BUPATI KUDUS
PROVINSI JAWA TENGAH

PERATURAN BUPATI KUDUS
NOMOR 4 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI KUDUS,

Menimbang : a. bahwa penyelenggaraan sistem pemerintahan berbasis elektronik harus dilaksanakan berdasarkan prinsip keamanan sehingga mampu menjamin terselenggaranya urusan pemerintahan dan pelayanan masyarakat secara optimal;

b. bahwa guna melindungi sumber daya sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Kudus dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, diperlukan manajemen keamanan informasi sistem pemerintah berbasis elektronik;

c. bahwa dalam rangka tertib administrasi dan kepastian hukum pelaksanaan manajemen keamanan informasi sistem pemerintahan berbasis elektronik serta melaksanakan ketentuan Pasal 23 ayat (8) Peraturan Bupati Kudus Nomor 30 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik, perlu mengatur manajemen keamanan informasi sistem pemerintahan berbasis elektronik di Lingkungan Pemerintah Daerah;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan 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 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);
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);
4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
5. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
6. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
7. Peraturan Bupati Kudus Nomor 30 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Kabupaten Kudus (Berita Daerah Kabupaten Kudus Tahun 2022 Nomor 30);

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. Pemerintah adalah Pemerintah Pusat.
2. Daerah adalah Kabupaten Kudus.

3. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
4. Bupati adalah Bupati Kudus.
5. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
6. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Kudus.
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan dengan memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
8. 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.
9. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam 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 sistem, aplikasi, komunikasi Data, pengolahan dan penyimpanan Data, perangkat integrasi/ penghubung, dan perangkat elektronik lainnya.

Pasal 2

(1) Maksud ditetapkannya Peraturan Bupati ini sebagai kebijakan internal manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah.

(2) Kebijakan internal manajemen Keamanan Informasi SPBE sebagaimana dimaksud ayat (1) meliputi:
   a. ruang lingkup;
   b. penanggung jawab;
   c. perencanaan;
   d. dukungan pengoperasian;
   e. evaluasi kinerja; dan
   f. perbaikan berkelanjutan terhadap Keamanan Informasi.

(3) Untuk mendukung kebijakan internal manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2), dapat dilakukan pengendalian teknis keamanan yang meliputi:

a. manajemen risiko;

b. prosedur pengendalian Keamanan Informasi SPBE; dan

c. pengelolaan pihak ketiga.

BAB II

KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 3

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.

Pasal 4

(1) Penanggung jawab sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dijabat oleh Sekretaris Daerah.

(2) Sekretaris Daerah sebagai penanggung jawab merupakan ketentuan yang tidak terpisahkan dari tugas sebagai koordinator SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan.

Pasal 5

(1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen Keamanan Informasi SPBE, Sekretaris Daerah menetapkan Tim Pelaksana Teknis Keamanan SPBE.

(2) Ketua Tim sebagaimana dimaksud pada ayat (1) dijabat oleh pimpinan Perangkat Daerah yang membidangi urusan komunikasi dan informatika.

(3) Anggota Tim sebagaimana dimaksud pada ayat (1) terdiri dari fungsional atau pelaksana yang ditunjuk pada Perangkat Daerah / Unit Kerja yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Daerah.

Pasal 6

Tugas Tim Pelaksana Teknis Keamanan SPBE sebagaimana dimaksud dalam pasal 5 ayat (1) meliputi:

a. menetapkan prosedur pengendalian Keamanan Informasi SPBE;

b. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE di lingkungan Pemerintah Daerah;

c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE pada Perangkat Daerah 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. merancang, melaksanakan dan mengelola kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans*; dan

f. melaporkan pelaksanaan manajemen Keamanan Informasi SPBE pada koordinator 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.

(3) Program kerja Keamanan SPBE sebagaimana dimaksud pada 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.

(4) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 8

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf d dilakukan oleh Sekretaris Daerah selaku penanggung jawab.

(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 9

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 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.

Pasal 10

Teknologi Keamanan SPBE sebagaimana dimaksud pada pasal 8 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

Pasal 11

Anggaran Keamanan SPBE sebagaimana dimaksud pada Pasal 8 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 12

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf e dilakukan oleh Sekretaris Daerah selaku penanggung jawab.

(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 efektivitas pelaksanaan Keamanan SPBE;

b. mendukung dan merealisasikan program audit Keamanan SPBE;

c. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE;

d. menetapkan indikator kinerja pada setiap area proses; dan

e. memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan.

(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 13

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf f dilakukan oleh Tim 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

(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 meliputi:
   a. inventarisasi aset SPBE;
   b. identifikasi ancaman dan kerentanan keamanan terhadap aset SPBE;
   c. penilaian risiko keamanan terhadap asset 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 15

(1) Prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf b digunakan untuk mengimplementasikan manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah 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 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.

(2) Prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Kepala Perangkat Daerah yang melaksanakan urusan Pemerintah di bidang komunikasi dan informatika.

Pasal 16

Kepala Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi pada Perangkat Daerah berpedoman pada prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 15.

Pasal 17

(1) Perangkat Daerah yang melibatkan pihak ketiga dalam kegiatan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE harus melakukan pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf e.

(2) Pengelolaan pihak ketiga sebagaimana dimaksud pada ayat (1) untuk memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur pengendalian Keamanan SPBE.

(3) Pengelolaan pihak ketiga sebagaimana dimaksud pada ayat (1) meliputi:

a. pemberian akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya oleh pihak ketiga;

b. penetapan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek Keamanan Informasi dalam hubungan Kerjasama dengan pihak ketiga; dan

c. penyusunan laporan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
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 Daerah Kabupaten Kudus.

Ditetapkan di Kudus
pada tanggal 9 Januari 2024

Pj. BUPATI KUDUS,

BERGAS C. PENANGGUNGAN

Diundangkan di Kudus
pada tanggal 10 Januari 2024

Pj. SEKRETARIS DAERAH KABUPATEN KUDUS,

REVLISIANTO SUBEKTI

BERITA DAERAH KABUPATEN KUDUS TAHUN 2024 NOMOR 4