WALI KOTA MAGELANG
PROVINSI JAWA TENGAH

PERATURAN WALI KOTA MAGELANG
NOMOR 39 TAHUN
TENTANG
MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA MAGELANG,

Menimbang :

a. bahwa penyelenggaraan pemerintahan berbasis elektronik yang aman di lingkungan Pemerintah Kota Magelang dilaksanakan dengan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan, dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;
b. bahwa untuk memenuhi kebutuhan akan keamanan sistem pemerintahan berbasis elektronik, diperlukan adanya suatu proses manajemen yang mencakup kebijakan, pengendalian teknis, sampai dengan dukungan operasional;
c. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur, perlu pengaturan mengenai manajemen keamanan informasi sistem pemerintahan berbasis elektronik;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Wali Kota tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Daerah;

Mengingat :

1. Undang-Undang Nomor 17 Tahun 1950 tentang Pembentukan Daerah-daerah Kota Kecil dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, dan Jawa Barat;
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 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);

MEMUTUSKAN:

MEMUTUSKAN:

Menetapkan : PERATURAN WALI KOTA TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH DAERAH.

BAB I
KETENTUAN UMUM

Bagian Kesatu
Pengertian

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:

1. Daerah adalah Kota Magelang.
2. Pemerintah Daerah adalah Wali Kota sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Wali Kota adalah Wali Kota Magelang.
4. Perangkat Daerah adalah unsur pembantu Wali Kota dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
5. Dinas adalah Perangkat Daerah yang menyelenggarakan urusan pemerintahan bidang Persandian dan Keamanan Informasi.
6. 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.
7. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan dan pemindahan informasi antarmedia.
8. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan informasi.
9. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan dengan memanfaatkan Teknologi Informasi dan Komunikasi yang memberikan layanan kepada pengguna SPBE.
10. Keamanan Informasi SPBE adalah penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan sumber daya terkait data dan informasi, infrastruktur SPBE, dan Aplikasi SPBE.
11. Manajemen Keamanan Informasi SPBE adalah serangkaian proses untuk mencapai penerapan Keamanan Informasi SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.

12. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas dan fungsi layanan SPBE.
13. Infrastruktur SPBE adalah semua perangkat keras, perangkat lubak, dan fasilitas penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
14. 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 Wali Kota ini dimaksudkan sebagai kebijakan internal dalam pengelolaan Keamanan Informasi SPBE secara terpadu di lingkungan Pemerintah Daerah.
(2) Peraturan Wali Kota ini bertujuan untuk:
    a. menciptakan tata kelola penyelenggaraan Keamanan Informasi SPBE di lingkungan Pemerintah Daerah;
    b. meningkatkan kapabilitas penyelenggaraan Keamanan Informasi SPBE di lingkungan Pemerintah Daerah;
    c. meningkatkan kepercayaan, kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan terhadap informasi; dan
    d. meningkatkan efisiensi dan efektivitas penyelenggaraan layanan pemerintahan dan layanan publik di lingkungan Pemerintah Daerah.

Pasal 3

Ruang lingkup Peraturan Wali Kota ini meliputi:
a. kebijakan internal Manajemen Keamanan Informasi SPBE;
b. pengendalian teknis Keamanan Informasi SPBE; dan
c. dukungan operasional penyelenggaraan Manajemen Keamanan Informasi SPBE.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu
Umum

Pasal 4

Kebijakan internal Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 3 huruf a meliputi:
a. penetapan ruang lingkup;
b. penetapan penanggung jawab;
c. perencanaan;
d. dukungan pengoperasian;
e. evaluasi kinerja; dan
f. perbaikan berkelanjutan terhadap Keamanan Informasi.

Bagian Kedua
Penetapan Ruang Lingkup

Pasal 5

(1) Penetapan ruang lingkup Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 4 huruf a meliputi aset:
   a. data dan informasi SPBE;
   b. Aplikasi SPBE; dan
   c. Infrastruktur SPBE.
(2) Aset sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Daerah yang harus diamankan dalam SPBE.

Bagian Ketiga
Penetapan Penanggung Jawab

Pasal 6

(1) Wali Kota menetapkan penanggung jawab Kebijakan internal Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 4 huruf b.
(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
(3) Sekretaris Daerah sebagai penanggung jawab merupakan ketentuan yang tidak terpisahkan dari tugas sebagai Koordinator SPBE yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 7

(1) Dalam melaksanakan tugas sebagai penanggung jawab Manajemen Keamanan Informasi SPBE, Sekretaris Daerah sebagaimana dimaksud dalam Pasal 6 ayat (3) dapat menetapkan tim pelaksana teknis Keamanan Informasi SPBE.
(2) Tim pelaksana teknis Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. ketua tim; dan
   b. anggota tim.
(3) Ketua tim sebagaimana dimaksud pada ayat (2) huruf a dijabat oleh Kepala Dinas.
(4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b terdiri atas seluruh pimpinan Perangkat Daerah yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan data dan informasi, aplikasi atau Infrastruktur SPBE di lingkungan Pemerintah Daerah.

Pasal 8

(1) Ketua tim sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf a bertugas memastikan pelaksanaan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah yang meliputi:
   a. menetapkan standar operasional dan prosedur pengendalian Keamanan Informasi SPBE Pemerintah Daerah;
   b. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE Pemerintah Daerah;

c. memastikan penerapan keamanan data dan informasi SPBE, keamanan Aplikasi SPBE dan Infrastruktur SPBE pada seluruh Perangkat Daerah sesuai dengan standar teknis dan prosedur Keamanan Informasi SPBE yang telah ditetapkan;
d. merumuskan, menetapkan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Informasi SPBE;
e. memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan/atau Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan Informasi SPBE yang telah ditetapkan;
f. memutuskan, merancang, melaksanakan, dan mengelola langkah keberlangsungan proses bisnis TIK dalam bentuk dokumen rencana kelangsungan bisnis (*business continuity plans*) dan dokumen rencana pemulihan pascabencana (*disaster recovery plans*); dan
g. melaporkan pelaksanaan manajemen Keamanan Informasi SPBE pada koordinator SPBE.

(2) Anggota tim sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf b bertugas:
a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian Keamanan Informasi SPBE pada Perangkat Daerah masing-masing;
b. memastikan penerapan keamanan data dan informasi, keamanan Aplikasi SPBE dan Infrastruktur SPBE pada Perangkat Daerah sesuai dengan standar teknis dan prosedur Keamanan Informasi SPBE yang telah ditetapkan;
c. memantau pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga agar memenuhi standar teknis dan prosedur Keamanan Informasi SPBE yang telah ditetapkan serta melaporakannya kepada ketua tim;
d. menyediakan sumber daya yang dibutuhkan untuk membentuk, memelihara, dan meningkatkan penerapan Keamanan Informasi SPBE secara berkelanjutan di Perangkat Daerah;
e. melakukan pemantauan dan pengendalian terhadap aktivitas penerapan Keamanan Informasi SPBE di Perangkat Daerah;
f. memberikan masukan terkait peningkatan kebijakan Manajemen Keamanan Informasi SPBE di Pemerintah Daerah;
g. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
h. berkoordinasi dengan ketua tim terkait penerapan Keamanan Informasi SPBE di Perangkat Daerah.

Bagian Keempat
Perencanaan

Pasal 9

(1) Perencanaan sebagaimana dimaksud dalam Pasal 4 huruf c ditetapkan oleh ketua tim pelaksana teknis Keamanan Informasi SPBE.
(2) Perencanaan sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. program kerja Keamanan Informasi SPBE; dan
    b. target realisasi program kerja Keamanan Informasi SPBE.
(3) Dalam merumuskan perencanaan Keamanan Informasi, Dinas berkoordinasi dengan Perangkat Daerah yang menyelenggarakan Urusan Pemerintahan bidang perencanaan pembangunan daerah.

Pasal 10

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

Pasal 11

(1) Penilaian kerentanan Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf a dilaksanakan paling sedikit melalui:
    a. menginventarisasi seluruh aset SPBE;
    b. mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
    c. mengukur tingkat risiko Keamanan SPBE.
(2) Peningkatan Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf b dapat dilaksanakan paling sedikit dengan:
    a. menerapkan standar teknis dan prosedur Keamanan SPBE; dan
    b. menguji fungsi keamanan terhadap aplikasi dan infrastruktur SPBE.
(3) Penanganan insiden Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf c dilaksanakan paling sedikit dengan:
    a. mengidentifikasi sumber serangan;
    b. menganalisis informasi yang berkaitan dengan insiden;
    c. memprioritaskan penanganan insiden;
    d. mendokumentasikan bukti insiden; dan
    e. mengurangi dampak risiko Keamanan Informasi SPBE.

(4) Edukasi kesadaran Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf d dilaksanakan paling sedikit melalui kegiatan:
a. sosialisasi; atau
b. literasi digital.

(5) Audit Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 10 ayat (1) huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima
Dukungan Pengoperasian

Pasal 12

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 4 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; dan
c. anggaran Keamanan Informasi SPBE.

(3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan Manajemen Keamanan Informasi SPBE diberikan alokasi sumber daya yang mencukupi.

Pasal 13

(1) Sumber daya manusia Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a harus memiliki kompetensi:
a. keamanan infrastruktur teknologi, informasi, dan komunikasi; dan
b. keamanan aplikasi.

(2) Kompetensi sebagaimana dimaksud pada ayat (1) diperoleh melalui pengembangan kompetensi paling sedikit dengan kegiatan:
a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi dan keamanan aplikasi; dan/atau
b. bimbingan teknis mengenai standar dan prosedur Keamanan Informasi SPBE.

(3) Teknologi Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b disediakan sesuai dengan kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

(4) Anggaran Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c disusun sesuai dengan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Keenam
Evaluasi Kinerja

Pasal 14

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 4 huruf e dilakukan oleh Koordinator SPBE.

(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan dengan:
   a. analisis efektivitas pelaksanaan Keamanan Informasi SPBE; atau
   b. mendukung dan merelealisasikan program audit Keamanan Informasi SPBE.
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Bagian Ketujuh
Perbaikan berkelanjutan terhadap Keamanan Informasi

Pasal 15

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 4 huruf f dilakukan oleh Perangkat Daerah sebagai tindak lanjut dari hasil evaluasi kinerja.
(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
   a. mengatasi permasalahan dalam pelaksanaan Keamanan Informasi SPBE;
   b. memperbaiki pelaksanaan Keamanan Informasi SPBE secara periodik; dan
   c. tindak lanjut hasil audit Keamanan Informasi SPBE.
(3) Hasil dari tindakan perbaikan dan peningkatan sebagaimana dimaksud ayat (3) dilaporkan kepada ketua tim pelaksana teknis Keamanan Informasi SPBE dan didokumentasikan.

BAB III
PENGENDALIAN TEKNIS KEAMANAN INFORMASI SPBE

Bagian Kesatu
Umum

Pasal 16

Pengendalian teknis Keamanan sebagaimana dimaksud dalam Pasal 3 huruf b meliputi:
a. manajemen risiko;
b. penetapan prosedur pengendalian Keamanan Informasi SPBE; dan
c. pengelolaan pihak ketiga.

Bagian Kedua
Manajemen Risiko

Pasal 17

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 16 huruf a harus dilakukan oleh setiap Perangkat Daerah.
(2) Manajemen risiko sebagaimana dimaksud pada ayat (1) dilakukan paling sedikit dengan menyusun daftar risiko.
(3) Daftar risiko sebagaimana dimaksud pada ayat (2) disusun dengan tahapan:
   a. identifikasi/inventarisasi aset SPBE;
   b. identifikasi ancaman dan kerentanan keamanan;

c. penilaian risiko keamanan;
d. penentuan prioritas risiko;
e. evaluasi risiko untuk analisis dampak;
f. analisis pengendalian/kontrol keamanan yang dapat diterapkan; dan
g. menetapkan rekomendasi kontrol keamanan.

(4) Prosedur manajemen risiko dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Ketiga
Penetapan Prosedur Pengendalian Keamanan Informasi SPBE

Pasal 18

(1) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 16 huruf b dilakukan oleh ketua tim pelaksana teknis Keamanan Informasi SPBE.
(2) Prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) dapat meliputi:
a. keamanan perangkat TIK;
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. pernyaratan keamanan terkait pembangunan dan pengembangan Aplikasi SPBE;
j. pengelolaan aset;
k. Keamanan migrasi data;
l. konfigurasi perangkat keamanan TIK;
m. perlindungan data pribadi;
n. keamanan komunikasi;
o. keamanan dalam proses akuisisi, pengembangan, dan pemeliharaan sistem informasi;
p. penerapan kriptografi;
q. pengelolaan insiden keamanan informasi;
r. kelangsungan bisnis atau layanan TIK;
s. perencanaan pemulihan bisnis atau layanan TIK pascabencana;
t. audit internal keamanan informasi SPBE; dan/atau
u. aspek prosedur pengendalian keamanan informasi SPBE lainnya.

(3) Prosedur pengendalian Keamanan Informasi sebagaimana dimaksud pada ayat (2) ditetapkan dengan Keputusan Sekretaris Daerah selaku Koordinator SPBE.

Pasal 19

(1) Prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 18 ayat (3) harus dilaksanakan oleh setiap Perangkat Daerah.
(2) Setiap Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian Keamanan Informasi SPBE.

Bagian Keempat
Pengelolaan Pihak Ketiga

Pasal 20

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 16 huruf c dilaksanakan oleh setiap Perangkat Daerah.
(2) Pengelolaan pihak ketiga sebagaimana dimaksud pada ayat (1) dilaksanakan sedikitnya melalui:
    a. memastikan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan Informasi SPBE yang telah ditetapkan;
    b. memastikan pihak ketiga memberikan akses sepenuhnya terhadap pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya;
    c. menerapkan proses, prosedur, atau rencana terdokumentasi untuk memantau layanan dan aspek Keamanan Informasi dalam hubungan kerja sama dengan pihak ketiga; dan
    d. membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
DUKUNGAN OPERASIONAL PENYELENGGARAAN MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu
Keamanan Informasi

Pasal 21

(1) Dalam penyelenggaraan operasional manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah, Dinas dapat melakukan koordinasi dan/atau konsultasi dengan BSSN, maupun kementerian atau instansi terkait.
(2) Dalam hal terjadi insiden Keamanan Informasi yang berdampak sangat luas, ketua tim dapat menunjuk auditor independen untuk melakukan investigasi yang diperlukan.

(3) Perangkat Daerah menyediakan akses kepada auditor independen sebagaimana dimaksud pada ayat (2) untuk melakukan audit terhadap seluruh aspek penyelenggaraan teknologi informasi.

Bagian Kedua
Pemantauan dan Pembinaan

Pasal 22

Perangkat Daerah melakukan pemantauan dan tindakan korektif atas penyimpangan terhadap Manajemen Keamanan Informasi SPBE meliputi:
a. kegiatan pemantauan secara terus menerus; dan
b. pelaksanaan fungsi pemeriksaan intern yang efektif dan menyeluruh.

Pasal 23

(1) Pembinaan dan pengawasan teknis terhadap penyelenggaraan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah dilakukan oleh Koordinator SPBE.
(2) Pembinaan dan pengawasan teknis terhadap penyelenggaraan Manajemen Keamanan Informasi SPBE dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Ketiga
Pendanaan

Pasal 24

Pendanaan penyelenggaraan Manajemen Keamanan Informasi SPBE 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 V
KETENTUAN PENUTUP

Pasal 25

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 Magelang.

Ditetapkan di Magelang
pada tanggal

WALI KOTA MAGELANG.

MUCHAMAD NUR AZIZ

Diundangkan di Magelang
pada tanggal

SEKRETARIS DAERAH KOTA MAGELANG,

HAMZAH KHOLIFI

BERITA DAERAH MAGELANG TAHUN NOMOR