S A L I N A N

BUPATI PONOROGO
PROVINSI JAWA TIMUR

PERATURAN BUPATI PONOROGO
NOMOR 80 TAHUN 2024

TENTANG

PEDOMAN PELAKSANAAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI PONOROGO,

Menimbang :

a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Kabupaten Ponorogo, perlu melaksanakan manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;

b. bahwa berdasarkan ketentuan Pasal 2 Peraturan Gubernur Jawa Timur Nomor 95 Tahun 2023 tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik, maka perlu menetapkan Peraturan Bupati tentang Pedoman Pelaksanaan Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

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

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia;

2. Undang-Undang Nomor 12 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Jawa Timur (Lembaran Negara Republik Indonesia Tahun 1950 Nomor 19, Tambahan Lembaran Negara Republik Indonesia Nomor 9) sebagaimana telah diubah dengan Undang-Undang Nomor 2 Tahun 1965 tentang Perubahan Batas Wilayah Kotapraja Surabaya dan Dati II Surabaya dengan mengubah Undang-Undang Nomor 12 tahun 1950 tentang Pembentukan Daerah-daerah Kabupaten dalam lingkungan Propinsi Jawa Timur dan Undang-Undang 16 Tahun 1950 tentang Pembentukan Daerah-Daerah Kota Besar dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, Jawa Barat dan DI. Yogyakarta (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);

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 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);
5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
6. 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);
7. Peraturan Gubernur Jawa Timur Nomor 95 tahun 2023 tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;
8. Peraturan Daerah Kabupaten Ponorogo 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Ponorogo Tahun 2016 Nomor 6) sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Ponorogo Nomor 4 Tahun 2019 tentang Perubahan atas Peraturan Daerah Kabupaten Ponorogo 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Ponorogo Tahun 2019 Nomor 4);
9. Peraturan Bupati Ponorogo Nomor 71 Tahun 2023 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Ponorogo (Berita Daerah Kabupaten Ponorogo Tahun 2019 Nomor 56)

MEMUTUSKAN :

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

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Ponorogo.
2. Pemerintah Daerah adalah Pemerintah Kabupaten Ponorogo.
3. Bupati adalah Bupati Ponorogo.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Ponorogo.
5. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Kepala Daerah dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan daerah.
6. Dinas adalah Dinas Komunikasi Informatika dan Statistik Kabupaten Ponorogo
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
8. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
9. Keamanan Informasi adalah suatu kondisi untuk melindungi aset yang dimiliki organisasi dari berbagai ancaman pihak internal maupun eksternal untuk menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, serta terjaganya aspek kerahasiaan, keutuhan dan ketersediaan dari informasi.
10. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
11. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasian atas informasi dan komunikasi secara Elektronik.
12. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan atas Informasi Elektronik.
13. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan atas Informasi Elektronik.
14. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
15. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
16. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.

17. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.
18. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat Elektronik lainnya
19. *Application Programming Interface* yang selanjutnya disingkat API adalah sekumpulan perintah, fungsi, serta protokol yang mengintegrasikan dua bagian dari aplikasi atau dengan aplikasi yang berbeda secara bersamaan.
20. Pihak ketiga adalah semua pihak atau pihak lain selain Pemerintah Daerah, yang memiliki hubungan kontrak dengan Pemerintah Daerah untuk membangun dan mengembangkan aplikasi.

Pasal 2

Peraturan Bupati ini dimaksudkan sebagai acuan dalam melaksanakan manajemen keamanan informasi SPBE di lingkungan Pemerintah Kabupaten Ponorogo.

Pasal 3

Peraturan Bupati ini bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak resiko keamanan informasi.

BAB II
RUANG LINGKUP

Pasal 4

Ruang lingkup Peraturan Bupati ini meliputi:

a. pedoman manajemen keamanan informasi SPBE;
b. standard teknis dan prosedur keamanan SPBE;
c. manajemen resiko keamanan informasi SPBE; dan
d. pengelolaan pihak ketiga.

BAB III
PEDOMAN MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 5

(1) Pedoman manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 4 meliputi :
    a. penetapan ruang lingkup;
    b. penetapan penanggung jawab;
    c. perencanaan;
    d. dukungan pengoperasian;
    e. evaluasi kinerja; dan
    f. perbaikan berkelanjutan terhadap keamanan informasi.

(2) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) huruf a meliputi:
   a. data dan informasi SPBE;
   b. aplikasi SPBE;
   c. infrastruktur SPBE; dan
   d. kebijakan keamanan informasi SPBE yang telah dimiliki.

(3) Penetapan ruang lingkup sebagaimana dimaksud pada Ayat (2) merupakan aset Pemerintah Daerah yang harus diamankan dalam SPBE.

Pasal 6

(1) Bupati menetapkan penanggung jawab manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 5 ayat (3) huruf b.

(2) Penanggung jawab manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.

(3) Selain sebagai penanggung jawab sebagaimana dimaksud pada ayat (2), Sekertaris Daerah mempunyai tugas sebagai koordinator SPBE sesuai dengan ketentuan peraturan perundang – undangan.

(4) Dalam melaksanakan tugas sebagai penanggung jawab manajemen keamanan informasi SPBE, dan koordinator SPBE sebagaimana dimaksud dalam ayat (3) menetapkan pelaksana teknis Keamanan SPBE.

(5) Pelaksana teknis keamanan SPBE sebagaimana dimaksud pada ayat (4) terdiri atas :
   a. pimpinan perangkat daerah yang membidangi urusan Komunikasi dan Informatika di Pemerintah Daerah, sebagai ketua tim; dan
   b. seluruh pimpinan perangkat daerah yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Daerah, sebagai anggota tim.

(6) Ketua tim sebagaimana dimaksud pada ayat (5) mempunyai tugas:
   a. menetapkan prosedur pengendalian keamanan informasi SPBE;
   b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE
   c. memastikan penerapan standar teknis dan prosedur keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan.
   d. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran keamanan SPBE;

e. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen kelangsungan bisnis atau layanan TIK dan perencanaan pemulihan bencana terhadap layanan TIK; dan

f. melaporkan pelaksanaan manajemen keamanan informasi SPBE pada koordinator SPBE.

(7) Anggota tim sebagaimana dimaksud pada ayat (5) huruf b mempunyai tugas :

a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada perangkat daerah masing – masing;

b. memastikan penerapan keamanan aplikasi SPBE dan infrastruktur SPBE sesuai dengan standar teknis dan prosedur keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundangan-undangan;

c. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen kelangsungan bisnis atau layanan TIK dan perencanaan pemulihan bencana terhadap layanan TIK ; dan

d. berkoordinasi dengan ketua tim terkait penerapan keamanan aplikasi SPBE dan infrastruktur SPBE

Pasal 7

(1) Perencanaan sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf c ditetapkan oleh ketua tim pelaksana teknis keamanan SPBE.

(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan oleh pelaksana teknis keamanan SPBE, dengan merumuskan:

a. program kerja keamanan SPBE; dan

b. target realisasi program kerja keamanan SPBE.

(3) Program kerja keamanan SPBE sebagaimana dimaksud dalam ayat (2) huruf a paling sedikit meliputi:

a. edukasi kesadaran keamanan SPBE;

b. penilaian kerentanan keamanan SPBE;

c. peningkatan keamanan SPBE;

d. penanganan insiden keamanan SPBE; dan

e. audit keamanan SPBE.

(4) Target realisasi program kerja keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b ditetapkan berdasarkan kebutuhan Pemerintah Daerah dan ketentuan prioritas setiap tahunnya.

Pasal 8

Edukasi kesadaran keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf a dilaksanakan paling sedikit melalui kegiatan:

a. sosialisasi; dan

b. pelatihan.

Pasal 9

Penilaian kerentanan keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf b dilaksanakan paling sedikit melalui:

a. menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur;
b. mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
c. mengukur tingkat risiko keamanan SPBE.

Pasal 10

(1) Peningkatan keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan keamanan SPBE sebagaimana dimaksud dalam Pasal 9.

(2) Peningkatan keamanan SPBE dilaksanakan paling sedikit melalui:
    a. menerapkan standar teknis dan prosedur keamanan SPBE; dan
    b. menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 11

Penanganan insiden keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf d dilaksanakan paling sedikit melalui:

a. mengidentifikasi sumber serangan;
b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
d. mendokumentasi bukti insiden yang terjadi; dan
e. memitigasi atau mengurangi dampak risiko keamanan SPBE.

Pasal 12

Audit keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (3) huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 13

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 5 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 SPBE;
    b. teknologi keamanan SPBE; dan
    c. anggaran keamanan SPBE.

(3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen keamanan informasi SPBE diberikan alokasi sumber daya yang sesuai.

Pasal 14

(1) Sumber daya manusia keamanan SPBE sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf a dengan ketentuan harus memiliki kompetensi:
   a. keamanan infrastruktur TIK; dan
   b. keamanan aplikasi.

(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus adanya dukungan kegiatan:
   a. pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi dan TIK; dan/atau
   b. bimbingan teknis mengenai standar teknis dan prosedur keamanan SPBE.

(3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan keamanan SPBE.

(4) Teknologi keamanan informasi sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.

(5) Anggaran keamanan SPBE sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 15

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 5 Ayat (1) huruf e dilakukan oleh Koordinator SPBE.

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

(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
   a. mengidentifikasi 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) Dalam rangka pelaksanaan audit keamanan SPBE, Koordinator SPBE dapat melimpahkan kepada pimpinan perangkat daerah yang membidangi urusan pengawasan intern di lingkungan Pemerintah Daerah.

(5) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 16

(1) Perbaikan berkelanjutan terhadap keamanan informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf f dilakukan oleh pelaksana teknis keamanan SPBE.

(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.

(3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
   a. Mengatasi permasalahan dalam pelaksanaan keamanan SPBE; dan
   b. Memperbaiki pelaksanaan keamanan SPBE secara periodik.

BAB IV
STANDAR TEKNIS DAN PROSEDUR KEAMANAN
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Pasal 17

(1) Pemerintah Daerah dapat menerapkan keamanan SPBE.

(2) Penerapan keamanan SPBE sebagaimana dimaksud pada ayat (1) harus memenuhi standar teknis dan prosedur keamanan SPBE.

Pasal 18

Standar teknis dan prosedur keamanan SPBE sebagaimana dimaksud dalam Pasal 17 ayat (2) diterapkan untuk:

a. keamanan data dan informasi;
b. keamanan Aplikasi SPBE;
c. keamanan Sistem Penghubung Layanan Pemerintah Daerah; dan
d. keamanan Jaringan Intra Pemerintah Daerah.

Pasal 19

(1) Standar teknis keamanan data dan informasi sebagaimana dimaksud dalam Pasal 18 huruf a terdiri atas terpenuhinya aspek:
   a. kerahasiaan;
   b. keaslian;
   c. keutuhan;
   d. kenirsangkalan; dan
   e. ketersediaan.

(2) Ketentuan lebih lanjut mengenai aspek keamanan data dan informasi dilaksanakan sesuai peraturan perundang-undangan.

Pasal 20

(1) Standar teknis dan prosedur keamanan Aplikasi SPBE sebagaimana dimaksud dalam Pasal 17 ayat (2) diterapkan pada:

a. aplikasi berbasis web; dan
b. aplikasi berbasis mobile.

(2) Aplikasi berbasis web sebagaimana dimaksud pada ayat (1) huruf a merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet.

(3) Aplikasi berbasis mobile sebagaimana dimaksud pada ayat (1) huruf b merupakan aplikasi yang dalam pengoperasiannya dapat berjalan di perangkat bergerak, dan memiliki sistem operasi yang mendukung perangkat lunak secara *standalone*.

(4) Aplikasi SPBE sebagaimana dimaksud pada ayat (1) harus dilakukan pengujian keamanan setiap periode tertentu yang dilakukan dengan:
a. mengidentifikasi persyaratan minimum keamanan yang belum diterapkan;
b. memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan;
c. melakukan pemindaian otomatis dan/atau pengujian penetrasi sistem;
d. mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan Aplikasi SPBE; dan
e. menganalisis kerentanan.

Pasal 21

(1) Standar teknis keamanan aplikasi berbasis web sebagaimana dimaksud dalam Pasal 20 ayat (1) huruf a terdiri atas terpenuhinya fungsi:
a. autentikasi;
b. manajemen sesi;
c. persyaratan kontrol akses;
d. validasi input;
e. kriptografi pada verifikasi statis;
f. penanganan *eror* dan pencatatan log;
g. proteksi data;
h. keamanan komunikasi;
i. pengendalian kode berbahaya;
j. logika bisnis;
k. *file*;
l. keamanan API dan *web service*; dan
m. keamanan konfigurasi.

(2) Ketentuan lebih lanjut mengenai aspek keamanan aplikasi berbasis web dilaksanakan sesuai ketentuan peraturan perundang-undangan.

Pasal 22

(1) Standar teknis keamanan aplikasi berbasis *mobile* sebagaimana dimaksud dalam Pasal 20 ayat (1) huruf b terdiri atas terpenuhinya fungsi:
a. penyimpanan data dan persyaratan privasi;
b. kriptografi;

c. autentikasi dan manajemen sesi;
d. komunikasi jaringan;
e. interaksi platform;
f. kualitas kode dan pengaturan build; dan
g. ketahanan.

(2) Ketentuan lebih lanjut mengenai aspek keamanan aplikasi berbasis *mobile* dilaksanakan sesuai peraturan perundang-undangan.

Pasal 23

(1) Standar teknis keamanan Sistem Penghubung Layanan Pemerintah Daerah sebagaimana dimaksud dalam Pasal 18 huruf c terdiri atas terpenuhinya fungsi:
a. keamanan interoperabilitas data dan informasi;
b. kontrol sistem integrasi;
c. kontrol perangkat *integrator*;
d. keamanan API dan *web service*; dan
e. keamanan migrasi data.

(2) Ketentuan lebih lanjut mengenai aspek keamanan Sistem Penghubung Layanan Pemerintah Daerah dilaksanakan sesuai peraturan perundang-undangan.

Pasal 24

(1) Standar teknis keamanan Jaringan Intra Pemerintah Daerah sebagaimana dimaksud pada Pasal 18 huruf d terdiri atas terpenuhinya:
a. aspek administrasi keamanan Jaringan Intra;
b. kontrol akses dan autentikasi;
c. persyaratan perangkat dan aplikasi keamanan Jaringan Intra;
d. kontrol keamanan *gateway*;
e. kontrol keamanan *access point* pada jaringan nirkabel; dan
f. kontrol konfigurasi *access point* pada jaringan nirkabel.

(2) Ketentuan lebih lanjut mengenai aspek keamanan Jaringan Intra Pemerintah Daerah dilaksanakan sesuai peraturan perundang-undangan.

BAB V
MANAJEMEN RESIKO KEAMANAN INFORMASI SPBE

Pasal 25

(1) Manajemen risiko keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 4 huruf c dilakukan oleh setiap Perangkat Daerah.

(2) Manajemen risiko keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko dengan ketentuan substansi meliputi:
a. inventarisasi aset SPBE;

b. identifikasi ancaman dan kerentanan keamanan terhadap aset SPBE;
c. penilaian risiko keamanan terhadap aset SPBE;
d. penentuan prioritas risiko;
e. analisa dampak jika terjadi risiko;
f. analisa kontrol keamanan yang bisa diterapkan; dan/atau
g. rekomendasi kontrol keamanan.

(3) Prosedur pelaksanaan manajemen risiko keamanan informasi SPBE dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI
PENGELOLAAN PIHAK KETIGA

Pasal 26

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 4 huruf d dilakukan oleh setiap Perangkat Daerah

(2) Perangkat Daerah sebagaimana dimaksud pada ayat (1) dapat memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga :
a. memenuhi standar teknis dan prosedur keamanan SPBE yang telah ditetapkan;
b. memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.

(3) Perangkat Daerah dapat menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerja sama dengan pihak ketiga.

(4) Perangkat Daerah dapat membuat laporan secara berkala tentang pencapaian Sasaran Tingkat Layanan dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB VII
KETENTUAN PENUTUP

Pasal 27

Peraturan Bupati ini berlaku pada saat diundangkan.

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

Ditetapkan di Ponorogo
pada tanggal 19 Agustus 2024
BUPATI PONOROGO,
TTD.
SUGIRI SANCOKO

Diundangkan di Ponorogo
pada tanggal 19-08-2024

SEKRETARIS DAERAH
KABUPATEN PONOROGO,

TTD.

AGUS PRAMONO

BERITA DAERAH KABUPATEN PONOROGO TAHUN 2024 NOMOR 80.

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM
SEKRETARIAT DAERAH

SOEGENG PRAKOSO, S.H., M.H.
NIP. 19680605 199303 1 003