keamanan jaringan;
c. kemanan pusat data;
d. keamanan perangkat titik akhir (*end point*);
e. keamanan pekerjaan remot (*remote working*);
f. kemanan 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 TIK;
k. keamanan migrasi data;
l. konfigurasi perangkat keamanan teknologi informasi (*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. audit internal keamanan SPBE; dan/ atau
t. aspek prosedur pengendalian Keamanan Informasi SPBE lainnya sesuai dengan ketentuan peraturan perundang-undangan.

(3) Prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) diatur lebih lanjut dalam keputusan Kepala Perangkat Daerah yang menyelenggarakan urusan pemerintahan bidang Komunikasi dan Informatika.

Pasal 14

(1) Data dan informasi SPBE sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf a, diklasifikasikan tingkat kerahasiaannya menjadi:
a. sangat rahasia;
b. rahasia;
c. internal; dan
d. publik

(2) Aplikasi SPBE dan Infrastruktur SPBE sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf b dan huruf c, diklasifikasikan berdasarkan asas risiko menjadi:
a. strategis;
b. tinggi; dan
c. rendah;

(3) Daftar aset dan klasifikasi sebagaimana dimaksud pada ayat (1) dan ayat (2) ditetapkan dengan keputusan penanggung jawab Keamanan Informasi SPBE.

Pasal 15

(1) Guna menjamin keberlangsungan layanan SPBE, Pemerintah Daerah Menyusun Rencana Bisnis Berkelanjutan (*Business Continuity* Plan).

(2) Rencana Bisnis Berkelanjutan (*Business Continuity* Plan) sebagaimana dimaksud pada ayat (1) ditetapkan oleh Ketua Tim Pelaksana Teknis Keamanan SPBE.

Pasal 16

(1) Dalam melaksanakan penanganan insiden Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (1) huruf d, Ketua Tim Pelaksana Teknis Keamanan SPBE dibantu oleh GCSIRT.
(2) GCSIRT sebagaimana dimaksud pada ayat (1) memiliki tugas dalam perencanaan, mitigasi, penanganan insiden, serta pemulihan layanan pasca insiden.
(3) Keanggotaan GCSIRT sebagaimana dimaksud pada ayat (1) ditetapkan oleh Penanggung Jawab Manajemen Keamanan Informasi SPBE.

Pasal 17

(1) Pemulihan layanan pasca insiden sebagaimana dimaksud dalam Pasal 16 ayat (2) harus berpedoman pada perencanaan pemulihan bencana (*Disaster Recovery Plan*).
(2) Perencanaan pemulihan bencana (*Disaster Recovery Plan*) sebagaiman dimaksud pada ayat (1) ditetapkan oleh ketua Tim Pelaksana Teknis Keamanan SPBE.

Pasal 18

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf b dilakukan oleh setiap perangkat daerah.
(2) Prosedur pelaksanaan manajemen risiko sebagaimana dimaksud pada ayat (1) berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 19

Setiap Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian Keamanan Infomasi SPBE, sebagaimana dimaksud dalam Pasal 13.

Pasal 20

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) 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) Pihak ketiga memberikan akses sepenuhnya kepada perangkat daerah terkait pekerjaan Pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.

(4) Perangkat Daerah menetapkan kerangka acuan kerja untuk memantau layanan dan aspek Keamanan Informasi dalam hubungan kerjasama dengan pihak ketiga.

(4) Perangkat daerah membuat laporan secara berkala tentang pencapaian *(service level agreement)* dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

(5) Perangkat Daerah yang menjalin kerja sama dengan Pihak Ketiga dapat menyediakan anggaran dalam melaksanakan pengamanan SPBE.

BAB IV

KETENTUAN PENUTUP

Pasal 21

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Brebes
pada tanggal 9 Oktober 2024
Pj. BUPATI BREBES,

Ttd

DJOKO GUNAWAN

Diundangkan di Brebes
Pada tanggal 9 Oktober 2024
Pj. SEKRETARIS DAERAH
KABUPATEN BREBES

Ttd

SUTARYONO, S.H.,M.Si
Pembina Utama Muda
NIP. 19720125 199303 1 004
BERITA DAERAH KAB.BREBES
NOMOR 98 TAHUN 2024

Salinan sesuai dengan aslinya
Plt. Kepala Bagian Hukum
Setda Kabupaten Brebes

ANANTO HERI WIBOWO, SH.,M.Si
Pembina Tk. I – IV/b
NIP. 19700808 199703 1 006