BUPATI CILACAP
PROVINSI JAWA TENGAH

PERATURAN BUPATI CILACAP
NOMOR 31 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI CILACAP,

Menimbang :

a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Kabupaten Cilacap, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;
b. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur sistem pemerintahan berbasis elektronik di lingkungan Kabupaten Cilacap dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai manajemen keamanan informasi sistem pemerintahan berbasis elektronik;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati Cilacap tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Pemerintah Daerah;

Mengingat :

1. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten Dalam Lingkungan Propinsi Jawa Tengah;
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 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);

3. 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 MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH DAERAH.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Cilacap.
2. Bupati adalah Bupati Cilacap.
3. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Cilacap.
4. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
5. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
6. 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.
7. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
8. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
9. Penyedia Jasa adalah penyedia jasa dalam bidang pengembangan aplikasi SPBE dan infrastruktur SPBE.
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 *system*, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat *integrase*/penghubung dan perangkat elektronik lainnya.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE di Daerah meliputi:
   a. penetapan ruang lingkup;
   b. penetapan penanggung jawab;

c. perencanaan;
d. dukungan pengoperasian;
e. evaluasi kinerja; dan
f. perbaikan berkelanjutan.

(2) Ketentuan lain untuk mendukung kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) dapat menerapkan pengendalian teknis keamanan, meliputi:
a. manajemen risiko;
b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
c. pengelolaan Penyedia Jasa.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 3

(1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (1) 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 (1) 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 ketentuan peraturan perundang-undangan.

Pasal 5

(1) Dalam melaksanakan tugasnya sebagai penanggung jawab manajemen keamanan informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) menetapkan pelaksana teknis Keamanan SPBE.

(2) Pelaksana teknis Keamanan SPBE sebagaimana 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 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 lingkungan 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, 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 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 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 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.

Pasal 7

(1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (1) 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 pada ayat (1) ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 9

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 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 sebagaimana dimaksud pada ayat (1) 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 yang dilakukan secara berkala meliputi:
    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 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 ketentuan peraturan perundang-undangan.

Pasal 11

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf e dilakukan oleh koordinator SPBE.
(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen keamanan informasi SPBE.
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan dengan:
    a. menganalisis efektivitas 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 (1) 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 II
PENGENDALIAN TEKNIS KEAMANAN

Pasal 13

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (2) 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 sebagaimana dimaksud pada ayat (1) sesuai ketentuan peraturan perundang-undangan.

Pasal 14

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (2) 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 dengan cakupan 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 *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 Teknologi Informasi dan Komunikasi (*disaster recovery plans*);
u. audit internal keamanan SPBE; dan/atau
v. aspek prosedur pengendalian keamanan informasi SPBE lainnya.

(3) Prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) ditetapkan oleh Keputusan Bupati.

Pasal 15

(1) Setiap perangkat daerah melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 14 ayat (3).
(2) Perangkat daerah sebagaimana dimaksud pada ayat (1) bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian keamanan informasi SPBE.

Pasal 16

(1) Pengelolaan Penyedia Jasa sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf c dilakukan oleh setiap perangkat daerah.
(2) Perangkat daerah memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh Penyedia Jasa memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan.
(3) Perangkat daerah memastikan Penyedia Jasa memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
(4) Perangkat daerah menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerja sama dengan Penyedia Jasa.
(5) Perangkat daerah membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan Penyedia Jasa.

BAB III
KETENTUAN PENUTUP

Pasal 17

Pada saat Peraturan Bupati ini mulai berlaku, Peraturan Bupati Cilacap Nomor 23 Tahun 2022 tentang Sistem Manajemen Keamanan Informasi di Lingkungan Pemerintah Kabupaten Cilacap (Berita Daerah Kabupaten Cilacap Tahun 2022 Nomor 23), dicabut dan dinyatakan tidak berlaku lagi.

Pasal 18

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Cilacap
pada tanggal 4 September 2024

Pj. BUPATI CILACAP,

Cap&ttd

MOHAMAD ARIEF IRWANTO

Diundangkan di Cilacap
pada tanggal 4 September 2024

Plh. SEKRETARIS DAERAH
KABUPATEN CILACAP,

Cap&ttd

SUMBOWO

BERITA DAERAH KABUPATEN CILACAP TAHUN 2024 NOMOR 31