

RANCANGAN
PERATURAN BUPATI MUARA ENIM
NOMOR ____ TAHUN 2026

TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH KABUPATEN MUARA ENIM

DENGAN RAHMAT TUHAN YANG MAHA ESA
BUPATI MUARA ENIM,

- Menimbang :
- a. bahwa perkembangan teknologi informasi dan komunikasi dalam penyelenggaraan pemerintahan daerah memerlukan pengelolaan keamanan informasi yang efektif, terstruktur, dan berkelanjutan;
 - b. bahwa penyelenggaraan sistem elektronik di lingkungan Pemerintah Kabupaten Muara Enim perlu dilindungi dari ancaman keamanan informasi, gangguan siber, kehilangan data, dan penyalahgunaan akses informasi;
 - c. bahwa untuk meningkatkan tata kelola keamanan informasi sesuai prinsip Sistem Pemerintahan Berbasis Elektronik dan penerapan Indeks Keamanan Informasi, perlu membentuk Sistem Manajemen Keamanan Informasi;
 - d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c perlu menetapkan Peraturan Bupati tentang Sistem Manajemen Keamanan Informasi di Lingkungan Pemerintah Kabupaten Muara Enim.

- Mengingat :
- 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
 - 2. Undang-Undang Nomor 91 Tahun 2024 tentang Kabupaten Muara Enim di Provinsi Sumatera Selatan

- (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 277, Tambahan Lembaran Negara Republik Indonesia Nomor 7028);
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 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 11, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);
 5. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah diubah dengan Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 143, Tambahan Lembaran Negara Republik Indonesia Nomor 6801);
 6. 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 1 Tahun 2026 tentang

- Penyesuaian Pidana (Lembaran Negara Republik Indonesia Tahun 2026 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 7153);
7. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 233, Tambahan Lembaran Negara Republik Indonesia Nomor 6820);
 8. 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);
 9. Peraturan Pemerintah Nomor 33 Tahun 2026 tentang Peraturan Pelaksanaan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2026 Nomor 88, Tambahan Lembaran Negara Republik Indonesia Nomor 7190);
 10. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
 11. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
 12. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 157);
 13. 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);

14. 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);
15. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 48 Tahun 2022 tentang Jabatan Fungsional Auditor;
16. 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);
17. 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);
18. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
19. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2024 tentang Standar Dan Tata Cara Pelaksanaan Audit Keamanan Sistem Pemerintahan Berbasis Elektronik;
20. Peraturan Bupati Nomor 18 Tahun 2023 tentang susunan, kedudukan, tugas, fungsi dan struktur organisasi Dinas Komunikasi, Informatika, Statistik dan Persandian;
21. Peraturan Bupati Nomor 5 Tahun 2022 tentang susunan, kedudukan, tugas, fungsi dan struktur organisasi Inspektorat;

22. Peraturan Bupati Nomor 52 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik;

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KABUPATEN MUARA ENIM.

BAB I

KETENTUAN UMUM

Bagian Kesatu

Pengertian, Definisi, dan Singkatan

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Kabupaten adalah Kabupaten Muara Enim.
2. Pemerintah Kabupaten adalah Pemerintah Kabupaten Muara Enim.
3. Bupati adalah Bupati Muara Enim.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Muara Enim.
5. Perangkat Daerah adalah Perangkat Daerah dilingkungan Pemerintah Kabupaten Muara Enim.
6. Dinas Komunikasi, Informatika, Statistik dan Persandian yang selanjutnya disebut Diskominfo SP merupakan unsur pelaksana urusan pemerintahan bidang komunikasi dan informatika, statistik, dan persandian yang menjadi kewenangan Kabupaten.
7. Inspektorat merupakan unsur pengawasan penyelenggaraan pemerintahan daerah.
8. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.

9. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
10. Keamanan Informasi adalah suatu kondisi untuk melindungi aset informasi dari berbagai ancaman internal maupun eksternal guna menjamin kerahasiaan, keutuhan, dan ketersediaan informasi.
11. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah serangkaian proses untuk mencapai penerapan keamanan informasi SPBE yang efektif, efisien, dan berkelanjutan.
12. Insiden Keamanan Informasi adalah kejadian yang tidak diinginkan dan tidak diperkirakan yang menimbulkan gangguan terhadap operasional dan mengancam keamanan informasi.
13. Risiko adalah segala kejadian dalam setiap aktivitas yang mungkin timbul karena faktor ketidakpastian, yang mengandung potensi untuk menghambat pencapaian sasaran kinerja dari Sistem Elektronik.
14. Manajemen Risiko adalah aktivitas terkoordinasi untuk identifikasi, penilaian, dan penentuan prioritas risiko yang kemudian dikelola, dipantau, dan dikontrol untuk mengurangi dampak dan/atau kemungkinan terjadinya risiko.
15. Aset Informasi adalah data, perangkat, aplikasi, jaringan, sumber daya manusia, dan fasilitas yang memiliki nilai bagi Pemerintah Daerah.
16. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas dan fungsi layanan SPBE.
17. 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.

18. Data Pribadi adalah data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi secara tersendiri atau dikombinasi dengan informasi lainnya baik secara langsung maupun tidak langsung melalui sistem elektronik atau nonelektronik.
19. Indeks Keamanan Informasi atau Indeks KAMI adalah alat evaluasi tingkat kematangan keamanan informasi yang digunakan pada instansi pemerintah.
20. IKASANDI adalah instrumen evaluasi untuk mengukur kesiapan instansi pemerintah dalam bidang keamanan siber dan persandian.
21. Audit Keamanan SPBE yang selanjutnya disebut Audit adalah audit teknologi informasi dan komunikasi dengan cakupan keamanan SPBE.
22. Auditor adalah aparatur sipil negara yang diberi tugas, tanggung jawab, dan wewenang untuk melakukan pengawasan intern.
23. Pemilik Sistem Elektronik adalah Perangkat Daerah di lingkungan Pemerintah Daerah yang memiliki, mengelola, dan/atau bertanggung jawab atas penyelenggaraan suatu Sistem Elektronik.
24. Koordinator SPBE adalah pejabat yang ditetapkan Bupati untuk bertanggung jawab atas pelaksanaan manajemen keamanan informasi SPBE.
25. Pengguna Sistem adalah pegawai atau pihak lain yang diberikan hak akses terhadap sistem elektronik.
26. SNI ISO/IEC 27001 adalah Standar Nasional Indonesia hasil adopsi standar internasional mengenai persyaratan sistem manajemen keamanan informasi, yang diterbitkan oleh Badan Standardisasi Nasional.
27. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan,

menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.

Bagian Kedua

Maksud dan Tujuan

Pasal 2

- (1) Peraturan Bupati ini dimaksudkan sebagai pedoman pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Kabupaten.
- (2) Peraturan Bupati ini bertujuan untuk:
 - a. melindungi Aset Informasi Pemerintah Daerah dari berbagai ancaman keamanan informasi;
 - b. menjaga kerahasiaan, keutuhan, dan ketersediaan informasi;
 - c. mengurangi risiko keamanan informasi dan gangguan siber;
 - d. mendukung penerapan SPBE yang aman dan andal; dan
 - e. meningkatkan tingkat kematangan keamanan informasi berdasarkan Indeks KAMI dan/atau IKASANDI.

BAB II

SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 3

SMKI sebagaimana dimaksud dalam Pasal 2 ayat (1) meliputi:

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

Bagian Kesatu

Ruang Lingkup

Pasal 4

- (1) Ruang lingkup sebagaimana dimaksud dalam Pasal 3 huruf a meliputi:
 - 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 Informasi Pemerintah Kabupaten yang harus diamankan dalam SPBE.
- (3) SMKI sebagaimana diatur dalam Peraturan Bupati ini berlaku untuk seluruh Perangkat Daerah di lingkungan Pemerintah Kabupaten.

Bagian Kedua

Penanggung Jawab

Pasal 5

- (1) Bupati menetapkan penanggung jawab Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 3 huruf b dengan Keputusan Bupati.
- (2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
- (3) Dalam melaksanakan tugas sebagai penanggung jawab Manajemen Keamanan Informasi SPBE, Sekretaris Daerah bertindak selaku Koordinator SPBE.

Pasal 6

- (1) Koordinator SPBE menetapkan pelaksana teknis manajemen keamanan informasi SPBE.
- (2) Pelaksana teknis sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. Tim Manajemen Keamanan Informasi SPBE; dan
 - b. Tim Tanggap Insiden Siber.

- (3) Tim Manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) huruf a terdiri atas:
 - a. ketua tim; dan
 - b. anggota tim.
- (4) Ketua tim sebagaimana dimaksud pada ayat (3) huruf a dijabat oleh Kepala Diskominfo SP.
- (5) Anggota tim sebagaimana dimaksud pada ayat (3) huruf b terdiri atas kepala Perangkat Daerah atau pejabat administrator yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Kabupaten.
- (6) Tim sebagaimana dimaksud pada ayat (2) ditetapkan dengan Keputusan Bupati.

Pasal 7

- (1) Ketua tim sebagaimana dimaksud dalam Pasal 6 ayat (4) mempunyai tugas:
 - a. memastikan penerapan standar teknis dan prosedur keamanan informasi SPBE;
 - b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran keamanan informasi SPBE; dan
 - c. melaporkan pelaksanaan Manajemen Keamanan Informasi SPBE kepada Koordinator SPBE.
- (2) Anggota tim sebagaimana dimaksud dalam Pasal 6 ayat (5) mempunyai tugas:
 - a. menerapkan standar teknis dan prosedur keamanan informasi pada unit kerja masing-masing;
 - b. memastikan pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE yang dilakukan pihak ketiga memenuhi standar teknis dan prosedur keamanan SPBE yang ditetapkan;

- c. memastikan keberlangsungan proses bisnis SPBE pada unit kerja masing-masing; dan
- d. berkoordinasi dengan ketua tim terkait perumusan program kerja dan anggaran keamanan informasi SPBE.

Pasal 8

- (1) Tim Tanggap Insiden Siber sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf b mempunyai tugas melakukan identifikasi, analisis, penanganan, dan pemulihan atas Insiden Keamanan Informasi.
- (2) Susunan keanggotaan Tim Tanggap Insiden Siber terdiri atas unsur Diskominfo SP dan Perangkat Daerah pemilik Sistem Elektronik terkait.
- (3) Dalam hal terjadi Insiden Keamanan Informasi yang berdampak besar, Tim Tanggap Insiden Siber dapat berkoordinasi dengan Badan Siber dan Sandi Negara dan instansi terkait.

Bagian Ketiga

Perencanaan

Pasal 9

- (1) Perencanaan sebagaimana dimaksud dalam Pasal 3 huruf c disusun oleh anggota tim dan 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.

Pasal 10

- (1) Program kerja keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf a paling sedikit meliputi:
 - a. edukasi kesadaran keamanan informasi SPBE;
 - b. penilaian kerentanan keamanan Aplikasi dan Infrastruktur SPBE;
 - c. peningkatan keamanan informasi SPBE;
 - d. penanganan Insiden Keamanan Informasi SPBE; dan
 - e. Audit Keamanan Informasi SPBE.
- (2) Target realisasi program kerja sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Bagian Keempat

Dukungan Pengoperasian

Pasal 11

- (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;
 - b. teknologi keamanan informasi SPBE;
 - c. anggaran keamanan informasi SPBE; dan
 - d. pengelolaan pihak ketiga.
- (3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan Manajemen Keamanan Informasi SPBE diberikan alokasi sumber daya yang memadai.

Pasal 12

- (1) Sumber daya manusia keamanan informasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a ditempatkan pada Diskominfo SP dan memiliki kompetensi:
 - a. keamanan Infrastruktur SPBE; dan
 - b. keamanan Aplikasi SPBE.
- (2) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (1) dilakukan melalui pelatihan dan/atau sertifikasi kompetensi, serta bimbingan teknis mengenai standar keamanan informasi SPBE.
- (3) Teknologi keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b disediakan sesuai kebutuhan dan tingkat urgensi setiap Perangkat Daerah.
- (4) Anggaran keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai ketentuan peraturan perundang-undangan.

Pasal 13

- (1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf d dilakukan oleh setiap Pemilik Sistem Elektronik.
- (2) Pemilik Sistem Elektronik 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) Pemilik Sistem Elektronik harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
- (4) Pemilik Sistem Elektronik harus menetapkan proses, prosedur, atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi

SPBE dalam hubungan kerja sama dengan pihak ketiga.

- (5) Pemilik Sistem Elektronik harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

Bagian Kelima

Evaluasi Kinerja

Pasal 14

- (1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 huruf e dilakukan oleh Koordinator SPBE terhadap pelaksanaan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah.
- (2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) 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 efektivitas pelaksanaan keamanan informasi SPBE; dan/atau
 - e. mendukung dan merealisasikan program Audit keamanan informasi SPBE.
- (3) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Bagian Keenam
Perbaikan Berkelanjutan

Pasal 15

- (1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 3 huruf f dilakukan oleh anggota tim Manajemen Keamanan Informasi 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 Manajemen Keamanan Informasi SPBE; dan/atau
 - b. memperbaiki pelaksanaan Manajemen Keamanan Informasi SPBE secara periodik.

Pasal 16

Petunjuk teknis mengenai pedoman pelaksanaan SMKI sebagaimana dimaksud dalam Pasal 3 ditetapkan dengan Keputusan Bupati.

BAB III

PENGENDALIAN TEKNIS KEAMANAN INFORMASI

Pasal 17

- (1) Pemilik Sistem Elektronik wajib menerapkan pengendalian teknis keamanan informasi terhadap seluruh Aset Informasi.
- (2) Pengendalian teknis sebagaimana dimaksud pada ayat (1) mencakup aspek:
 - a. keamanan perangkat teknologi informasi dan komunikasi;
 - b. keamanan jaringan;
 - c. keamanan pusat data;
 - d. keamanan perangkat pengguna akhir (*end point*);
 - e. keamanan kerja jarak jauh (*remote working*);
 - f. keamanan penyimpanan elektronik;

- g. pengelolaan akses kontrol;
 - h. pengelolaan akun dan kata sandi;
 - i. pengendalian keamanan dari ancaman virus dan malware;
 - j. persyaratan keamanan terkait pembangunan dan pengembangan Aplikasi SPBE;
 - k. pengelolaan aset;
 - l. keamanan migrasi data;
 - m. konfigurasi perangkat keamanan teknologi informasi;
 - n. pelindungan Data Pribadi;
 - o. keamanan komunikasi;
 - p. keamanan dalam proses akuisisi, pengembangan, dan pemeliharaan sistem informasi;
 - q. pengendalian keamanan informasi terhadap pihak ketiga;
 - r. penerapan kriptografi;
 - s. penanganan Insiden Keamanan Informasi;
 - t. kelangsungan proses bisnis atau layanan TIK (*business continuity*);
 - u. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*);
 - v. Audit internal keamanan SPBE; dan/atau
 - w. aspek prosedur pengendalian keamanan informasi SPBE lainnya.
- (3) Ketentuan lebih lanjut mengenai standar dan prosedur teknis pengendalian keamanan informasi sebagaimana dimaksud pada ayat (2) ditetapkan dengan Keputusan Bupati.

Pasal 18

- (1) Setiap Pengguna Sistem wajib menjaga kerahasiaan akun dan kata sandi.
- (2) Kata sandi sebagaimana dimaksud pada ayat (1) paling sedikit memenuhi standar kompleksitas dan periode

penggantian sebagaimana ditetapkan dalam Keputusan Bupati sebagaimana dimaksud dalam Pasal 17 ayat (3).

BAB IV

MANAJEMEN RISIKO KEAMANAN INFORMASI

Bagian Kesatu

Kategorisasi Sistem Elektronik

Pasal 19

- (1) Sistem Elektronik di lingkungan Pemerintah Daerah dikategorikan berdasarkan asas Risiko, terdiri atas:
 - a. Sistem Elektronik strategis;
 - b. Sistem Elektronik tinggi; dan
 - c. Sistem Elektronik rendah.
- (2) Sistem Elektronik strategis sebagaimana dimaksud pada ayat (1) huruf a merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara.
- (3) Sistem Elektronik tinggi sebagaimana dimaksud pada ayat (1) huruf b merupakan Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau Daerah.
- (4) Sistem Elektronik rendah sebagaimana dimaksud pada ayat (1) huruf c merupakan Sistem Elektronik selain sebagaimana dimaksud pada ayat (2) dan ayat (3).
- (5) Kategorisasi Sistem Elektronik sebagaimana dimaksud pada ayat (1) ditentukan melalui Penilaian Mandiri oleh Pemilik Sistem Elektronik dan dilaporkan kepada Badan Siber dan Sandi Negara untuk diverifikasi dan ditetapkan, sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 20

- (1) Pemilik Sistem Elektronik yang menyelenggarakan Sistem Elektronik strategis wajib menerapkan:
 - a. SNI ISO/IEC 27001;

- b. standar keamanan siber lain yang ditetapkan oleh Badan Siber dan Sandi Negara; dan
 - c. standar keamanan siber lain yang ditetapkan oleh Kementerian/Lembaga sektor terkait.
- (2) Pemilik Sistem Elektronik yang menyelenggarakan Sistem Elektronik tinggi wajib menerapkan:
- a. SNI ISO/IEC 27001 dan/atau standar keamanan siber lain yang ditetapkan oleh Badan Siber dan Sandi Negara; dan
 - b. standar keamanan siber lain yang ditetapkan oleh Kementerian/Lembaga sektor terkait.
- (3) Pemilik Sistem Elektronik yang menyelenggarakan Sistem Elektronik rendah wajib menerapkan SNI ISO/IEC 27001 atau standar keamanan siber lain yang ditetapkan oleh Badan Siber dan Sandi Negara.
- (4) Dalam hal standar keamanan siber sebagaimana dimaksud pada ayat (1) huruf c dan ayat (2) huruf b belum ditetapkan oleh Kementerian/Lembaga sektor terkait, Pemilik Sistem Elektronik wajib melaksanakan ketentuan sebagaimana dimaksud pada ayat (1) huruf a dan huruf b, atau ayat (2) huruf a.
- (5) Ketentuan lebih lanjut mengenai kategorisasi dan standar keamanan Sistem Elektronik sebagaimana dimaksud pada ayat (1), ayat (2), dan ayat (3) mengacu pada ketentuan peraturan perundang-undangan mengenai sistem pengamanan dalam penyelenggaraan sistem elektronik.

Bagian Kedua

Pelaksanaan Manajemen Risiko

Pasal 21

- (1) Diskominfo SP dan setiap Pemilik Sistem Elektronik wajib melaksanakan Manajemen Risiko keamanan informasi.

- (2) Manajemen Risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar Risiko (*risk register*) melalui:
- a. inventarisasi Aset Informasi elektronik dan nonelektronik;
 - b. identifikasi ancaman dan kerentanan terhadap Aset Informasi;
 - c. penilaian Risiko keamanan terhadap Aset Informasi;
 - d. penentuan prioritas Risiko;
 - e. analisis dampak jika terjadi Risiko;
 - f. analisis kontrol keamanan yang dapat diterapkan; dan/atau
 - g. rekomendasi kontrol keamanan.
- (3) Prosedur pelaksanaan Manajemen Risiko mengacu sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 22

- (1) Diskominfo SP wajib menyusun Profil Risiko Keamanan Informasi sebagai dokumen yang memuat hasil identifikasi, analisis, dan penetapan tingkat Risiko sebagaimana dimaksud dalam Pasal 21.
- (2) Profil Risiko sebagaimana dimaksud pada ayat (1) paling sedikit memuat:
- a. daftar Risiko keamanan informasi;
 - b. sumber dan penyebab Risiko;
 - c. tingkat kemungkinan dan dampak Risiko;
 - d. peringkat atau level Risiko;
 - e. rencana dan status tindakan mitigasi; dan
 - f. pihak yang bertanggung jawab atas mitigasi Risiko.
- (3) Profil Risiko sebagaimana dimaksud pada ayat (1) dimutakhirkan paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau sewaktu-waktu apabila terjadi perubahan signifikan terhadap Aset Informasi, ancaman, atau kerentanan.

- (4) Profil Risiko sebagaimana dimaksud pada ayat (1) disusun oleh Tim Manajemen Keamanan Informasi SPBE dan dilaporkan kepada Koordinator SPBE.

BAB V

PENANGANAN INSIDEN KEAMANAN INFORMASI

Pasal 23

- (1) Setiap Insiden Keamanan Informasi wajib dilaporkan kepada Tim Tanggap Insiden Siber sebagaimana dimaksud dalam Pasal 8.
- (2) Penanganan Insiden sebagaimana dimaksud pada ayat (1) dilakukan melalui:
 - a. identifikasi Insiden;
 - b. pelaporan Insiden;
 - c. analisis dan investigasi;
 - d. tindakan pemulihan; dan
 - e. dokumentasi dan evaluasi.

BAB VI

PENCADANGAN DAN PEMULIHAN DATA

Pasal 24

- (1) Pemilik Sistem Elektronik wajib melaksanakan pencadangan data secara berkala.
- (2) Pencadangan data sebagaimana dimaksud pada ayat (1) meliputi data aplikasi, basis data, konfigurasi server, dan log sistem.
- (3) Pemilik Sistem Elektronik wajib memiliki dan menguji secara berkala prosedur pemulihan data dan pemulihan layanan (*disaster recovery plan*).

BAB VII

KLASIFIKASI INFORMASI

Pasal 25

- (1) Informasi di lingkungan Daerah diklasifikasikan berdasarkan tingkat kerahasiaannya, yang terdiri atas

informasi publik, informasi internal, informasi rahasia, dan informasi sangat rahasia.

- (2) Pengelolaan dan distribusi informasi wajib disesuaikan dengan klasifikasi informasi sebagaimana dimaksud pada ayat (1).

BAB VIII

PELINDUNGAN DATA PRIBADI

Pasal 26

- (1) Pemilik Sistem Elektronik wajib melindungi Data Pribadi yang diperoleh, dikumpulkan, diolah, dianalisis, disimpan, ditampilkan, dipublikasikan, dan/atau disebarluaskan dalam penyelenggaraan Sistem Elektronik pemerintahan.
- (2) Pelindungan Data Pribadi sebagaimana dimaksud pada ayat (1) dilakukan melalui:
 - a. penerapan prinsip pengumpulan Data Pribadi secara terbatas dan sesuai tujuan;
 - b. pembatasan akses terhadap Data Pribadi hanya kepada pihak yang berwenang;
 - c. enkripsi dan/atau pseudonimisasi terhadap Data Pribadi yang bersifat sensitif;
 - d. pencatatan aktivitas pemrosesan Data Pribadi; dan
 - e. penghapusan atau pemusnahan Data Pribadi yang telah melampaui jangka waktu penyimpanan atau tidak lagi diperlukan.

Pasal 27

- (1) Dalam hal terjadi kegagalan pelindungan Data Pribadi, Pemilik Sistem Elektronik bersama Diskominfo SP wajib:
 - a. menghentikan kebocoran dan/atau penyalahgunaan Data Pribadi;
 - b. melakukan mitigasi dan pemulihan;
 - c. memberitahukan kepada pemilik Data Pribadi dan instansi yang berwenang paling lambat 3 x 24 (tiga

kali dua puluh empat) jam sejak diketahuinya kegagalan perlindungan Data Pribadi; dan

d. mendokumentasikan kejadian dan langkah penanganan.

(2) Ketentuan lebih lanjut mengenai perlindungan Data Pribadi berpedoman pada peraturan perundang-undangan mengenai perlindungan data pribadi.

BAB IX

AUDIT KEAMANAN INFORMASI

Pasal 28

(1) Pemerintah Kabupaten wajib melaksanakan Audit Keamanan Informasi secara berkala.

(2) Audit sebagaimana dimaksud pada ayat (1) dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun melalui audit internal dan/atau audit eksternal.

(3) Pelaksana Audit sebagaimana dimaksud pada ayat (2) dilaksanakan oleh:

a. audit internal, merupakan Auditor dari Inspektorat bersama Diskominfo SP; dan

b. audit eksternal, merupakan lembaga milik pemerintah dan/atau lembaga swasta yang memiliki sertifikasi khusus untuk melaksanakan penilaian terhadap kepatuhan standar Manajemen Keamanan Informasi.

Pasal 29

Hasil Audit digunakan sebagai dasar:

a. evaluasi penerapan SMKI;

b. peningkatan keamanan informasi;

c. penyusunan rencana tindak lanjut; dan

d. peningkatan nilai Indeks KAMI dan/atau IKASANDI.

BAB X SANKSI ADMINISTRATIF

Pasal 30

- (1) Pegawai atau Pengguna Sistem yang melanggar ketentuan keamanan informasi sebagaimana diatur dalam Peraturan Bupati ini dapat dikenakan sanksi administratif.
- (2) Sanksi administratif sebagaimana dimaksud pada ayat (1) dapat berupa:
- a. teguran lisan;
 - b. teguran tertulis;
 - c. pembatasan hak akses;
 - d. penonaktifan akun; dan/atau
 - e. sanksi lain sesuai ketentuan peraturan perundang-undangan.

BAB XI PEMBIAYAAN

Pasal 31

Pembiayaan pelaksanaan Manajemen Keamanan Informasi SPBE bersumber dari:

- a. Anggaran Pendapatan dan Belanja Daerah; dan/atau
- b. sumber pendanaan lain yang sah sesuai ketentuan peraturan perundang-undangan.

BAB XII KETENTUAN PENUTUP

Pasal 32

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Muara Enim
pada tanggal _____ 2026
BUPATI MUARA ENIM,

(_____)

Diundangkan di Muara Enim
pada tanggal _____ 2026

SEKRETARIS DAERAH
KABUPATEN MUARA ENIM,

(_____)

BERITA DAERAH KABUPATEN MUARA ENIM TAHUN 2026 NOMOR ____