S A L I N A N

BUPATI PONOROGO
PROVINSI JAWA TIMUR

PERATURAN BUPATI PONOROGO
NOMOR 70 TAHUN 2024

TENTANG

PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

BUPATI PONOROGO,

Menimbang : a. bahwa persandian merupakan urusan Pemerintah Daerah yang penting untuk menjaga keamanan dan kerahasaian data dan informasi;

b. bahwa berdasarkan ketentuan Pasal 4 ayat (2) Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, Bupati sesuai dengan kewenangannya bertanggung jawab terhadap Penyelenggaraan Persandian untuk Pengamanan Informasi;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Pelaksanaan Persandian untuk Pengamanan Informasi;

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 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. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
7. 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);
8. Peraturan Daerah Kabupaten Ponorogo Nomor 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Ponorogo Tahun 2016 Nomor 6) sebagaimana telah beberapa kali diubah, terakhir dengan Peraturan Daerah Nomor 1 Tahun 2023 tentang Perubahan Kedua atas Peraturan Daerah Kabupaten Ponorogo Nomor 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Ponorogo Tahun 2023 Nomor 1)

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG PEDOMAN PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

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. Dinas adalah Dinas Komunikasi, Informasi dan Statistik Kabupaten Ponorogo.
5. Aparatur Sipil Negara adalah Pegawai Aparatur Sipil Negara yang bekerja di Lingkup Pemerintah Kabupaten Ponorogo.
6. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Bupati dalam penyelenggaraan urusan Pemerintahan yang menjadi kewenangan daerah.
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. Keamanan informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan informasi.
9. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
10. Sistem elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
11. 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.
12. Pola Hubungan Komunikasi Sandi adalah keterhubungan antar pengguna persandian melalui jaringan komunikasi.
13. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta otentifikasi data.
14. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan urusan Pemerintahan bidang Persandian dan yang memiliki manfaat.
15. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
16. Badan Siber dan Sandi Negara yang selanjutnya disebut BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan dibidang keamanan siber dan persandian.
17. Otoritas Sertifikat Digital Badan Siber dan Sandi Negara yang selanjutnya disebut OSD BSSN adalah sistem elektronik yang berfungsi sebagai Layanan Sertifikat Elektronik di Badan Siber dan Sandi Negara.
18. Balai Sertifikasi Elektronik merupakan unit pelaksana teknis penyelenggara OSD BSSN yang berada di bawah dan bertanggung jawab kepada Kepala Badan Siber dan Sandi Negara.

Pasal 2

Peraturan Bupati ini dimaksudkan sebagai pedoman bagi Pemerintah Daerah dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan persandian untuk pengamanan informasi.

Pasal 3

Peraturan Bupati ini bertujuan :

a. menciptakan harmonisasi dalam melaksanakan persandian untuk pengamanan informasi.
b. meningkatkan komitmen, efektivitas, dan kinerja PD dalam melaksanakan program dan kegiatan pelaksanaan persandian untuk pengamanan informasi; dan
c. memberikan pedoman bagi Pemerintah Daerah dalam menetapkan pola hubungan komunikasi sandi antar PD.

BAB II
RUANG LINGKUP

Pasal 4

Ruang Lingkup Peraturan Bupati ini meliputi :

a. Penyelenggaraan Persandian untuk Pengamanan Informasi.
b. Penetapan Pola Hubungan Komunikasi Sandi.
c. Operasional Dukungan Persandian Untuk Pengamanan Informasi.

BAB III
PENYELENGGARAAN PERSANDIAN
UNTUK PENGAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 5

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;
d. penyedia Layanan Keamanan Informasi;
e. penyediaan kebutuhan penyelenggaraan persandian untuk pengamanan informasi melalui identifikasi dan analisis pola hubungan komunikasi sandi;
f. penyelenggaraan operasional dukungan persandian untuk pengamanan informasi;
g. pemanfaatan layanan sertifikat elektronik;

h. pengawasan dan evaluasi penyelenggaraan pengamanan informasi melalui persandian di seluruh PD; dan

i. koordinasi dan konsultasi penyelenggaraan persandian untuk pengamanan informasi.

Pasal 6

(1) Bupati sesuai dengan kewenangannya bertanggung jawab terhadap Penyelenggaraan Persandian untuk Pengamanan Informasi.

(2) Bupati dalam melaksanakan tangggung jawabnya dibantu oleh Dinas.

Pasal 7

(1) Dinas menyusun perencanaan penyelenggaraan Persandian.

(2) Perencanaan penyelenggaraan Persandian sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam Perencanaan Pembangunan Daerah.

(3) Perencanaan Pembangunan Daerah sebagaimana dimaksud pada ayat (2) merupakan bagian integral dari sistem perencanaan pembangunan nasional dan dituangkan dalam dokumen Perencanaan Pembangunan Daerah.

(4) Dokumen Perencanaan Pembangunan Daerah sebagaimana dimaksud pada ayat (3) berupa :

a. Rencana Pembangunan Jangka Panjang Daerah;

b. Rencana Pembangunan Jangka Menengah Daerah; dan

c. Rencana Kerja Pemerintah Daerah.

Pasal 8

(1) Dalam rangka menjabarkan Rencana Pembangunan Jangka Menengah Daerah sebagaimana dimaksud dalam Pasal 7 ayat (4) huruf b, Dinas menyusun Rencana Strategis PD yang memuat tujuan, sasaran, program, dan kegiatan penyelenggaraan Persandian untuk pengamanan informasi.

(2) Dalam rangka menjabarkan Rencana Kerja Pemerintah Daerah sebagaimana dimaksud dalam Pasal 6 ayat (4) huruf c, Dinas menyusun Rencana Kerja Perangkat Daerah yang memuat program, kegiatan, lokasi, dan kelompok sasaran berdasarkan layanan urusan pemerintah bidang Pe rsandian, disertai indikator kinerja program dan kegiatan, serta penganggaran penyelenggaraan Persandian untuk pengamanan informasi.

Bagian Kedua
Penyusunan Kebijakan Pengamanan Informasi

Pasal 9

Penyusunan Kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf a, dilakukan dengan:

a. menyusun Rencana Strategis Pengamanan Informasi;

b. menetapkan Arsitektur Keamanan Informasi; dan
c. menetapkan aturan mengenai Tata Kelola Keamanan Informasi.

Pasal 10

(1) Rencana Strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf a, disusun oleh Bupati.
(2) Dalam melakukan penyusunan Rencana Strategis sebagaimana dimaksud pada ayat (1), Bupati dapat melakukan koordinasi dan konsultasi BSSN.
(3) Dalam melaksanakan penyusunan Rencana Strategis Bupati dapat menunjuk Dinas.
(4) Dinas dapat melakukan koordinasi dan konsultasi dengan BSSN.

Pasal 11

(1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf b, ditetapkan oleh Bupati.
(2) Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) memuat:
    a. Infrastruktur teknologi informasi;
    b. Desain keamanan perangkat teknologi informasi dan keamanan jaringan; dan
    c. Aplikasi keamanan perangkat teknologi informasi dan keamanan jaringan.
(3) Dalam melakukan penyusunan arsitektur keamanan jaringan informasi, Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.
(4) Arsitektur Keamanan Informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.
(5) Arsitektur Keamanan Informasi dilakukan evaluasi oleh Bupati pada paruh waktu dan tahun terakhir atau sewaktu-waktu sesuai dengan kebutuhan.

Pasal 12

(1) Aturan mengenai Tata Kelola Keamanan Informasi dalam Pasal 9 huruf c ditetapkan oleh Bupati.
(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) Dalam melakukan penyusunan aturan mengenai Tata Kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1), Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.

Pasal 13

(1) Dinas dapat melaksanakan pengelolaan sumber daya keamanan informasi.

(2) Pengelolaan sumber daya keamanan informasi sebagaimana dimaksud pada ayat (1), terdiri dari:
a. pengelolaan aset keamanan teknologi informasi dan komunikasi;
b. pengelolaan sumber daya manusia; dan
c. manajemen pengetahuan.

Pasal 14

(1) Pengelolaan Aset Keamanan Teknologi Informasi dan Komunikasi dilaksanakan oleh Pemerintah Daerah, melalui:
a. perencanaan kebutuhan;
b. pengadaan;
c. pemanfaatan dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan; dan
d. pengawasan dan pengendalian.

(2) Aset Keamanan Teknologi Informasi dan Komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi, dan/atau memulihkan insiden Keamanan Informasi dalam Sistem Elektronik.

Pasal 15

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf b dilakukan oleh PD.

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

(3) Pengembangan kompetensi sebagaimana dimaksud pada ayat (2) huruf a dapat dilakukan melalui berbagai kegiatan pengembangan kompetensi di bidang Keamanan Informasi, termasuk pelatihan teknis dan pendidikan formal atau informal.

(4) Pembinaan karir sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan dengan menyediakan peluang untuk pengembangan jabatan fungsional di bidang keamanan informasi dan pengisian jabatan struktural sesuai dengan standar kompetensi yang ditetapkan.

(5) Pendayagunaan sebagaimana yang dimaksud pada ayat (2) huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di bidang keamanan informasi dapat bekerja sesuai dengan standar kompetensi pegawai yang ditetapkan.

Pasal 16

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 15 ayat (1) dilakukan melalui berbagai upaya, seperti pendidikan, pelatihan, bimbingan, dan kegiatan pengembangan kompetensi terkait dengan keamanan informasi dan teknologi.

(2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) bertujuan untuk meningkatkan kualitas dan keahlian dalam bidang persandian dan teknologi informasi.

(3) Dinas dapat melakukan pengelolaan sumber daya keamanan informasi.

Pasal 17

Sumber daya manusia yang tidak lagi menjalankan tugas pada Dinas harus disesuaikan kewenangannya, yaitu :

a. Pencabutan atau pemutusan hak akses terhadap informasi dan fasilitas informasi yang diamankan.
b. Pelaksanaan prosedur pengamanan (serah terima) materiil sandi.

Pasal 18

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf c dilakukan oleh Dinas.

(2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) bertujuan untuk meningkatkan kualitas layanan keamanan informasi dan mendukung proses pengambilan keputusan terkait keamanan informasi.

(3) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan keamanan informasi pemerintah daerah.

(4) Dalam pelaksanaan manajemen pengetahuan, Pemerintah Daerah dapat melakukan koordinasi dan konsultasi dengan BSSN.

Bagian Keempat
Pengamanan Sistem Elektronik
dan Pengamanan Informasi Nonelektronik

Pasal 19

Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik sebagaimana dimaksud dalam Pasal 5 huruf c, dilaksanakan oleh Dinas sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 20

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 19 terdiri atas:

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

Pasal 21

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 19, 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 melalui kegiatan mitigasi risiko dan penerapan perlindungan terhadap sistem elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintah 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 22

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 19, PD wajib 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 23

(1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 22 ayat (1), Dinas dapat menyelenggarakan Pusat Operasi Pengamanan Informasi sesuai standar yang ditetapkan oleh BSSN.

(2) Pusat Operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (1), bertujuan untuk pengamanan Sistem Elektronik dengan melakukan proses pengawasan, penanggulangan, dan pemulihan atas insiden keamanan Sistem Elektronik dengan memperhatikan aspek personel, proses pelaksanaan, dan ketersediaan teknologi.

Pasal 24

(1) Pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 19, 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 25

(1) PD yang memiliki fungsi pengawasan internal bertugas untuk melaksanakan audit Keamanan Informasi.

(2) Pelaksanaan Audit Keamanan Informasi sebagaimana dimaksud ayat (1), dapat melibatkan pegawai Aparatur Sipil Negara dari unit kerja lain yang memiliki kompetensi.

(3) Audit Keamanan Informasi meliputi audit keamanan Sistem Elektronik dan Audit Sistem Manajemen.

(4) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (3), dilaksanakan sesuai ketentuan peraturan perundang-undangan.

Pasal 26

(1) Penyediaan Layanan Keamanan informasi sebagaimana dimaksud dalam Pasal 5 huruf d, dilaksanakan oleh Dinas.

(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1), disediakan untuk Pengguna Layanan yang terdiri atas:
   a. Bupati dan Wakil Bupati;
   b. PD;
   c. Aparatur Sipil Negara; dan
   d. Pihak lainnya.

Pasal 27

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 25 ayat (1), meliputi:

a. identifikasi kerentanan dan penilaian risiko terhadap Sistem Elektronik;
b. asistensi dan fasilitasi penguatan keamanan Sistem Elektronik;
c. penerapan Sertifikasi 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 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 Kabupaten Ponorogo melalui teknik pengamanan gelombang frekuensi atau sinyal;
n. perlindungan informasi pada aset/fasilitas penting milik atau yang akan digunakan Pemerintah Kabupaten Ponorogo melalui kegiatan kontra penginderaan;
o. konsultasi Keamanan Informasi bagi pengguna layanan; dan/atau
p. jenis Layanan Keamanan Informasi lainnya.

Pasal 28

(1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 26, 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 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 manajemen Layanan Keamanan Informasi.

(5) Dalam melaksanakan Layanan Keamanan Informasi sebagaimana yang dimaksud pada ayat 1, Dinas berkoordinasi dan berkonsultasi kepada Dinas Komunikasi Informatika Provinsi Jawa Timur dan BSSN.

BAB IV
PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI

Pasal 29

(1) Penetapan pola hubungan komunikasi sandi antar PD ditetapkan oleh Bupati.

(2) Penetapan pola hubungan komunikasi sandi antar PD sebagaimana dimaksud pada ayat (1), untuk menentukan jaring komunikasi internal Pemerintah Daerah.

(3) Untuk jaring komunikasi sandi di Lingkungan Pemerintah Daerah mengacu pada peraturan perundang-undangan.

Pasal 30

Penetapan pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 29, dilaksanakan melalui:

a. identifikasi pola hubungan komunikasi sandi; dan
b. analisis pola hubungan komunikasi sandi.

Pasal 31

Identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 30 huruf (a), dilakukan terhadap:

a. pola hubungan komunikasi pimpinan dan pejabat struktural internal Pemerintah Daerah;
b. alur informasi yang dikomunikasikan antar PD dan Internal PD;
c. teknologi Informasi dan Komunikasi;
d. kompetensi personel; dan
e. Infrastruktur komunikasi.

Pasal 32

Analisis pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 30 huruf (b), dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi yang 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, serta fasilitas lainnya yang dibutuhkan; dan
d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.

Pasal 33

(1) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud dalam Pasal 32 ditetapkan sebagai pola hubungan komunikasi sandi antar PD.

(2) Penetapan pola hubungan komunikasi sandi antar PD sebagaimana dimaksud pada ayat (1) ditetapan dengan Keputusan Bupati.

(3) Keputusan sebagaimana dimaksud pada ayat (2), 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 tanggung jawab pengelola dan Pengguna Layanan.

(4) Salinan Keputusan sebagaimana dimaksud pada ayat (2), disampaikan oleh Bupati kepada Gubernur sebagai Wakil Pemerintah Pusat dan ditembuskan kepada Kepala BSSN.

BAB V
OPERASIONAL DUKUNGAN PERSANDIAN
UNTUK PENGAMANAN INFORMASI

Pasal 34

(1) Operasional dukungan Persandian untuk pengamanan informasi merupakan kegiatan operasional yang tidak terkait dengan Kriptografi namun mendukung terciptanya keamanan informasi.

(2) Operasional dukungan persandian untuk pengamanan informasi sebagaimana dimaksud pada ayat (1) meliputi :
    a. Pengamanan gelombang frekuensi;
    b. Kontra penginderaan; dan
    c. Penilaian Keamanan Sistem Informasi

(3) Pelaksana kegiatan operasional dukungan persandian untuk pengamanan informasi adalah Aparatur Sipil Negara yang bertugas di Dinas

(4) Pelaksana op.rasional dukungan Persandian untuk pengamanan informasi Pemerintah Daerah mengacu pada ketentuan peraturan perundang-undangan.

Pasal 35

(1) Pengamanan gelombang frekuensi sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf a, merupakan upaya pengamanan sinyal dari ancaman penyalahgunaan sinyal untuk kepentingan yang tidak bertanggung jawab dengan cara menutup/memutuskan frekuensi

(2) Pengamanan gelombang frekuensi dilakukan berdasarkan hasil identifikasi pada kegiatan Pemerintah Daerah yang berpotensi timbulnya ancaman penyalahgunaan sinyal.

Pasal 36

(1) Kontra penginderaan sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf b, merupakan upaya melakukan deteksi dari pengawasan oleh pihak yang tidak berwenang pada objek ruang tertentu.

(2) Kontra penginderaan sebagaimana dimaksud pada ayat (1) dilakukan pada objek ruang milik Pemerintah Daerah yang dilakukan untuk melakukan komunikasi terkait informasi yang harus diamankan.

(3) Pelaksanaan kontra penginderaan sebagaimana dimaksud pada ayat (2), dilakukan secara berkala.

(4) Temuan hasil kontra penginderaan berupa barang yang diduga menjadi peralatan penginderaan dapat dikonsultasikan ke Badan Siber dan Sandi Negara.

(5) Hasil pelaksanaan kontra penginderaan harus ditindaklanjuti oleh Pemerintah Daerah sebagai bahan evaluasi dan perbaikan penyelenggaraan urusan pemerintah bidang Persandian.

Pasal 37

(1) Penilaian keamanan sistem informasi sebagaimana dimaksud dalam Pasal 34 ayat (2) huruf c, merupakan upaya untuk mengukur tingkat kerawanan dan keamanan dari sistem informasi di Pemerintah Daerah.

(2) Penilaian keamanan sistem informasi dilakukan pada sistem informasi milik Pemerintah Daerah.

(3) Pemerintah Daerah melaksanakan kegiatan penilaian keamanan sistem informasi berkoordinasi ke Badan Siber dan Sandi Negara.

(4) Hasil pelaksanaan penilaian keamanan sistem informasi sebagaimana dimaksud pada ayat (3), harus ditindaklanjuti oleh Pemerintah Daerah sebagai bahan evaluasi dan perbaikan penyelenggaraan urusan Pemerintahan bidang Persandian.

BAB VI
LAYANAN SERTIFIKAT ELEKTRONIK

Pasal 38

(1) Layanan Sertifikat Elektronik di Pemerintah Daerah bertujuan untuk menjamin keutuhan, otentikasi dan nirsangkal Dokumen Elektronik.

(2) Layanan Sertifikat Elektronik dapat dimanfaatkan oleh Pemerintah Daerah jika memenuhi persyaratan dan telah diberikan kewenangan oleh Balai Sertifikasi Elektronik BSSN sesuai ketentuan peraturan perundang-undangan.

(3) Setiap Aparatur Sipil dapat memiliki Sertifikat Elektronik yang dapat digunakan selama melaksanakan tugas kedinasan.

(4) Kepemilikan Sertifikat Elektronik sebagaimana dimaksud pada ayat (2), difasilitasi oleh Dinas –.

(5) Tugas kedinasan sebagaimana dimaksud pada ayat (3) meliputi:
   a. pengiriman dan pembuatan surat elektronik ;
   b. pembuatan dokumen persuratan elektronik; dan/atau
   c. pembuatan dokumen elektronik lainnya yang menggunakan aplikasi dan sistem elektronik.

(6) Aplikasi dan Sistem Elektronik yang dimiliki oleh Pemerintah Daerah harus memanfaatkan layanan Sertifikat Elektronik dalam rangka pengamanan informasi.

Pasal 39

(1) Proses pemanfaatan Layanan Sertifikat Elektronik dilakukan melalui:
   a. pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaharuan dan pencabutan Sertifikat Elektronik;
   b. pengembangan aplikasi pendukung penggunaan Sertifikat Elektronik;
   c. fasilitasi kegiatan sosialisasi dan bimbingan teknis terkait sertifikat elektronik; dan
   d. pengawasan dan evaluasi penggunaan sertifikat elektronik.

(2) Pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaharuan dan pencabutan Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) huruf a meliputi:
   a. menangani verifikasi identitas berdasarkan identitas resmi, keanggotaan pada instansi dan rekomendasi dari instansi;
   b. menyetujui/menolak permintaan pendaftaran sertifikat elektronik;
   c. menindaklanjuti permintaan Sertifikat Elektronik kepada Badan Sertifikat Elektronik (BsrE);
   d. menyampaikan sertifikat elektronik kepada pemohon; dan
   e. melakukan pengarsipan berkas pendaftaran Sertifikat Elektronik (hardcopy dan softcopy).

BAB VII
PEMANTAUAN, EVALUASI DAN PELAPORAN

Pasal 40

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar PD.

(2) Dinas melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1), setiap 1 (satu) tahun sekali.

(3) Dinas menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1), kepada Bupati dan Gubernur Jawa Timur sebagai Wakil Pemerintah Pusat.

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

BAB VIII
PENDANAAN

Pasal 41

Pendanaan penyelenggaraan persandian untuk pengamanan informasi bersumber dari:

a. Anggaran Pendapatan dan Belanja Daerah Kabupaten Ponorogo; dan
b. Sumber lain yang sah dan tidak mengikat sesuai ketentuan peraturan perundang-undangan.

BAB IX
KETENTUAN PENUTUP

Pasal 42

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Ponorogo
pada tanggal 30 Juli 2024

BUPATI PONOROGO,

TTD.

SUGIRI SANCOKO

Diundangkan di Ponorogo
pada tanggal 30-07-2024

SEKRETARIS DAERAH
KABUPATEN PONOROGO,

TTD.

AGUS PRAMONO

BERITA DAERAH KABUPATEN PONOROGO TAHUN 2024 NOMOR 70.

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM
SEKRETARIAT DAERAH

SOEGENG PRAKOSO, S.H., M.H.
NIP. 19630605 199303 1 003