



SALINAN

BUPATI REMBANG
PROVINSI JAWA TENGAH

PERATURAN BUPATI REMBANG

NOMOR 31 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN
BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI REMBANG,

- Menimbang : a. bahwa berdasarkan Pasal 17 ayat (1) Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, Setiap Instansi Pusat dan Pemerintah Daerah harus menerapkan keamanan SPBE;
- b. bahwa berdasarkan Pasal 41 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, Setiap Instansi Pusat dan Pemerintah Daerah harus menerapkan keamanan SPBE;
- c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang 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 Djawa Tengah;
3. 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);

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 Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
8. Peraturan Presiden Nomor 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 99);
9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
10. 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);
11. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
12. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);

13. Peraturan Daerah Kabupaten Rembang Nomor 5 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Rembang (Lembaran Daerah Kabupaten Rembang Tahun 2016 Nomor 6, Tambahan Lembaran Daerah Kabupaten Rembang Nomor 128) sebagaimana telah diubah beberapa kali terakhir dengan Peraturan Daerah Kabupaten Rembang Nomor 6 Tahun 2021 tentang Perubahan Kedua atas Peraturan Daerah Kabupaten Rembang Nomor 5 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Rembang Lembaran Daerah Kabupaten Rembang Tahun 2021 Nomor 6, Tambahan Lembaran Daerah Kabupaten Rembang Nomor 157);
14. Peraturan Bupati Rembang Nomor 43 Tahun 2019 tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik di Kabupaten Rembang (Berita Daerah Kabupaten Rembang Tahun 2019 Nomor 46) sebagaimana telah diubah dengan Peraturan Bupati Rembang Nomor 18 Tahun 2021 tentang Perubahan atas Peraturan Bupati Nomor 43 Tahun 2019 tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik di Kabupaten Rembang (Berita Daerah Kabupaten Rembang Tahun 2021 Nomor 18);

MEMUTUSKAN:

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

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Rembang.
2. Bupati adalah Bupati Rembang.
3. Perangkat Daerah adalah Perangkat Daerah yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE.
Perangkat Daerah adalah Perangkat Daerah yang membidangi urusan persandian.
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, yang mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
8. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas informasi elektronik.
9. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas informasi elektronik.
10. Manajemen Keamanan Informasi SPBE adalah serangkaian proses untuk mencapai penerapan keamanan informasi yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
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 integrasi/penghubung, dan perangkat elektronik lainnya.

BAB II

MAKSUD

Pasal 2

Peraturan Bupati ini dimaksudkan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi.

BAB III

RUANG LINGKUP

Pasal 3

Manajemen Keamanan Informasi SPBE meliputi:

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

BAB IV

PENETAPAN RUANG LINGKUP

Pasal 4

- (1) Ruang lingkup Manajemen Keamanan Informasi SPBE terdiri atas:
 - a. data dan informasi SPBE;
 - b. Aplikasi SPBE;
 - c. Infrastruktur SPBE; dan
 - d. kebijakan keamanan informasi SPBE yang telah dimiliki.
- (2) Ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Daerah.

BAB V

PENETAPAN PENANGGUNGJAWAB

Pasal 5

- (1) Bupati menetapkan Sekretaris Daerah sebagai penanggung jawab Keamanan Informasi SPBE.
- (2) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan Informasi SPBE, Sekretaris Daerah disebut sebagai koordinator SPBE.

Pasal 6

- (1) Koordinator SPBE sebagaimana dimaksud dalam Pasal 5 ayat (2) menetapkan pelaksana teknis Keamanan Informasi SPBE.
- (2) Pelaksana teknis Keamanan Informasi 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 Kepala Perangkat Daerah yang membidangi urusan persandian.
- (4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b yaitu seluruh Kepala Perangkat Daerah lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE.

Pasal 7

- (1) Ketua Tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan Manajemen Keamanan Informasi SPBE yang meliputi:
 - a. memastikan penerapan standar teknis dan prosedur Keamanan Informasi SPBE;
 - b. mengevaluasi penerapan standar teknis dan prosedur Keamanan Informasi SPBE di lingkungan Pemerintah Kabupaten Rembang;

- c. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Informasi SPBE;
 - d. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans*; dan
 - e. melaporkan pelaksanaan Manajemen Keamanan Informasi SPBE pada koordinator SPBE.
- (2) Anggota Tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf b mempunyai tugas:
- a. menerapkan standar teknis dan prosedur pengendalian Keamanan Informasi SPBE pada Perangkat Daerah masing-masing;
 - b. memastikan penerapan keamanan aplikasi dan infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan Informasi SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan;
 - c. membantu Ketua Tim merancang dan merumuskan langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans* sesuai sistem elektronik yang dikelola pada Perangkat Daerah masing-masing;
 - d. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
 - e. berkoordinasi dengan Ketua Tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

BAB VI

PERENCANAAN

Pasal 8

- (1) Perencanaan sebagaimana dimaksud dalam Pasal 3 huruf c ditetapkan oleh ketua tim.
- (2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
 - a. program kerja Keamanan Informasi SPBE yang disusun berdasarkan kategori risiko Keamanan Informasi SPBE; dan
 - b. target realisasi program kerja Keamanan Informasi SPBE.
- (3) Daftar kategori risiko sebagaimana dimaksud pada ayat (2) huruf a mengacu pada dokumen manajemen risiko yang disusun oleh Perangkat Daerah.
- (4) Dokumen manajemen risiko sebagaimana dimaksud pada ayat (3) disusun berdasarkan peraturan perundang-undangan.

Pasal 9

- (1) Program kerja Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf a meliputi:
 - a. edukasi kesadaran keamanan Informasi SPBE;
 - b. penilaian kerentanan Keamanan Informasi SPBE;
 - c. peningkatan Keamanan Informasi SPBE;
 - d. penanganan insiden Keamanan Informasi SPBE; dan

- e. audit keamanan SPBE.
- (2) Target realisasi program kerja Keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 10

Edukasi kesadaran Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf a dilaksanakan melalui kegiatan:

- a. sosialisasi; dan
- b. pelatihan.

Pasal 11

Penilaian kerentanan Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf b dilaksanakan melalui:

- a. menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur;
- b. mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
- c. mengukur tingkat risiko Keamanan Informasi SPBE.

Pasal 12

- (1) Peningkatan Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 11.
- (2) Peningkatan Keamanan Informasi SPBE dilaksanakan melalui:
- a. menerapkan standar teknis dan prosedur pengendalian Keamanan Informasi SPBE; dan
 - b. menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 13

Penanganan insiden Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf d dilaksanakan melalui:

- a. mengidentifikasi sumber serangan;
- b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
- c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
- d. mendokumentasi bukti insiden yang terjadi; dan
- e. memitigasi atau mengurangi dampak risiko Keamanan Informasi SPBE.

Pasal 14

Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (1) huruf e harus dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan mencakup:

- a. audit keamanan Infrastruktur SPBE; dan
- b. audit keamanan aplikasi khusus.

BAB VII
DUKUNGAN PENGOPERASIAN

Pasal 15

- (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 Informasi SPBE; dan
 - b. anggaran Keamanan Informasi SPBE.

Pasal 16

- (1) Sumber daya manusia Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 15 ayat (2) huruf a paling sedikit harus memiliki kompetensi:
 - a. keamanan infrastruktur TIK; dan
 - b. keamanan aplikasi.
- (2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), melakukan kegiatan:
 - a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur TIK dan keamanan aplikasi; dan
 - b. bimbingan teknis mengenai standar Keamanan Informasi SPBE.
- (3) Anggaran Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 15 ayat (2) huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VIII
EVALUASI KINERJA

Pasal 17

- (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.
- (3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
 - a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan Informasi SPBE;
 - b. menetapkan indikator kinerja pada setiap area proses;
 - c. memformulasi pelaksanaan Keamanan Informasi SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
 - d. menganalisis efektifitas pelaksanaan Keamanan Informasi SPBE; dan
 - e. mendukung dan merealisasikan program audit Keamanan Informasi SPBE.
- (4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

BAB IX
PERBAIKAN BERKELANJUTAN

Pasal 18

- (1) Perbaikan berkelanjutan terhadap Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 3 huruf f dilakukan oleh pelaksana teknis Keamanan Informasi SPBE.
- (2) Perbaikan berkelanjutan terhadap Manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.
- (3) Perbaikan berkelanjutan terhadap Manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) dilakukan dengan:
 - a. mengatasi permasalahan dalam pelaksanaan Keamanan Informasi SPBE; dan
 - b. memperbaiki pelaksanaan Manajemen Keamanan Informasi SPBE secara periodik.

BAB X
PENGENDALIAN TEKNIS KEAMANAN

Pasal 19

- (1) Penetapan prosedur pengendalian Keamanan Informasi SPBE digunakan untuk mengimplementasikan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Kabupaten Rembang dengan cakupan aspek meliputi:
 - a. manajemen risiko;
 - b. kelangsungan bisnis atau layanan TIK (*business continuity*);
 - c. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);
 - d. audit internal Keamanan Informasi SPBE;
 - e. pengendalian Keamanan Informasi SPBE terhadap pihak ketiga;
 - f. pengelolaan aset;
 - g. perlindungan data pribadi;
 - h. keamanan perangkat teknologi informasi komunikasi;
 - i. keamanan jaringan;
 - j. keamanan pusat data;
 - k. keamanan perangkat *end point*;
 - l. keamanan penyimpanan elektronik;
 - m. keamanan fisik dan lingkungan;
 - n. keamanan *remote working*;
 - o. pengelolaan akses kontrol;
 - p. persyaratan keamanan pembangunan dan pengembangan Aplikasi SPBE;
 - q. keamanan migrasi data;
 - r. konfigurasi perangkat *IT Security*;
 - s. keamanan komunikasi;
 - t. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
 - u. penerapan kriptografi;

- v. penanganan insiden Keamanan Informasi SPBE; dan/atau
 - w. aspek prosedur pengendalian Keamanan Informasi SPBE lainnya.
- (2) Prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) selanjutnya ditetapkan Koordinator SPBE.

Pasal 20

- (1) Perangkat Daerah memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi prosedur pengendalian Keamanan Informasi SPBE yang telah ditetapkan.
- (2) Perangkat Daerah harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
- (3) Perangkat Daerah harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek Keamanan Informasi dalam hubungan kerja sama dengan pihak ketiga.
- (4) Perangkat Daerah harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB XI

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 Rembang.

Ditetapkan di Rembang
pada tanggal 15 Agustus 2024

BUPATI REMBANG,

ttd

ABDUL HAFIDZ

Diundangkan di Rembang
pada tanggal 15 Agustus 2024

SEKRETARIS DAERAH
KABUPATEN REMBANG,

ttd

FAHRUDIN

BERITA DAERAH KABUPATEN REMBANG TAHUN 2024 NOMOR 31

Salinan sesuai dengan aslinya
Kepala Bagian Hukum
Setda Kabupaten Rembang



DEDHY NUGRAHA, S.H., M.Si
Pembina
NIP. 19791206 200604 1 006