BUPATI MAGELANG
PROVINSI JAWA TENGAH

PERATURAN BUPATI MAGELANG
NOMOR 24 TAHUN 2024

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MAGELANG,

Menimbang : a. bahwa pengembangan sistem pemerintahan berbasis elektronik diarahkan untuk meningkatkan efisiensi dan transparansi dalam penyelenggaraan pemerintahan dan pembangunan serta pelayanan publik yang berkualitas dan terpercaya guna mewujudkan kesejahteraan Masyarakat berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

b. bahwa penyelenggaraan pemerintahan berbasis elektronik yang aman di Daerah dilaksanakan dengan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan, dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;

c. bahwa berdasarkan ketentuan Pasal 41 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik dan Pasal 17 ayat (1) 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, setiap Instansi Pusat dan Pemerintah Daerah harus menerapkan Keamanan Sistem Pemerintahan Berbasis Elektronik;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c perlu menetapkan Peraturan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Djawa Tengah sebagaimana telah diubah dengan Undang-Undang Nomor 9 Tahun 1965 tentang Pembentukan Daerah Tingkat II Batang dengan mengubah Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Djawa Tengah (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 52, Tambahan Lembaran Negara Republik Indonesia Nomor 2757);

3. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
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 beberapa kali diubah 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);
6. Undang-Undang Nomor 11 Tahun 2023 tentang Provinsi Jawa Tengah (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 6867);
7. 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);
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
10. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
11. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
12. Peraturan Bupati Magelang Nomor 26 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kabupaten Magelang (Berita Daerah Kabupaten Magelang Tahun 2021 Nomor 26);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Magelang.
2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Magelang.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Magelang.
5. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
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 maupun non elektronik.
7. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
8. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan Informasi.
9. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
10. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE
11. Keamanan Informasi SPBE adalah penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan sumber daya terkait data dan informasi, infrastruktur SPBE, dan Aplikasi SPBE.
12. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
13. 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 integrase/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.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal dalam pengelolaan Keamanan Informasi SPBE secara terpadu di lingkungan Pemerintah Daerah.

(2) Peraturan Bupati 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 Bupati ini meliputi:
a. penerapan Manajemen Keamanan Informasi SPBE;
b. pengendalian teknis Keamanan Informasi SPBE; dan
c. dukungan operasional penyelenggaraan Manajemen Keamanan Informasi SPBE.

BAB II
PENERAPAN MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu
Umum

Pasal 4

Ruang lingkup penerapan manajemen keamanan informasi SPBE sebagaimana dimaksud Pasal 3 huruf a meliputi:
a. penetapan cakupan;
b. penetapan penanggung jawab;
c. perencanaan;
d. dukungan pengoperasian;
e. evaluasi kinerja; dan
f. perbaikan berkelanjutan terhadap keamanan informasi

Bagian Kedua
Penetapan

Pasal 5

(1) Penetapan cakupan manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 4 huruf a meliputi:
    a. data informasi SPBE;
    b. apikasi SPBE; dan
    c. infrastruktur SPBE.
(2) Penetapan cakupan sebagaimana dimaksud pada ayat (1) merupakan aset Daerah yang harus diamanakan dalam SPBE.

Bagian Ketiga
Penetapan Penanggung Jawab

Pasal 6

(1) Bupati menetapkan penanggung jawab manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b.
(2) Penanggung jawab manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
(3) Dalam melaksanakan tugas sebagai penanggung jawab manajemen Keamanan Informasi SPBE, Sekretaris Daerah disebut sebagai koordinator SPBE.

Pasal 7

(1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen Keamanan Informasi SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) membentuk tim manajemen Keamanan Informasi SPBE yang ditetapkan melalui keputusan.

(2) Tim manajemen 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 dapat dijabat oleh Kepala Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

(4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh Kepala Perangkat Daerah lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di Daerah.

Pasal 8

(1) Ketua tim sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen Keamanan Informasi SPBE meliputi:
   a. menetapkan standar operasional 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, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Informasi SPBE;
   e. memutuskan, merancang, melaksanakan dan mengelola langkah keberlangsungan proses bisnis TIK dalam bentuk dokumen rencana kelangsungan bisnis/*business continuity plans* dan dokumen rencana pemulihan pasca bencana *disaster recovery plans*; dan
   f. melaporkan pelaksanaan manajemen Keamanan Informasi SPBE pada koordinator SPBE.

(2) Anggota tim sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf b mempunyai tugas:
   a. mengkoordinasikan 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. menyediakan sumber daya yang dibutuhkan untuk membentuk, memelihara, dan meningkatkan penerapan Keamanan Informasi SPBE secara berkelanjutan pada Perangkat Daerah; dan
   d. melakukan pemantauan dan pengendalian terhadap aktifitas penerapan Keamanan Informasi SPBE di Perangkat Daerah;
   e. memberikan masukan terkait peningkatan kebijakan Manajemen Keamanan Informasi SPBE di Pemerintah Daerah;

f. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
g. berkoordinasi dengan ketua tim terkait perumusan program dan anggaran keamanan Informasi SPBE.

Bagian Keempat
Penetapan Perencanaan

Pasal 9

(1) Perencanaan sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf c ditetapkan oleh ketua tim manajemen Keamanan Informasi SPBE.
(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
    a. program kerja Keamanan Informasi SPBE; dan
    b. target realisasi program kerja Keamanan Informasi SPBE.

Pasal 10

(1) Program kerja Keamanan Informasi SPBE sebagaimana dimaksud pada 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; dan
    d. edukasi kesadaran Keamanan Informasi SPBE;
    e. audit Keamanan Informasi SPBE.
(2) Target realisasi program kerja Keamanan Informasi SPBE sebagaimana dimaksud pada 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. menginventasisasi 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. pelatihan.
(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 ayat (1) 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 12 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 Informasi 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 Informasi SPBE.

(4) Teknologi keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf b disediakan sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

(3) Anggaran Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Keenam
Evaluasi Kinerja

Pasal 14

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

(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen keamanan informasi SPBE di Daerah.

(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
   a. mengidentifiasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan keamanan SPBE;
   b. menetapkan indikator kinerja pada setiap area proses;
   c. memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
   d. menganalisis efektifitas pelaksanaan Keamanan SPBE; atau

e. 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.

Bagian Ketujuh
Perbaikan berkelanjutan terhadap Keamanan Informasi

Pasal 15

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf f dilakukan oleh Tim manajemen Keamanan Informasi SPBE.
(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.
(3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
   a. mengatasi permasalahan dalam pelaksanaan Keamanan Informasi SPBE;
   b. memperbaiki pelaksanaan Keamanan Informasi SPBE secara periodik; dan
   c. tindak lanjut hasil audit Keamanan Informasi SPBE.

BAB III
PENGENDALIAN TEKNIS KEAMANAN

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
Manajeman Risiko

Pasal 17

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 16 huruf a harus
(2) Prosedur manajemen risiko dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Ketiga
Penetapan Prosedur Pengendalian Keamanan Informasi SPBE

Pasal 18

(1) Ketua Tim manajemen Keamanan Informasi SPBE menyusun prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada Pasal 16 huruf b.
(2) Prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen Keamanan Informasi SPBE di Daerah dengan cangkupan 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. persayaratan 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;
t. perencanaan pemulihan bisnis atau layanan TIK pascabencana;
u. audit internal keamanan informasi SPBE; dan/atau
v. aspek prosedur pengendalian keamanan informasi SPBE lainnya.

(3) Prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) ditetapkan oleh Sekretaris Daerah selaku Koordinator SPBE.

Pasal 19

(1) Prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 18 ayat (3) 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 dilakukan oleh setiap perangkat daerah yang menggunakan jasa atau layanan pihak ketiga.

(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 SPBE yang telah ditetapkan;
b. memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya;
c. menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama 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, Perangkat Daerah dapat melakukan koordinasi dan/atau konsultasi dengan Pemerintah Provinsi Jawa Tengah, BSSN, maupun kementerian atau instansi terkait melalui ketua tim manajemen Keamanan Informasi SPBE.

(2) Dalam hal terjadi insiden Keamanan Informasi, Perangkat Daerah harus segera melapor kepada tim yang berwenang menangani insiden keamanan informasi.

(3) Dalam hal terjadi insiden Keamanan Informasi yang berdampak sangat luas, ketua tim manajemen Keamanan Informasi SPBE dapat menunjuk auditor independen untuk melakukan investigasi yang diperlukan.

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

Bagian Kedua
Pemantauan dan Pembinaan

Pasal 22

Perangkat Daerah harus 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 dilakukan oleh Koordinator SPBE.

(2) Pembinaan dan pengawasan teknis terhadap penyelenggaraan manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) 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
b. sumber pendanaan lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB V
KETENTUAN PENUTUP

Pasal 25

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Kota Mungkid
pada tanggal 3 Desember 2024

Pj. BUPATI MAGELANG,

ttd

SEPYO ACHANTO

Diundangkan di Kota Mungkid
pada tanggal 3 Desember 2024

SEKRETARIS DAERAH KABUPATEN MAGELANG,

ttd

ADI WARYANTO

BERITA DAERAH KABUPATEN MAGELANG TAHUN 2024 NOMOR 25

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

RATNA YULIANTY, S.H., M.H.
Pembina Tingkat I
NIP. 196807301997032003