



SALINAN

BUPATI MADIUN
PROVINSI JAWA TIMUR
PERATURAN BUPATI MADIUN
NOMOR 16 TAHUN 2024
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
PEMERINTAH KABUPATEN MADIUN
DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MADIUN,

- Menimbang :
- a. bahwa guna melindungi aset data/informasi Pemerintah Kabupaten Madiun yang bersifat digital dari kemungkinan penggunaan, penyebaran, perusakan, dan perubahan oleh pihak yang tidak berwenang diperlukan pembakuan tata kerja pelaksanaan operasional pengelolaan keamanan informasi agar dapat terlaksana secara sistematis dan konsisten sesuai dengan ketentuan yang telah ditetapkan di lingkungan Pemerintah Kabupaten Madiun;
 - b. bahwa keamanan informasi sebagaimana dimaksud huruf a dilaksanakan untuk menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan akuntabilitas (*accountability*) data/informasi institusi, khususnya yang dikelola dengan menggunakan teknologi informasi komunikasi (TIK);
 - c. bahwa untuk mengoptimalkan pengelolaan risiko penggunaan TIK, dengan mencegah dan mengurangi dampak insiden keamanan siber dan/atau keamanan informasi sehingga memelihara dan meningkatkan reputasi institusi;
 - d. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a huruf b, dan huruf c perlu ditetapkan Peraturan Bupati Madiun tentang Sistem Manajemen Keamanan Informasi Pemerintah Kabupaten Madiun.

- Mengingat : 1. Undang-Undang Nomor 12 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Djawa Timur (Lembaran Negara Republik Indonesia Tahun 1950 Nomor 19, Tambahan Lembaran Negara Republik Indonesia Nomor 9) sebagaimana telah diubah dengan Undang-Undang Nomor 2 Tahun 1965 tentang Perubahan Batas Wilayah Kota Praja Surabaya dan Daerah Tingkat II Surabaya dengan mengubah Undang-Undang Nomor 12 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten Dalam Lingkungan Propinsi Djawa Timur dan Undang-Undang Nomor 16 Tahun 1950 tentang Pembentukan Daerah-Daerah Kota Besar Dalam Lingkungan Propinsi Djawa Timur, Djawa Tengah, Djawa Barat dan Dalam Daerah Istimewa Jogjakarta (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 19, Tambahan Negara Republik Indonesia Nomor 2730);
2. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Tahun 2008 Nomor 61 Tambahan Lembaran Negara Nomor 4846);
3. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Tahun 2009 Nomor 112 Tambahan Lembaran Negara Nomor 5038);
4. 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);
5. 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 9 Tahun 2015 tentang Perubahan Kedua Atas

Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);

6. Peraturan Pemerintah Nomor 12 Tahun 2017 tentang Pembinaan dan Pengawasan Penyelenggaraan Pemerintahan Daerah (Lembaran Negara Tahun 2017 Nomor 73, Tambahan Lembaran Negara Nomor 6041); Peraturan Pemerintah Nomor 2 Tahun 2018 Tentang Standar Pelayanan Minimal (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 2, Tambahan Lembaran Negara Republik Indonesia Nomor 6178);
7. Peraturan Pemerintah Nomor 12 Tahun 2017 tentang Pembinaan dan Pengawasan Penyelenggaraan Pemerintahan Daerah (Lembaran Negara Tahun 2017 Nomor 73, Tambahan Lembaran Negara Nomor 6041); Peraturan Pemerintah Nomor 2 Tahun 2018 Tentang Standar Pelayanan Minimal (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 2, Tambahan Lembaran Negara Republik Indonesia Nomor 6178);
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 96 Tahun 2012 tentang Pelaksana Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Tahun 2012 Nomor 215, Tambahan Lembaran Negara Nomor 5357);

10. Peraturan Presiden Nomor 87 Tahun 2014 tentang Peraturan Pelaksanaan Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan sebagaimana telah diubah dengan Peraturan Presiden Nomor 76 Tahun 2021 tentang Perubahan Atas Peraturan Presiden Nomor 87 Tahun 2014 tentang Peraturan Pelaksanaan Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan;
11. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
12. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital;
13. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah 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;
14. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik;
15. Peraturan Menteri Dalam Negeri Nomor 5 Tahun 2017 tentang Pedoman Nomenklatur Perangkat Daerah Provinsi dan Daerah Kabupaten/Kota yang Melaksanakan Fungsi Penunjang Penyelenggaraan Urusan Pemerintahan;
16. Peraturan Menteri Dalam Negeri Nomor 70 Tahun 2019 tentang Sistem Informasi Pemerintahan Daerah;
17. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik;
18. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;

19. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik;
20. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE;
21. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
22. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
23. Peraturan Daerah Nomor 6 Tahun 2016 tentang susunan perangkat daerah sebagaimana telah diubah beberapa kali terakhir dengan Peraturan Daerah Nomor 13 Tahun 2019 tentang Perubahan Kedua Atas Peraturan Daerah Nomor 6 Tahun 2016 Tentang Susunan Perangkat Daerah;
24. Peraturan Bupati Madiun Nomor 85 Tahun 2018 tentang Pedoman Pengelolaan Pelayanan Informasi dan Dokumentasi di Lingkungan Pemerintah Kabupaten Madiun;
25. Peraturan Bupati Madiun Nomor 24 Tahun 2020 tentang Satu Data Indonesia Tingkat Kabupaten Madiun;
26. Peraturan Bupati Madiun Nomor 46 Tahun 2020 Tentang Pelaksanaan Persandian Untuk Pengamanan Informasi di Pemerintah Kabupaten Madiun;
27. Peraturan Bupati Madiun Nomor 62 Tahun 2022 Tentang Perubahan Atas Peraturan Bupati Nomor 81 Tahun 2019 Tentang Sistem Pemerintahan Berbasis Elektronik Pemerintahan Daerah;

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAH KABUPATEN MADIUN

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Madiun.
2. Pemerintah Daerah adalah Pemerintah Kabupaten Madiun.
3. Bupati adalah Bupati Kabupaten Madiun.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Madiun.
5. Dinas Komunikasi dan Informatika, yang selanjutnya disebut Dinas adalah Dinas Komunikasi dan Informatika Kabupaten Madiun.
6. Kepala Dinas Komunikasi dan Informatika, yang selanjutnya disingkat Kepala Dinas adalah Kepala Dinas Komunikasi dan Informatika Kabupaten Madiun.
7. Perangkat Daerah adalah perangkat daerah pada Pemerintah Daerah yang merupakan unsur pembantu Bupati dalam 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 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.

11. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
12. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan (*confidentiality*) atas informasi dan komunikasi secara Elektronik.
13. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas Informasi Elektronik.
14. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas Informasi Elektronik.
15. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
16. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
17. 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 integrasi/penghubung, dan perangkat Elektronik lainnya.
18. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan Teknologi Informasi dan komunikasi secara elektronik maupun nonelektronik.
19. Sistem adalah suatu kesatuan yang terdiri komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran Informasi, materi atau energi untuk mencapai suatu tujuan.
20. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan Informasi.

21. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan Keamanan Informasi berdasarkan pendekatan risiko.
22. Aset Informasi adalah unit Informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
23. Aset Pengolahan adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting Informasi.
24. Penyimpanan Informasi adalah suatu proses menyimpan Informasi dengan menggunakan media baik elektronik maupun nonelektronik.
25. Data Center/Pusat Data adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat perangkat terkait, seperti Sistem komunikasi data dan penyimpanan data.

Pasal 2

- (1) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan Kabupaten Madiun.
- (2) Kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud ayat (1) meliputi:
 - a. penetapan ruang lingkup;
 - b. penetapan penanggung jawab;
 - c. perencanaan;
 - d. dukungan pengoperasian;
 - e. evaluasi kinerja;
 - f. perbaikan berkelanjutan terhadap keamanan; dan
 - g. informasi.

- (3) Ketentuan lain untuk mendukung kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) dapat menerapkan pengendalian teknis keamanan yang meliputi:
- a. manajemen risiko;
 - b. penetapan prosedur pengendalian keamanan;
 - c. informasi SPBE; dan
 - d. pengelolaan pihak ketiga.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN
INFORMASI SPBE

Pasal 3

- (1) Penetapan 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.
- (2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Kabupaten Madiun yang harus diamankan dalam SPBE.

Pasal 4

- (1) Penetapan penanggung jawab sebagaimana dimaksud dalam pasal 2 ayat (2) huruf b dilaksanakan oleh Bupati dengan Keputusan Bupati.
- (2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh sekretaris daerah Kabupaten Madiun.
- (3) Sekretaris daerah Kabupaten Madiun sebagai penanggung jawab merupakan koordinator SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan.

Pasal 5

- (1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen keamanan informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) menetapkan pelaksana teknis Keamanan SPBE dengan Keputusan Sekretaris Daerah;
- (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 Dinas.
- (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 Kabupaten Madiun.

Pasal 6

- (1) Ketua tim sebagaimana dimaksud dalam pasal 5 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di lingkungan Kabupaten Madiun yang meliputi:
 - a. menetapkan prosedur pengendalian keamanan informasi SPBE Kabupaten Madiun;
 - b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di lingkungan Kabupaten Madiun;
 - c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan 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 dengan 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 (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.

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;
 - b. peningkatan Keamanan SPBE;

- c. penanganan insiden Keamanan SPBE; dan
 - d. audit Keamanan SPBE.
- (2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada pasal 7 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 9

- (1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 ayat (2) 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 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:
- 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 pada pasal 9 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.
- (5) Anggaran Keamanan SPBE sebagaimana dimaksud pada pasal 9 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 11

- (1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf e dilakukan oleh koordinator SPBE.
- (2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen keamanan informasi SPBE di lingkungan Kabupaten Madiun.
- (3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
 - a. menganalisis efektifitas 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 (2) 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 13

- (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 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 mengacu sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 14

- (1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada Pasal 2 ayat (3) 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 Kabupaten Madiun dengan cakupan aspek dapat 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.
- (3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk surat edaran sekretaris daerah atau kebijakan teknis lainnya.

Pasal 15

- (1) Setiap perangkat daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada Pasal 14 ayat (3).

- (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 16

- (1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) 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 (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV

PENERAPAN SISTEM MANAJEMEN

KEAMANAN INFORMASI

Pasal 17

- (1) Pengelolaan Sistem Manajemen Keamanan Informasi (SMKI) meliputi organisasi, sumber daya manusia, keamanan infrastruktur komputer, jaringan, dan sistem Informasi/ aplikasi.

- (2) Sistem Manajemen Keamanan Informasi pada Kantor Pemerintah Kabupaten Madiun berpedoman pada standar ISO/IEC 27001:2022.
- (3) Ketentuan penerapan SMKI sesuai ISO/IEC 27001:2022 ditetapkan dalam Surat Keputusan Kepala Dinas.

BAB V
KETENTUAN PENUTUP

Pasal 18

Peraturan ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang dapat mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan menempatkannya dalam Berita Daerah Pemerintah Daerah.

Ditetapkan di Caruban
pada tanggal 12 Juni 2024

Pj. BUPATI MADIUN,

ttd.

TONTRO PAHLAWANTO

Diundangkan di Caruban
pada tanggal 12 Juni 2024

Pj. SEKRETARIS DAERAH,

ttd.

SODIK HERY PURNOMO

BERITA DAERAH KABUPATEN MADIUN TAHUN 2024 NOMOR 16

Salinan sesuai dengan aslinya

