



SALINAN

WALI KOTA MADIUN

PROVINSI JAWA TIMUR

PERATURAN WALI KOTA MADIUN

NOMOR 33 TAHUN 2025

TENTANG

PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA MADIUN,

- Menimbang : a. bahwa penyelenggaraan persandian harus dilakukan untuk pengamanan informasi guna mendukung kelancaran penyelenggaraan pemerintahan;
- b. bahwa berdasarkan ketentuan Pasal 3 Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, perlu menetapkan kebijakan Pelaksanaan Persandian untuk Pengamanan Informasi;
- c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Wali Kota Madiun tentang Pelaksanaan Persandian untuk Pengamanan Informasi;
- Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. 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 (Berita Negara Republik Indonesia Tahun 1950 Nomor 45) sebagaimana telah diubah dengan Undang-Undang Nomor 13 Tahun 1954 tentang Pengubahan Undang-Undang NR 16 dan 17 Tahun 1950 (Republik Indonesia Dahulu) tentang Pembentukan Kota-Kota Besar dan Kota-Kota Kecil di Jawa (Lembaran Negara Republik Indonesia Tahun 1954 Nomor 40, Tambahan Lembaran Negara Republik Indonesia Nomor 551);

3. 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 beberapa kali terakhir 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);
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. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820);
6. Peraturan Pemerintah Nomor 49 Tahun 1982 tentang Perubahan Batas Wilayah Kotamadya Daerah Tingkat II Madiun (Lembaran Negara Republik Indonesia Tahun 1982 Nomor 76, Tambahan Lembaran Negara Republik Indonesia Nomor 3244);
7. Peraturan Pemerintah Nomor 12 Tahun 2017 tentang Pembinaan dan Pengawasan Penyelenggaraan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 73, Tambahan Lembaran Negara Republik Indonesia Nomor 6041);
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 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);
10. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
11. 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);
12. Peraturan Daerah Kota Madiun Nomor 6 Tahun 2017 tentang Pedoman Pembentukan Produk Hukum Daerah (Lembaran Daerah Kota Madiun Tahun 2017 Nomor 6/D, Tambahan Lembaran Daerah Kota Madiun Nomor 40);

MEMUTUSKAN:

Menetapkan : PERATURAN WALI KOTA TENTANG PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:

1. Daerah adalah Kota Madiun.
2. Pemerintah Daerah adalah Pemerintah Kota Madiun.
3. Wali Kota adalah Wali Kota Madiun.
4. Perangkat Daerah adalah Perangkat Daerah di Lingkungan Pemerintah Kota Madiun.
5. Dinas adalah Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang Persandian.

6. Persandian adalah kegiatan di bidang pengamanan data/informasi yang dilaksanakan dengan menerapkan konsep, teori, seni dan ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terkait pada etika profesi sandi.
7. Jaring Komunikasi Sandi yang selanjutnya disingkat JKS adalah keterhubungan antar pengguna persandian melalui jaringan telekomunikasi.
8. 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 ataupun non elektronik.
9. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan menyebarkan informasi.
10. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.
11. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan keamanan informasi.
12. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
13. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikat elektronik.
14. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan urusan pemerintahan bidang persandian dan yang memiliki nilai manfaat.
15. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan layanan keamanan informasi.
16. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

BAB II
PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN
INFORMASI
Bagian Kesatu
Umum
Pasal 2

- (1) Penyelenggaraan Persandian untuk Pengamanan Informasi dilaksanakan melalui:
 - a. penyusunan kebijakan Pengamanan Informasi;
 - b. pengelolaan sumber daya Keamanan Informasi;
 - c. pengamanan Sistem Elektronik dan Pengamanan Informasi nonelektronik; dan
 - d. penyediaan layanan Keamanan Informasi.
- (2) Wali Kota sesuai dengan kewenangannya bertanggung jawab terhadap penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1).

Bagian Kedua
Penyusunan Kebijakan Pengamanan Informasi
Paragraf 1
Umum
Pasal 3

- Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf a dilakukan dengan:
- a. menyusun rencana strategis Pengamanan Informasi;
 - b. menetapkan arsitektur Keamanan Informasi; dan
 - c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

Paragraf 2
Rencana Strategis Pengamanan Informasi
Pasal 4

- (1) Rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 3 huruf a disusun oleh Wali Kota.
- (2) Penyusunan rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.

- (3) Rencana strategis sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. tujuan, sasaran, program, kegiatan, dan target pelaksanaan Pengamanan Informasi setiap tahun untuk jangka waktu 5 (lima) tahun; dan
 - b. peta rencana penyelenggaraan Pengamanan Informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun untuk jangka waktu 5 (lima) tahun.
- (4) Rencana strategis Pengamanan Informasi yang telah disusun sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah.
- (5) Dalam melakukan penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) Wali Kota dapat melakukan koordinasi dan konsultasi kepada BSSN.
- (6) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (5) Wali Kota dapat menunjuk Dinas.

Paragraf 3

Arsitektur Keamanan Informasi

Pasal 5

- (1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 3 huruf b ditetapkan oleh Wali Kota.
- (2) Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) memuat:
 - a. infrastruktur Teknologi Informasi;
 - b. desain keamanan perangkat Teknologi Informasi dan keamanan jaringan; dan
 - c. aplikasi keamanan perangkat Teknologi Informasi dan keamanan jaringan.
- (3) Dalam melakukan penyusunan Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) Wali Kota dapat melakukan koordinasi dan konsultasi kepada BSSN.
- (4) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (3) Wali Kota dapat menunjuk Dinas.
- (5) Arsitektur Keamanan Informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.
- (6) Arsitektur Keamanan Informasi dilakukan evaluasi oleh Wali Kota pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu-waktu sesuai dengan kebutuhan.

Paragraf 4
Tata Kelola Keamanan Informasi
Pasal 6

- (1) Aturan mengenai tata Kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 3 huruf c ditetapkan oleh Wali Kota.
- (2) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) paling sedikit terdiri atas:
 - a. keamanan sumber daya Teknologi Informasi;
 - b. keamanan akses control;
 - c. keamanan data dan Informasi;
 - d. keamanan sumber daya manusia
 - e. keamanan jaringan;
 - f. keamanan surat elektronik;
 - g. keamanan pusat data;
 - h. keamanan komunikasi; dan/atau
 - i. keamanan aplikasi Sistem Pemerintahan Berbasis Elektronik.
- (3) Dalam melakukan penyusunan aturan atau prosedur teknis mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1), Wali Kota dapat melakukan koordinasi dan konsultasi kepada BSSN.
- (4) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (3) Wali Kota dapat menunjuk Dinas.
- (5) Dalam kondisi tertentu, masing-masing Perangkat Daerah dapat menyusun dan menetapkan aturan atau prosedur teknis mengenai tata kelola Keamanan Informasi di lingkungannya setelah terlebih dahulu berkoordinasi dan berkonsultasi dengan Dinas.

Bagian Ketiga
Pengelolaan Sumber Daya Keamanan Informasi
Paragraf 1
Umum
Pasal 7

- (1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf b dilaksanakan oleh Dinas.

- (2) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
- a. pengelolaan aset keamanan Teknologi Informasi dan komunikasi;
 - b. pengelolaan sumber daya manusia; dan
 - c. manajemen pengetahuan.

Paragraf 2

Pengelolaan Aset Keamanan Teknologi Informasi dan
Komunikasi

Pasal 8

- (1) Pengelolaan aset keamanan Teknologi Informasi dan komunikasi sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf a dilakukan oleh Dinas dan berkoordinasi dengan Badan Keuangan dan Aset Daerah.
- (2) Pengelolaan aset keamanan Teknologi Informasi dan komunikasi dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan Teknologi Informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.
- (3) Aset keamanan Teknologi Informasi dan komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi, dan/atau memulihkan insiden Keamanan Informasi dalam Sistem Elektronik.

Paragraf 3

Pengelolaan Sumber Daya Manusia

Pasal 9

Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf b dilakukan oleh Dinas dan berkoordinasi dengan Badan Kepegawaian dan Pengembangan Sumber Daya Manusia.

Paragraf 3

Manajemen Pengetahuan

Pasal 10

- (1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf c dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.

- (2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi Pemerintah Daerah.
- (3) Manajemen pengetahuan sebagaimana dimaksud pada ayat (2) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi Pemerintah Daerah.
- (4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.
- (5) Dalam pelaksanaan manajemen pengetahuan, Dinas berkoordinasi dan berkonsultasi dengan BSSN.

Bagian Keempat

Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Paragraf 1

Umum

Pasal 11

Pengamanan Sistem Elektronik dan Pengamanan Informasi nonelektronik sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf c dilaksanakan oleh Dinas.

Paragraf 2

Pengamanan Sistem Elektronik

Pasal 12

Pengamanan Sistem Elektronik terdiri atas:

- a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirangkal terhadap data dan Informasi;
- b. penjaminan ketersediaan infrastruktur yang terdiri atas pusat data, jaringan intra pemerintah, dan sistem penghubung layanan penyelenggaraan pemerintahan berbasis elektronik; dan
- c. penjaminan keutuhan, ketersediaan, dan keaslian aplikasi.

Pasal 13

- (1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 12, Dinas melakukan:
 - a. identifikasi;
 - b. deteksi;
 - c. proteksi; dan
 - d. penanggulangan dan pemulihan.

- (2) Identifikasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui kegiatan analisis kerawanan dan risiko terhadap Sistem Elektronik.
- (3) Deteksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui kegiatan analisis untuk menentukan adanya ancaman atau kejadian insiden pada Sistem Elektronik.
- (4) Proteksi sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan kegiatan mitigasi risiko dan penerapan perlindungan terhadap Sistem Elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintahan berbasis elektronik.
- (5) Penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (1) huruf d dilakukan dengan kegiatan penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Pasal 14

- (1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 13 Pemerintah Daerah wajib menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.
- (2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh Balai Besar Sertifikasi Elektronik.
- (3) Pemanfaatan Sertifikat Elektronik di lingkungan Pemerintah Daerah bertujuan:
 - a. membantu Perangkat Daerah dalam Pengamanan Informasi milik Pemerintah Daerah;
 - b. meningkatkan kinerja Perangkat Daerah dalam pelaksanaan Sistem Pemerintahan Berbasis Elektronik;
 - c. menjamin integritas Informasi untuk memastikan bahwa Informasi tidak diubah/dimodifikasi selama penyimpanan atau pada saat dikirimkan;
 - d. menjamin keautentikan pemilik Informasi untuk memastikan bahwa Informasi dikirimkan dan diterima oleh pihak yang benar (keaslian pengirim/penerima Informasi);

- e. menjamin nir-penyangkalan untuk memastikan bahwa pemilik Informasi tidak dapat menyangkal bahwa Informasi tersebut adalah miliknya atau telah disahkan olehnya;
 - f. menjaga kerahasiaan untuk memastikan bahwa Informasi hanya dapat diakses oleh pihak yang sah;
 - g. meningkatkan kepercayaan dan penerimaan terhadap implementasi Sistem Elektronik; dan
 - h. meningkatkan efisiensi dan efektifitas penyelenggaraan pemerintahan dan pelayanan publik.
- (4) Untuk mendapatkan Sertifikat Elektronik sebagaimana dimaksud pada ayat (2), Otoritas Pendaftaran bertanggung jawab melakukan pemeriksaan, pemberian persetujuan atau penolakan atas setiap permintaan penerbitan, pembaruan, dan pencabutan Sertifikat Elektronik yang diajukan oleh pemilik atau calon Pemilik Sertifikat Elektronik.
- (5) Dinas berkedudukan sebagai Otoritas Pendaftaran.
- (6) Pemanfaatan Sertifikat Elektronik sebagaimana dimaksud pada ayat (4) berpedoman pada Peraturan Wali Kota Madiun yang mengatur tentang Pemanfaatan Sertifikat Elektronik.

Pasal 15

- (1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 14 ayat (1) Pemerintah Daerah dapat menyelenggarakan pusat operasi Pengamanan Informasi sesuai standar yang ditetapkan oleh BSSN.
- (2) Pusat operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk pengamanan Sistem Elektronik dengan melakukan proses pengawasan, penanggulangan, dan pemulihan atas insiden keamanan Sistem Elektronik dengan memperhatikan aspek personel, proses pelaksanaan, dan ketersediaan teknologi.

Paragraf 3

Pengamanan Informasi Nonelektronik

Pasal 16

- (1) Pengamanan Informasi nonelektronik dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan Informasi nonelektronik.

- (2) Pengamanan Informasi nonelektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 17

- (1) Dinas melaksanakan audit Keamanan Informasi.
- (2) Audit Keamanan Informasi meliputi audit keamanan Sistem Elektronik dan audit pelaksanaan sistem manajemen.
- (3) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima

Penyediaan Layanan Keamanan Informasi

Pasal 18

- (1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 2 ayat (1) huruf d dilaksanakan oleh Dinas.
- (2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
 - a. Wali Kota dan Wakil Wali Kota;
 - b. Perangkat Daerah;
 - c. aparatur sipil negara dan pegawai pada Pemerintah Daerah; dan
 - d. pihak lainnya.

Pasal 19

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 18 ayat (1) meliputi:

- a. identifikasi kerentanan dan penilaian risiko terhadap Sistem Elektronik;
- b. asistensi dan fasilitasi penguatan keamanan Sistem Elektronik;
- c. penerapan Sertifikat Elektronik untuk melindungi Sistem Elektronik dan dokumen elektronik;
- d. perlindungan Informasi melalui penyediaan perangkat teknologi Keamanan Informasi dan JKS;

- e. fasilitasi sertifikasi penerapan manajemen pengamanan Sistem Elektronik;
- f. audit keamanan Sistem Elektronik;
- g. audit keamanan pelaksanaan sistem manajemen;
- h. literasi Keamanan Informasi dalam rangka peningkatan kesadaran Keamanan Informasi dan pengukuran tingkat kesadaran Keamanan Informasi di lingkungan Pemerintah Daerah dan Publik;
- i. peningkatan kompetensi sumber daya manusia di bidang Keamanan Informasi dan/atau persandian;
- j. pengelolaan pusat operasi Pengamanan Informasi;
- k. penanganan insiden keamanan Sistem Elektronik;
- l. forensik digital;
- m. perlindungan Informasi pada kegiatan penting Pemerintah Daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
- n. perlindungan Informasi pada aset/fasilitas penting milik atau yang akan digunakan Pemerintah Daerah melalui kegiatan kontra penginderaan;
- o. konsultasi Keamanan Informasi bagi Pengguna Layanan; dan/atau
- p. jenis Layanan Keamanan Informasi lainnya.

Pasal 20

- (1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 19, Dinas melaksanakan manajemen Layanan Keamanan Informasi.
- (2) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan Keamanan Informasi kepada Pengguna Layanan.
- (3) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) merupakan penanganan terhadap keluhan, gangguan, masalah, permintaan, dan/atau perubahan Layanan Keamanan Informasi dari Pengguna Layanan.
- (4) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen Layanan Keamanan Informasi.

BAB III
PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI
Pasal 21

- (1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah ditetapkan oleh Wali Kota.
- (2) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (1) untuk menentukan JKS internal Pemerintah Daerah.
- (3) JKS internal Pemerintah Daerah sebagaimana dimaksud pada ayat (2) terdiri atas:
 - a. JKS antar Perangkat Daerah;
 - b. JKS internal Perangkat Daerah; dan
 - c. JKS pimpinan daerah.
- (4) JKS antar Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh Perangkat Daerah.
- (5) JKS internal Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar Pengguna Layanan di lingkup internal Perangkat Daerah.
- (6) JKS pimpinan daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Wali Kota, Wakil Wali Kota, dan kepala Perangkat Daerah.

Pasal 22

- (1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 21 ayat (1) dilaksanakan melalui:
 - a. identifikasi pola hubungan komunikasi sandi; dan
 - b. analisis pola hubungan komunikasi sandi.
- (2) Identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf a, dilakukan terhadap:
 - a. pola hubungan komunikasi pimpinan dan pejabat struktural internal Pemerintah Daerah;
 - b. alur Informasi yang dikomunikasikan antar Perangkat Daerah dan internal Perangkat Daerah;
 - c. Teknologi Informasi dan komunikasi;
 - d. infrastruktur komunikasi; dan
 - e. kompetensi personel.

- (3) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2).
- (4) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3) memuat:
 - a. Pengguna Layanan yang akan terhubung dalam JKS;
 - b. topologi atau bentuk atau model keterhubungan JKS antar Pengguna Layanan;
 - c. perangkat keamanan Teknologi Informasi dan komunikasi, infrastruktur komunikasi, serta fasilitas lainnya yang dibutuhkan; dan
 - d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.
- (5) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (4) ditetapkan sebagai pola hubungan komunikasi sandi antar Perangkat Daerah oleh Wali Kota dengan Keputusan Wali Kota.

BAB IV

PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 23

- (1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.
- (2) Kepala Dinas melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali dan menyampaikan laporannya kepada Wali Kota dan Gubernur sebagai wakil Pemerintah Pusat.

Pasal 24

Pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB V
PENDANAAN
Pasal 25

Pendanaan pelaksanaan Persandian untuk Pengamanan Informasi bersumber dari:

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

BAB VI
KETENTUAN PENUTUP
Pasal 26

Peraturan Wali Kota ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Wali Kota ini dengan penempatannya dalam Berita Daerah Kota Madiun.

Ditetapkan di Madiun
pada tanggal 22 September 2025

WALI KOTA MADIUN,

ttd

MAIDI

Diundangkan di Madiun
pada tanggal 22 September 2025

SEKRETARIS DAERAH,

ttd

SOEKO DWI HANDIARTO

BERITA DAERAH KOTA MADIUN
TAHUN 2025 NOMOR 33/G

Salinan sesuai dengan aslinya
a.n. Sekretaris Daerah,
u.b.
Kepala Bagian Hukum,



Ika Puspitaria, S.H., M.M.
Pembina (IV/a)
NIP 198212132006042009