WALIKOTA MAGELANG
PROVINSI JAWA TENGAH

PERATURAN WALIKOTA MAGELANG
NOMOR 53 TAHUN 2022
TENTANG
PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH KOTA MAGELANG

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALIKOTA MAGELANG,

Menimbang :

a. bahwa penyelenggaraan persandian dilakukan guna mendukung kelancaran penyelenggaraan pemerintahan, adminstrasi pemerintahan, dan/atau pelayanan publik untuk sebesar-besar kesejahteraan masyarakat berdasarkan Pancasila dan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
b. bahwa untuk memenuhi kebutuhan pengamanan informasi di lingkungan Pemerintah Kota Magelang, diperlukan adanya pedoman penyelenggaraan yang mengatur norma, standar, prosedur, dan kriteria;
c. bahwa untuk memberikan kepastian hukum dan kejelasan kebijakan persandian di lingkungan Pemerintah Kota Magelang, perlu adanya peraturan mengenai penyelenggaraan persandian untuk pengamanan informasi;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Walikota tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintah Kota Magelang;

Mengingat :

1. Undang-Undang Nomor 17 Tahun 1950 tentang Pembentukan Daerah-daerah Kota Kecil dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, dan Jawa Barat (Berita Negara Republik Indonesia Tanggal 14 Agustus Tahun 1950) sebagaimana telah diubah dengan Undang-Undang Nomor 13 Tahun 1954 tentang Pengubahan Undang-Undang Nomor 16 dan 17 Tahun 1950 (Lembaran Negara Republik Indonesia Tahun 1954 Nomor 40, Tambahan Lembaran Negara Republik Indonesia Nomor 551);
2. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);

3. Peraturan Kepala 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);

MEMUTUSKAN:

Menetapkan : PERATURAN WALIKOTA TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KOTA MAGELANG.

BAB I
KETENTUAN UMUM

Bagian Kesatu
Pengertian

Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan:

1. Daerah adalah Kota Magelang.
2. Pemerintah Daerah adalah Walikota sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Walikota adalah Walikota Magelang.
4. Perangkat Daerah adalah unsur pembantu Walikota dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Pemerintah Daerah.
5. Urusan Pemerintahan adalah kekuasaan pemerintahan yang menjadi kewenangan Presiden yang pelaksanaannya dilakukan oleh kementrian negara dan penyelenggara Pemerintah Daerah untuk melindungi, melayani, memberdayakan, dan menyejahterakan masyarakat.
6. Dinas adalah Perangkat Daerah yang menyelenggarakan Urusan Pemerintahan bidang persandian.
7. 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.
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. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan informasi.

10. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang persandian yang memiliki nilai manfaat.
11. Pengguna Layanan Keamanan Infomasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
12. Pengamanan Informasi adalah segala upaya, kegiatan, dan Tindakan untuk mewujudkan Keamanan Informasi.
13. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
14. 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 sertifikasi elektronik.
15. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

Bagian Kedua
Maksud, Tujuan, dan Ruang Lingkup

Pasal 2

(1) Peraturan Walikota ini dimaksudkan untuk memberikan pedoman dalam melaksanakan kebijakan, program, dan kegiatan penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah.
(2) Peraturan Walikota ini bertujuan untuk:
    a. menciptakan harmonisasi dalam pembagian Urusan Pemerintahan di bidang Persandian;
    b. meningkatkan efektivitas pelaksanaan kebijakan, program, dan kegiatan penyelenggaraan Persandian untuk Pengamanan Informasi.

Pasal 3

Ruang lingkup Peraturan Walikota ini meliputi:
a. perencanaan;
b. pelaksanaan;
c. forum Keamanan Informasi;
d. pemantauan, evaluasi, dan pelaporan;
e. pembinaan dan pengawasan teknis; dan
f. pembiayaan.

BAB II
PERENCANAAN

Pasal 4

(1) Perencanaan penyelenggaraan Persandian di lingkungan Pemerintah Daerah dimuat dalam rencana strategis Dinas dan dikoordinasikan dengan Perangkat Daerah yang menyelenggarakan Urusan Pemerintahan di bidang perencanaan pembangunan.

(2) Perencanaan penyelenggaraan Persandian sebagaimana dimaksud pada ayat (1) diintregasikan dengan Dokumen Perencanaan Pembangunan Daerah berupa Rencana Pembangunan Jangka Panjang Daerah (RPJPD), Rencana Pembangunan Jangka Menengah Daerah (RPJMD), dan Rencana Kerja Pemerintah Daerah (RKPD).

(3) Penyusunan perencanaan penyelenggaraan Persandian sebagaimana dimaksud pada ayat (1) dikoordinasikan kepada Pemerintah Provinsi Jawa Tengah dan BSSN oleh Dinas.

BAB III
PELAKSANAAN

Bagian Kesatu
Umum

Pasal 5

(1) Pelaksanaan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah meliputi:
   a. penyelenggaraan kegiatan Persandian untuk Pengamanan Informasi;
   b. penetapan pola hubungan komunikasi sandi antar-Perangkat Daerah;
   c. penyelenggaraan Sertifikat Elektronik di lingkungan Pemerintah Daerah untuk mendukung Sistem Pemerintahan Berbasis Elektronik.

(2) Pelaksanaan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Walikota melalui:
   a. penguatan kapasitas kelembagaan, sumber daya manusia, dan sarana prasarana;
   b. koordinasi kegiatan antar-Perangkat Daerah; dan
   c. kerja sama dengan kabupaten/kota lain dan/atau provinsi.

Pasal 6

(1) Pelaksanaan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah meliputi:
   a. penyediaan analisis kebutuhan penyelenggaraan Persandian untuk Pengamanan Informasi;
   b. penyediaan kebijakan penyelenggaraan Persandian untuk Pengamanan Informasi;
   c. pengelolaan dan perlindungan informasi;

d. pengelolaan sumber daya Persandian meliputi sumber daya manusia, Materiil Sandi dan Jaring Komunikasi Sandi serta anggaran;
e. penyelenggaraan operasional dukungan Persandian untuk Pengamanan Informasi;
f. pengawasan dan evaluasi penyelenggaraan Pengamanan Informasi melalui Persandian di seluruh Perangkat Daerah; dan
g. koordinasi dan konsultasi penyelenggaraan Persandian untuk Pengamanan Informasi.

(2) Pengamanan informasi sebagaimana dimaksud pada ayat (1) mencakup pengamanan fisik, pengamanan logis, dan perlindungan secara administrasi.

Bagian Kedua
Penyelenggaraan Persandian untuk Pengamanan Informasi

Paragraf 1
Umum

Pasal 7

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.

Paragraf 2
Penyusunan Kebijakan Pengamanan Informasi

Pasal 8

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 7 ayat (1) dilaksanakan dengan:
a. menyusun rencana penyelenggaraan Pengamanan Informasi yang dimuat dalam rencana strategis Dinas;
b. menetapkan arsitektur Keamanan Informasi; dan
c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

Pasal 9

(1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 8 huruf b memuat:
   a. infrastruktur teknologi informasi;
   b. desain keamanan perangkat teknologi informasi dan keamanan jaringan; dan
   c. aplikasi keamanan perangkat teknologi informasi dan keamanan jaringan.
(2) Dalam melakukan penyusunan arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) Dinas dapat melakukan koordinasi dan konsultasi kepada Pemerintah Provinsi Jawa Tengah dan BSSN.
(3) Arsitektur Keamanan Informasi berlaku untuk jangka waktu 5 (lima) tahun.

(4) Arsitektur Keamanan Informasi dievaluasi pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu-waktu sesuai dengan kebutuhan.

Pasal 10

(1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 7 ayat (3) dituangkan dalam kebijakan yang ditetapkan oleh Walikota.
(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 kontrol;
    c. keamanan data dan informasi;
    d. keamanan sumber daya manusia;
    e. keamanan jaringan;
    f. keamanan surat elektronik;
    g. keamanan pusat data; dan/atau
    h. keamanan komunikasi.
(3) Penyusunan aturan tata kelola Keamanan Informasi dilaksanakan oleh Dinas.
(4) Dalam penyusunan aturan tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) Dinas melakukan koordinasi dan konsultasi kepada Pemerintah Provinsi Jawa Tengah dan BSSN.

Paragraf 3
Pengelolaan Sumber Daya Keamanan Informasi

Pasal 11

(1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 7 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.

Pasal 12

(1) Pengelolaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a dilakukan oleh Dinas dan berkoordinasi dengan Perangkat Daerah yang melaksanakan fungsi pengelolaan barang milik daerah.
(2) Pengelolaan aset keamanan teknologi informasi dan komunikasi dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi infomasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.

(3) Aset keamanan teknologi infomasi dan komunikasi sebagimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi, dan/atau memulihkan insiden Keamanan Informasi pada Sistem Elektronik.

Pasal 13

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b dilakukan oleh Dinas dan berkoordinasi dengan Perangkat Daerah yang melaksanakan fungsi penunjang kepegawaian, Pendidikan, dan pelatihan.

(2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses sebagai berikut:
   a. pengembangan kompetensi;
   b. pembinaan karir;
   c. pendayagunaan; dan
   d. pemberian tunjangan pengamanan persandian.

Pasal 14

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf a dilaksanakan melalui:
   a. tugas belajar, pendidikan dan pelatihan pembentukan dan penjenjangan fungsional, pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, *workshop,* seminar, dan kegiatan lainnya yang terkait pengembangan kompetensi sumber saya manusia di bidang Keamanan Informasi;
   b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, Pemerintah Daerah atau pihak lainnya; dan
   c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi bidangnya.

(2) Pengembangan kompetensi sebagaimana dimaksud pada ayat (1) dilaksanakan dengan ketentuan memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi di bidang Keamanan Informasi.

(3) Pembinaan karir sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf b dilaksanakan melalui:
   a. pembinaan jabatan fungsional di bidang Keamanan Informasi; dan
   b. pengisian formasi jabatan sesuai dengan standar kompetensi yang ditetapkan.

(4) Pendayagunaan sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf b dilaksanakan dengan ketentuan:
   a. seluruh sumber daya manusia yang bertugas di bidang Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi pegawai yang ditetapkan;

b. untuk memenuhi kebutuhan dan mengantisipasi keterbatasan sumber daya manusia persandian/Keamanan Informasi, pegawai yang telah memiliki sertifikasi, keahlian dan atau pernah mengikuti Pendidikan dan pelatihan sandi yang diselenggarakan oleh BSSN sebagai Pembina dan penyelenggara persandian nasional, tetap ditugaskan secara penuh di bidang Persandian dan tidak dimutasi ke bidang tugas lain kecuali promosi jabatan.

Pasal 15

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.
(2) Manajemen pengetahuan 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 (1) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi Pemerintah Daerah.
(4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.

Paragraf 4

Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Pasal 16

Pengamanan Sistem Elektronik dan Pengamanan Informasi nonelektronik sebagaimana dimaksud dalam Pasal 7 huruf c dilaksanakan oleh Dinas.

Pasal 17

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 16 terdiri atas:

a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan nirsangkal terhadap data, dan informasi;
b. penjaminan ketersediaan infrastruktur yang terdiri atas pusat data, jaringan intrapemerintah, dan sistem penghubung layanan penyelenggaraan sistem informasi berbasis elektronik; dan
c. penjaminan keutuhan, ketersediaan, dan keaslian aplikasi.

Pasal 18

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 17, 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 19

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 17, Pemerintah Daerah dapat menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.
(2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh BSSN dan /atau lembaga Penyelenggara Sertifikasi Elektronik dalam negeri yang telah diakui.
(3) Untuk mendapatkan Sertifikat Elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 20

(1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 18 ayat (1), Pemerintah Daerah dapat menyelenggarakan pusat operasi Pengamanan Informasi sesuai dengan standar yang diterapkan 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, pelaksanaan, dan ketersediaan teknologi.

Pasal 21

(1) Pengamanan Informasi nonelektronik sebagaimana dimaksud dalam Pasal 16 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 22

(1) Dinas melaksanakan audit Keamanan Informasi di lingkup Pemerintah Daerah.
(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.

Paragraf 5
Penyediaan Layanan Keamanan Informasi

Pasal 23

(1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 7 huruf d dilaksanakan oleh Dinas.
(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
    a. Walikota dan Wakil Walikota;
    b. Perangkat Daerah;
    c. Pegawai atau Aparatur Sipil Negara pada Pemerintah Daerah; dan
    d. pihak lainnya.

Pasal 24

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 23 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 jaring komunikasi sandi;
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 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 25

(1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 24, 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.

Bagian Ketiga

Penetapan Pola Hubungan Komunikasi Sandi antar-Perangkat Daerah

Pasal 26

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

Pasal 27

(1) Penetapan pola hubungan komunikasi sandi antar-Perangkat Daerah sebagaimana dimaksud dalam Pasal 26 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 jaring komunikasi sandi;
   b. topologi atau bentuk atau model keterhubungan Jaring Komunikasi Sandi antar-Pengguna Layanan;
   c. perangkat keamanan teknologi informasi dan komunikasi, dan 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 Walikota dalam bentuk keputusan.

(6) Keputusan sebagaimana dimaksud pada ayat (5) paling sedikit memuat:
   a. entitas Pengguna Layanan yang terhubung dalam jaring komunikasi sandi;
   b. topologi atau bentuk atau model keterhubungan antar-Pengguna Layanan;
   c. sarana dan prasarana yang digunakan; dan
   d. tugas dan tanggungjawab pengelola dan Pengguna Layanan.

(7) Salinan keputusan sebagaimana dimaksud pada ayat (6) disampaikan oleh Walikota kepada Gubernur Provinsi Jawa Tengah sebagai wakil Pemerintah Pusat dan ditembuskan kepada Kepala BSSN.

Bagian Keempat
Penyelenggaraan Sertifikat Elektronik di Lingkungan Pemerintah Daerah Guna Mendukung Sistem Pemerintahan Berbasis Elektronik

Pasal 28

(1) Dalam melaksanakan Pengamanan Sistem Elektronik dapat menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.
(2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh Balai Sertifikasi Elektronik atau lembaga Penyelenggara Sertifikasi Elektronik dalam negeri yang telah diakui.
(3) Penyelenggaraan Sertifikat Elektronik di lingkungan Pemerintah Daerah bertujuan:
    a. meningkatkan kapabilitas dan tata kelola Keamanan Informasi dalam penyelenggaraan Sistem Elektronik;
    b. meningkatkan Keamanan Informasi pada Sistem Elektronik;
    c. meningkatkan kepercayaan, kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan terhadap implementasi Sistem Elektronik; dan
    d. meningkatkan efisiensi dan efektivitas penyelenggaraan pemerintahan dan pelayanan publik.
(4) Untuk mendapatkan Sertifikat Elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan oleh Otoritas Pendaftaran (OP) yang bertanggung jawab melakukan pemeriksaan, pemebrian 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 (OP).

BAB IV
FORUM KOMUNIKASI KEAMANAN INFORMASI

Pasal 29

(1) Dalam mendukung penyelenggaran Jaring Komunikasi Sandi yang efektif, efisien, dan komprehensif di lingkungan Pemerintah Daerah, perlu dibentuk Forum Komunikasi Keamanan Informasi.
(2) Forum Komunikasi Keamanan Informasi sebagaimana dimaksud pada ayat (1) dapat beranggotakan Instansi di lingkungan Pemerintah Daerah, Instansi Vertikal, komunitas serta Badan Usaha Milik Daerah.
(3) Forum Komunikasi Keamanan Informasi sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Walikota.

BAB V
PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 30

(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.
(3) Kepala Dinas menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) kepada Walikota dan Gubernur sebagai wakil Pemerintah Pusat.

Pasal 31

Pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI
PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 32

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi pada Pemerintah Daerah dilaksanaan oleh BSSN dan Gubernur Provinsi Jawa Tengah sebagai wakil Pemerintah Pusat.

Pasal 33

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi pada Pemerintah Daerah dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII
PEMBIAYAAN

Pasal 34

Pembiayaan pelaksanaan penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah 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 VII
KETENTUAN PENUTUP

Pasal 35

Peraturan Walikota ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Magelang
pada tanggal 4 Oktober 2022
WALIKOTA MAGELANG

MUCHAMAD NUR AZIZ

Diundangkan di Magelang
Pada tanggal 4 Oktober 2022

SEKRETARIS DAERAH
KOTA MAGELANG

JOKO BUDIYONO

BERITA DAERAH PEMERINTAH KOTA MAGELANG TAHUN 2022 NOMOR 55