SALINAN

BUPATI KEBUMEN
PROVINSI JAWA TENGAH

PERATURAN BUPATI KEBUMEN
NOMOR 33 TAHUN 2023

TENTANG

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

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI KEBUMEN,

Menimbang :

a. bahwa dalam rangka penyelenggaraan sistem pemerintahan berbasis elektronik yang aman di lingkungan Pemerintah Kabupaten Kebumen, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;
b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kebumen;

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 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 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);
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 Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Daerah Kabupaten Kebumen Nomor 4 Tahun 2018 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Kebumen (Lembaran Daerah Kabupaten Kebumen Tahun 2018 Nomor 4, Tambahan Lembaran Daerah Kabupaten Kebumen Nomor 151);

MEMUTUSKAN :

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

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:
1. Daerah adalah Kabupaten Kebumen.
2. Bupati adalah Bupati Kebumen.

3. 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.
4. Pemerintah Daerah adalah kepala Daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan Daerah otonom.
5. Perangkat Daerah adalah unsur pembantu Bupati dalam menyelenggarakan urusan pemerintahan yang menjadi kewenangan Daerah.
6. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Kebumen.
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 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.
10. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan *(availability)* atas Informasi Elektronik.
11. Manajemen Keamanan Informasi SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
12. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan SPBE.
13. 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.

Pasal 2

Peraturan Bupati ini dimaksudkan sebagai kebijakan internal Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu
Umum
Pasal 3

Kebijakan internal Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 meliputi:

a. penetapan ruang lingkup;
b. penetapan penanggung jawab;
c. perencanaan;
d. dukungan pengoperasian;
e. evaluasi kinerja; dan
f. perbaikan berkelanjutan terhadap keamanan informasi.

Bagian Kedua
Penetapan Ruang Lingkup
Pasal 4

(1) Penetapan ruang lingkup Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 3 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.

Bagian Ketiga
Penetapan Penanggung Jawab
Pasal 5

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 3 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 6

(1) Dalam melaksanakan tugas sebagai penanggung jawab Manajemen Keamanan Informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 5 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 Kepala Perangkat Daerah yang membidangi urusan 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 7

(1) Ketua tim sebagaimana dimaksud dalam Pasal 6 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 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 *business continuity* dan *disaster recovery plans*; dan
   f. melaporkan pelaksanaan Manajemen Keamanan Informasi SPBE pada koordinator SPBE.
(2) Anggota tim sebagaimana dimaksud dalam Pasal 6 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 *business continuity* dan *disaster recovery plans*; dan
   d. berkoordinasi dengan ketua tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Bagian Keempat
Perencanaan
Pasal 8

(1) Perencanaan sebagaimana dimaksud dalam Pasal 3 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 9

(1) Program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 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 8 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Bagian Kelima
Dukungan Pengoperasian
Pasal 10

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 3 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 11

(1) Sumber daya manusia keamanan SPBE sebagaimana dimaksud dalam Pasal 10 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 dalam Pasal 10 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.
(5) Anggaran keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Keenam
Evaluasi Kinerja
Pasal 12

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 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; dan
   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.

Bagian Ketujuh
Perbaikan Berkelanjutan Terhadap Keamanan Informasi.
Pasal 13

(1) Perbaikan berkelanjutan terhadap keamanan informasi sebagaimana dimaksud dalam Pasal 3 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 14

Untuk mendukung kebijakan internal Manajemen Keamanan Informasi SPBE dapat menerapkan pengendalian teknis keamanan yang meliputi:

a. manajemen risiko;
b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
c. pengelolaan pihak ketiga.

Pasal 15

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 14 huruf a dilakukan oleh setiap Perangkat Daerah.
(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 dilaksanakan sesuai dengan ketentuan peraturan perundang- undangan.

Pasal 16

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 14 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 lingkungan Pemerintah Daerah dengan cakupan aspek meliputi:
    a. keamanan perangkat TIK;
    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 *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 surat edaran Sekretaris Daerah.

Pasal 17

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 16.
(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 18

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 14 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 dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
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 Kebumen.

Ditetapkan di Kebumen
pada tanggal 9 Juni 2023

BUPATI KEBUMEN,

ttd.

ARIF SUGIYANTO

Diundangkan di Kebumen
pada tanggal 9 Juni 2023

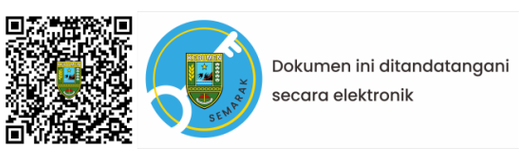
SEKRETARIS DAERAH
KABUPATEN KEBUMEN,

ttd.

AHMAD UJANG SUGIONO

BERITA DAERAH KABUPATEN KEBUMEN TAHUN 2023 NOMOR 33

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM
SEKRETARIAT DAERAH KABUPATEN KEBUMEN,



AKHMAD HARUN, S.H.
Pembina Tk. I
NIP 19690809 199803 1 006