SALINAN

BUPATI KUTAI KARTANEGARA
PROVINSI KALIMANTAN TIMUR

PERATURAN BUPATI KUTAI KARTANEGARA
NOMOR 34 TAHUN 2025
TENTANG
PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI KUTAI KARTANEGARA,

Menimbang :

a. 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, yang menyatakan Bupati sesuai dengan kewenangannya bertanggung jawab terhadap Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah;

b. bahwa berdasarkan ketentuan Pasal 12 Ayat (2) huruf o Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah, penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah merupakan urusan pemerintahan wajib yang tidak berkaitan dengan pelayanan dasar menjadi kewenangan Pemerintah Daerah;

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

Mengingat:

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang–Undang Nomor 27 Tahun 1959 tentang Penetapan Undang-Undang Darurat No. 3 Tahun 1953 tentang Perpanjangan Pembentukan Daerah Tingkat II di Kalimantan (Lembaran Negara Republik Indonesia Tahun 1953 No. 9) Sebagai Undang-Undang, (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 72, Tambahan Lembaran Negara Nomor 1820), sebagaimana telah beberapa kali diubah terakhir dengan Undang- Undang Nomor 8 Tahun 1965 tentang Pembentukan Daerah Tingkat II Tanah Laut, daerah Tingkat II Tapin dan Daerah Tingkat II Tabalong dengan Mengubah Undang-Undang Nomor 27 Tahun 1959 tentang Penetapan Undang-Undang Darurat No. 3 Tahun 1953 tentang Perpanjangan Pembentukan Daerah Tingkat II di Kalimantan (Lembaran Negara Tahun 1965 Nomor 51, Tambahan Lembaran Negara Nomor 2756);
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 beberapa kali diubah dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);

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);

MEMUTUSKAN:

Menetapkan: PERATURAN BUPATI TENTANG PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH DAERAH.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini, yang dimaksud dengan:

1. Daerah adalah Kabupaten Kutai Kartanegara.
2. Bupati adalah Bupati Kutai Kartanegara.
3. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom Kabupaten Kutai Kartanegara.
4. Perangkat Daerah yang selanjutnya disingkat PD adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
5. PD Pelaksana Urusan Pemerintahan di Bidang Persandian adalah Dinas Komunikasi dan Informatika Kabupaten Kutai Kartanegara.
6. 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.
7. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keaslian (*authentication*), keutuhan (*integrity*), ketersediaan (*availability*), dan kenirsangkalan (*nonrepudiation*) informasi.
8. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
9. Sistem Elektronik adalah serangkaian perangkat dan Prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
10. 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 sertifikat elektronik.

11. Pola Hubungan Komunikasi Sandi adalah keterhubungan antar pengguna persandian melalui jaringan komunikasi.
12. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data serta otentifikasi data.
13. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan urusan Pemerintahan bidang Persandian dan yang memiliki manfaat.
14. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
15. Balai Besar Sertifikasi Elektronik yang selanjutnya disingkat BSrE merupakan unit pelaksana teknis penyelenggara Otoritas Sertifikat Digital BSSN yang berada di bawah dan bertanggung jawab kepada Kepala BSSN.

Pasal 2

Peraturan Bupati ini dimaksudkan sebagai pedoman bagi Pemerintah Daerah dalam:

a. melaksanakan kebijakan, program dan kegiatan pelaksanaan persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah; dan
b. menetapkan Pola Hubungan Komunikasi Sandi antar PD.

Pasal 3

Peraturan Bupati ini Bertujuan untuk:

a. menciptakan harmonisasi dalam melaksanakan persandian untuk Pengamanan Informasi di Pemerintah Daerah;
b. meningkatkan komitmen, efektifitas, dan kinerja PD dalam melaksanakan program dan kegiatan pelaksanaan persandian untuk Pengamanan Informasi.

BAB II

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI PEMERINTAH DAERAH

Bagian Kesatu

Umum

Pasal 4

Penyelenggaraan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, meliputi:

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 5

Penyelenggara Persandian untuk Pengamanan Informasi di Pemerintah Daerah terdiri atas Bupati dibantu PD Pelaksana Urusan Pemerintahan di Bidang Persandian.

Pasal 6

(1) Bupati memimpin dan bertanggung jawab atas penyelenggaraan persandian yang menjadi kewenangan Daerah.
(2) PD Pelaksana Urusan Pemerintahan di bidang Persandian bertanggung jawab atas kinerja pelaksanaan urusan

pemerintahan bidang persandian sesuai tugas dan fungsinya.

Pasal 7

(1) PD Pelaksana Urusan Pemerintahan di Bidang Persandian menyusun perencanaan penyelenggaraan Persandian sesuai dengan kewenangannya.

(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 Rencana Pembangunan Jangka Menengah Daerah, dan Rencana Kerja Pemerintah Daerah.

Pasal 8

(1) Dalam rangka menjabarkan Rencana Pembangunan Jangka Menengah Daerah sebagaimana dimaksud dalam Pasal 7 ayat (4), PD pelaksana urusan Pemerintahan Bidang Persandian menyusun Rencana Strategis PD yang memuat tujuan, sasaran, program dan kegiatan penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah.

(2) Dalam rangka menjabarkan Rencana Kerja Pemerintah Daerah sebagaimana dimaksud dalam Pasal 7 ayat (4), PD pelaksana Urusan Pemerintahan Bidang Persandian menyusun Rencana Kerja Perangkat Daerah yang memuat program, kegiatan, lokasi dan kelompok sasaran berdasarkan layanan urusan pemerintah bidang Persandian, disertai penganggaran penyelenggaraan Persandian untuk pengamanan informasi di Lingkungan Pemerintah Daerah.

Kedua

Penyusunan Kebijakan Pengamanan Informasi

Pasal 9

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 4 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 sesuai dengan kewenangannya.
(2) Dalam melakukan penyusunan Rencana Strategis sebagaimana dimaksud pada ayat (1), Bupati dapat melakukan koordinasi dan konsultasi kepada BSSN dan menunjuk PD Pelaksana Urusan Pemerintahan di Bidang Persandian.

Pasal 11

(1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf b, ditetapkan oleh Bupati sesuai dengan kewenangannya.
(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 Bupati melalui PD Pelaksana Urusan Pemerintahan di Bidang Persandian 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 sesuai dengan kewenangannya.

(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 atau aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) Bupati melalui PD Pelaksana Urusan Pemerintahan di Bidang Persandian dapat melakukan koordinasi dan konsultasi kepada BSSN.

Bagian Ketiga

Pengelolaan Sumber Daya Keamanan Informasi

Pasal 13

(1) PD Pelaksana Urusan di Bidang Persandian harus melakukan 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 sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf a 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 Perangkat Daerah.

(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:
a. melalui tugas belajar, pendidikan dan pelatihan, pembentukan dan penjenjangan fungsional,

pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, *workshop*, seminar dan kegiatan lainnya yang terkait pengembangan kompetensi sumber daya manusia di bidang Keamanan Informasi;

b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya atau Pemerintah Daerah; dan

c. memenuhi jumlah waktu minimal sebagai seorang pegawai untuk meningkatkan kompetensi bidangnya.

(4) Pembinaan karir sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan dengan ketentuan:

a. pembinaan jabatan fungsional di bidang Keamanan Informasi, dan

b. pengisian jabatan struktural sesuai 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:

a. pendidikan dan pelatihan jabatan fungsional;

b. pendidikan dan pelatihan teknis sandi;

c. bimbingan teknis; dan

d. kegiatan pengembangan kompetensi lain yang terkait dengan Persandian dan teknologi informasi serta bidang ilmu lainnya yang dibutuhkan.

(2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) merupakan pengembangan sumber daya manusia yang terkait dengan ilmu Persandian dan teknologi informasi serta bidang ilmu lainnya yang dibutuhkan.

Pasal 17

Sumber daya manusia yang sudah tidak melaksanakan tugas pada PD pelaksana urusan Pemerintah bidang Persandian harus disesuaikan kewenangannya, yaitu:

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

Pasal 18

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 13 ayat (2) huruf c dilakukan oleh PD Pelaksana Urusan Pemerintahan di Bidang Persandian untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.
(2) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi Pemerintah Daerah.
(3) Dalam pelaksanaan manajemen pengetahuan, Pemerintah Daerah berkoordinasi dan dapat melakukan 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 4 huruf c, dilaksanakan oleh PD Pelaksana Urusan Pemerintahan Bidang Persandian 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 20, PD Pelaksana Urusan Pemerintahan di Bidang Persandian 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 pemerintahan berbasis elektronik.
(5) Penanggulangan dan pemulihan sebagaimana dimaksud pada ayat (1) huruf d, dilakukan dengan kegiatan penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Pasal 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 Sertifikat 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), PD Pelaksana Urusan Pemerintahan di Bidang Persandian 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 Pelaksana Urusan Pemerintahan di Bidang Persandian melaksanakan audit Keamanan Informasi di lingkup Pemerintah Daerah.
(2) PD mendukung pelaksanaan kegiatan audit Keamanan Informasi di wilayah kerjanya.
(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.

Bagian Kelima
Penyediaan Layanan Keamanan Informasi

Pasal 26

(1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 huruf d, dilaksanakan oleh PD Pelaksana Urusan Pemerintahan di Bidang Persandian.
(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1), disediakan untuk pengguna layanan yang terdiri dari :
    a. Bupati dan Wakil Bupati;
    b. PD;
    c. aparatur sipil negara pada Pemerintah Daerah; dan
    d. pihak lainnya.

Pasal 27

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 26 ayat (1), meliputi:

a. identifikasi kerentanan dan penilaian resiko terhadap Sistem Elektronik;
b. asistensi dan fasilitasi penguatan keamanan Sistem Elektronik;
c. penerapan Sertifikat Elektronik untuk melindungi Sistem Elektronik dan dokumen elektronik;
d. perlindungan informasi melalui penyediaan perangkat

teknologi Keamanan Informasi dan jaring komunikasi sandi;

e. fasilitasi sertifikasi penerapan manajemen pengamanan Sistem Elektronik;
f. audit keamanan Sistem Elektronik;
g. audit keamanan pelaksanaan sistem manajemen;
h. literasi Keamanan Informasi dalam rangka peningkatan kesadaran Keamanan Informasi dan pengukuran tingkat kesadaran Keamanan Informasi di lingkungan Pemerintah Daerah dan publik;
i. peningkatan kompetensi sumber daya manusia dibidang 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 Daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
n. perlindungan informasi pada aset/fasilitas penting milik atau yang akan digunakan Pemerintah Daerah melalui kegiatan kontra penginderaan;
o. konsultasi Keamanan Informasi bagi pengguna layanan; dan/atau
p. jenis Layanan Keamanan Informasi lainnya.

Pasal 28

(1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 22, PD melaksanakan manajemen Layanan Keamanan Informasi.
(2) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan Keamanan Informasi kepada pengguna layanan.
(3) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) merupakan penanganan terhadap keluhan, gangguan, masalah, permintaan, dan/atau

perubahan Layanan Keamanan Informasi dari pengguna layanan.

(4) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen Layanan Keamanan Informasi.

BAB III
PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PD

Pasal 29

(1) Penetapan Pola Hubungan Komunikasi Sandi antar PD sebagaimana dimaksud dalam Pasal 3 huruf c ditetapkan oleh Bupati.

(2) Penetapan Pola Hubungan Komunikasi Sandi antar PD sebagaimana dimaksud pada ayat (1) untuk menentukan jaring komunikasi sandi internal Pemerintah Daerah.

(3) Jaring komunikasi sandi internal Pemerintah Daerah sebagaimana dimaksud pada ayat (2) terdiri atas:
   a. jaring komunikasi sandi antar PD;
   b. jaring komunikasi sandi internal PD; dan
   c. jaring komunikasi sandi pimpinan Daerah.

(4) Jaring komunikasi sandi antar PD sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh PD.

(5) Jaring komunikasi sandi internal PD sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar pengguna layanan di lingkup internal PD.

(6) Jaring komunikasi sandi pimpinan Daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Bupati, Wakil Bupati dan Kepala PD.

Pasal 30

(1) Untuk kelancaran pelaksanaan Pola Hubungan Komunikasi Sandi, PD Pelaksana Urusan Pemerintahan di Bidang Persandian dapat melakukan kerja sama dengan BSSN, kementerian/lembaga yang

menyelenggarakan tugas pemerintahan di bidang Persandian dan Keamanan Informasi serta antar pemerintah daerah.

(2) Pemerintah Daerah dapat melakukan kegiatan operasional jaring komunikasi sandi secara mandiri berkoordinasi dengan BSSN.

(3) Tata cara kerja sama sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 31

(1) Penetapan Pola Hubungan Komunikasi Sandi sebagaimana dimaksud dalam Pasal 29, dilakukan melalui:
   a. identifikasi Pola Hubungan Komunikasi Sandi; dan
   b. analisis Pola Hubungan Komunikasi Sandi.

(2) Identifikasi Pola Hubungan Komunikasi Sandi sebagaimana dimaksud pada ayat (1) huruf a, dilakukan terhadap:
   a. pola hubungan komunikasi pimpinan dan pejabat struktural internal Pemerintah Daerah;
   b. alur informasi yang dikomunikasikan antar PD dan internal PD;
   c. teknologi informasi dan komunikasi;
   d. infrastruktur komunikasi; dan
   e. kompetensi personel.

(3) Analisis Pola Hubungan Komunikasi Sandi sebagaimana dimaksud pada ayat (1) huruf b, dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi 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 32

(1) Hasil analisis Pola Hubungan Komunikasi Sandi pada Pasal 31 ayat (3) ditetapkan sebagai Pola Hubungan Komunikasi Sandi antar PD oleh Bupati dalam bentuk keputusan.

(2) Keputusan sebagaimana dimaksud pada ayat (1), 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.

(3) Salinan keputusan sebagaimana dimaksud pada ayat (2), disampaikan oleh Bupati kepada Gubernur sebagai wakil pemerintah pusat dan ditembuskan kepada Kepala BSSN.

BAB IV

OPERASIONAL DUKUNGAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

Pasal 33

(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 *(jamming)*;
   b. kontra penginderaan; dan
   c. penilaian Keamanan Sistem Informasi.

(3) Pelaksana kegiatan operasional dukungan persandian untuk Pengamanan Informasi adalah Aparatur Sipil

Negara di Pemerintah Daerah yang berada pada Bidang atau Seksi penyelenggara Persandian pada PD pelaksana urusan Pemerintahan bidang Persandian.

(4) Pelaksanaan operasional dukungan Persandian untuk Pengamanan Informasi Pemerintah Daerah mengacu pada ketentuan peraturan perundang-undangan.

Pasal 34

(1) Pengamanan gelombang frekuensi *(jamming)* sebagaimana dimaksud dalam Pasal 33 ayat (2) huruf a, merupakan upaya pengamanan sinyal dan ancaman penyalahgunaan sinyal untuk kepentingan yang tidak bertanggung jawab dengan cara menutup/memutuskan frekuensi.

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

Pasal 35

(1) Kontra penginderaan sebagaimana dimaksud dalam Pasal 33 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 *(surveillance)* dapat dikonsultasikan ke BSSN.

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

Pasal 36

(1) Penilaian keamanan sistem informasi sebagaimana dimaksud dalam Pasal 33 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 BSSN.

(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 V

LAYANAN SERTIFIKAT ELEKTRONIK

Pasal 37

(1) Layanan Sertifikat Elektronik di Pemerintah Daerah bertujuan untuk menjamin keutuhan, otentifikasi dan nirsangkal dokumen elektronik.

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

(3) Setiap aparatur sipil negara Pemerintah Daerah dapat memiliki Sertifikat Elektronik yang dapat digunakan selama melaksanakan tugas kedinasan.

(4) Kepemilikan Sertifikat Elektronik sebagaimana dimaksud pada ayat (2), difasilitasi oleh PD Pelaksana Urusan Pemerintahan di Bidang Persandian.

(5) Tugas kedinasan sebagaimana dimaksud pada ayat (3) meliputi:

a. pengiriman dan pembuatan surat elektronik *(email)*;

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 38

(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 BSrE;
   d. menyampaikan Sertifikat Elektronik kepada pemohon; dan
   e. melakukan pengarsipan berkas pendaftaran Sertifikat Elektronik (*hardcopy* dan *softcopy*).

BAB VI

PEMANTAUAN, EVALUASI DAN PELAPORAN

Pasal 39

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan Pola Hubungan Komunikasi Sandi antar PD.

(2) PD Pelaksana Urusan Pemerintahan di Bidang Persandian melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1), setiap 1 (satu) tahun sekali.

(3) PD Pelaksana Urusan Pemerintahan di Bidang Persandian menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1), kepada Bupati dan Gubernur 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 VII

PENDANAAN

Pasal 40

Pendanaan penyelenggaraan Persandian untuk Pengamanan Informasi bersumber dari:

a. anggaran pendapatan dan belanja Daerah; dan

b. sumber lain yang sah dan tidak mengikat sesuai ketentuan peraturan perundang-undangan.

BAB VIII

KETENTUAN PENUTUP

Pasal 41

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Tenggarong
pada tanggal 4 Agustus 2025

BUPATI KUTAI KARTANEGARA

ttd

AULIA RAHMAN BASRI

Diundangkan di Tenggarong
pada tanggal 4 Agustus 2025

SEKRETARIS DAERAH
KABUPATEN KUTAI KARTANEGARA

ttd

SUNGGONO

BERITA DAERAH KABUPATEN KUTAI KARTANEGARA TAHUN 2025 NOMOR 82

Salinan Sesuai Dengan Aslinya
Sekretariat Kabupaten Kutai Kartanegara
Kepala Bagian Hukum

PURNOMO, SH
NIP. 19780605 200212 1 002