



BUPATI TABALONG
PROVINSI KALIMANTAN SELATAN

PERATURAN BUPATI TABALONG
NOMOR 39 TAHUN 2025

TENTANG

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI TABALONG,

- Menimbang : a. bahwa penyelenggaraan persandian merupakan perwujudan dari prinsip kedaulatan daerah dalam mengelola dan melindungi informasi yang bersifat strategis, demi menjamin keberlangsungan tata kelola pemerintahan yang baik, serta merupakan implementasi dari nilai tanggung jawab moral untuk menjaga kerahasiaan dan integritas data publik dari ancaman dan penyalahgunaan;
- b. bahwa meningkatnya ketergantungan masyarakat dan Pemerintah Daerah terhadap sistem dan teknologi informasi menuntut adanya kepastian perlindungan data dan informasi, sehingga penyelenggaraan persandian dibutuhkan untuk menumbuhkan kepercayaan publik terhadap keamanan layanan digital Pemerintah Daerah;
- c. bahwa berdasarkan ketentuan Pasal 33 Peraturan Bupati Tabalong Nomor 37 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Tabalong, Perangkat Daerah berkoordinasi dan dapat melakukan konsultasi dengan dinas yang menyelenggarakan urusan pemerintahan bidang persandian berdasarkan pedoman manajemen keamanan informasi sistem pemerintahan berbasis elektronik untuk mewujudkan penyelenggaraan persandian secara aman untuk mencegah penyalahgunaan;
- d. 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;
- e. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, huruf c dan huruf d, perlu menetapkan Peraturan Bupati tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi;

- 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 Nomor 3 Tahun 1953 tentang Perpanjangan Pembentukan Daerah Tingkat II di Kalimantan (Lembaran Negara Republik Indonesia Tahun 1953 Nomor 9), sebagai Undang-Undang (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 72, Tambahan Lembaran Negara Republik Indonesia 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 Nomor 3 Tahun 1953 tentang Pembentukan Daerah Tingkat II Di Kalimantan (Lembaran Negara Republik Indonesia Tahun 1965 Nomor 51, Tambahan Lembaran Negara Republik Indonesia 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, terakhir 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 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234), sebagaimana telah beberapa kali diubah, terakhir dengan Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua Atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 143, Tambahan Lembaran Negara Republik Indonesia Nomor 6801);
 6. 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 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);

7. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601), sebagaimana telah diubah 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);
8. Undang-Undang Nomor 8 Tahun 2022 tentang Provinsi Kalimantan Selatan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 68, Tambahan Lembaran Negara Republik Indonesia Nomor 6779);
9. 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);
10. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 114, Tambahan Lembaran Negara Republik Nomor 5888), sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 72 Tahun 2019 tentang Perubahan Atas Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 187, Tambahan Lembaran Negara Republik Indonesia Nomor 6402);
11. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
12. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan Atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 157);
13. 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);
14. Peraturan Daerah Kabupaten Tabalong Nomor 05 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Tabalong Tahun 2016 Nomor 05, Tambahan Lembaran Daerah Kabupaten Tabalong Nomor 02), sebagaimana telah beberapa kali diubah, terakhir dengan Peraturan Daerah Kabupaten Tabalong Nomor 3 Tahun 2024 tentang Perubahan Kedua Atas Peraturan Daerah Kabupaten Tabalong Nomor 05 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Tabalong Tahun 2024 Nomor 3, Tambahan Lembaran Daerah Kabupaten Tabalong Nomor 3);

15. Peraturan Bupati Tabalong Nomor 37 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Tabalong (Berita Daerah Kabupaten Tabalong Tahun 2021 Nomor 37);
16. Peraturan Bupati Tabalong Nomor 69 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Perangkat Daerah Kabupaten Tabalong (Berita Daerah Kabupaten Tabalong Tahun 2021 Nomor 69), sebagaimana telah diubah dengan Peraturan Bupati Tabalong Nomor 17 Tahun 2025 tentang Perubahan Atas Peraturan Bupati Tabalong Nomor 69 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Perangkat Daerah Kabupaten Tabalong (Berita Daerah Kabupaten Tabalong Tahun 2025 Nomor 17);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

**BAB I
KETENTUAN UMUM**

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Pemerintah Pusat adalah Presiden Republik Indonesia yang memegang kekuasaan pemerintahan negara Republik Indonesia yang dibantu oleh Wakil Presiden dan menteri sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
2. Gubernur adalah Gubernur Kalimantan Selatan.
3. Daerah adalah Kabupaten Tabalong.
4. Pemerintahan Daerah adalah penyelenggaraan urusan pemerintahan oleh pemerintah daerah dan dewan perwakilan rakyat daerah menurut asas otonomi dan tugas pembantuan dengan prinsip otonomi seluas-luasnya dalam sistem dan prinsip Negara Kesatuan Republik Indonesia sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
5. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin Pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
6. Bupati adalah Bupati Tabalong.
7. Wakil Bupati adalah Wakil Bupati Tabalong.
8. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
9. Dinas adalah Perangkat Daerah yang menyelenggarakan urusan pemerintahan bidang Persandian.
10. Kepala Dinas adalah Kepala Dinas Komunikasi dan Informatika Kabupaten Tabalong.
11. Rencana Pembangunan Jangka Menengah Daerah yang selanjutnya disebut RPJMD adalah dokumen perencanaan pembangunan Daerah untuk periode 5 (lima) tahun.
12. Persandian adalah kegiatan di bidang pengamanan data atau informasi yang dilaksanakan dengan menerapkan konsep, teori, seni dan ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis, dan konsisten serta terikat pada etika profesi sandi.

13. Jaring Komunikasi Sandi yang selanjutnya disebut JKS adalah keterhubungan antar pengguna persandian melalui jaring telekomunikasi.
14. 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 yang dimaksud adalah informasi publik, informasi berklasifikasi serta informasi elektronik, dan informasi siber.
15. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan dan kenirsangkalan Informasi.
16. Pengamanan Informasi adalah segala upaya, kegiatan dan tindakan untuk mewujudkan Keamanan Informasi.
17. Dokumen Elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirim, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal atau sejenisnya yang dapat dilihat, ditampilkan dan atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
18. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan Informasi elektronik.
19. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subyek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh balai sertifikasi elektronik lembaga sandi negara.
20. Kontra Penginderaan adalah kegiatan atau proses dalam mengidentifikasi ancaman penyadapan maupun kerawanan kebocoran informasi dari alat atau perangkat *surveillance*.
21. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah Lembaga Pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
22. Otoritas Pendaftaran adalah unit yang bertanggung jawab melakukan pemeriksaan, pemberian persetujuan atau penolakan atas setiap permintaan penerbitan, pembaruan, dan pencabutan Sertifikat Elektronik yang diajukan oleh pemilik atau calon Pemilik Sertifikat Elektronik.
23. Sumber Daya Keamanan Informasi adalah semua komponen yang disediakan untuk merancang, menerapkan, dan memelihara perlindungan terhadap informasi agar terhindar dari akses, modifikasi, pengungkapan, atau perusakan yang tidak sah.
24. Informasi Non Elektronik adalah data atau informasi yang disimpan dan disampaikan dalam bentuk fisik atau manual, tanpa bantuan perangkat digital.
25. Rencana Strategis Pengamanan Informasi adalah dokumen kebijakan jangka menengah yang menetapkan arah, tujuan, prioritas, dan langkah-langkah untuk melindungi aset informasi organisasi dari ancaman, memastikan kerahasiaan, integritas, dan ketersediaan informasi.
26. Arsitektur Keamanan adalah sebuah kerangka kerja sistematis yang bertujuan melindungi aset informasi organisasi dari berbagai ancaman.
27. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
28. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan layanan Keamanan Informasi.

Pasal 2

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

Pasal 3

Peraturan Bupati ini bertujuan untuk:

- a. memfasilitasi penyelenggaraan persandian untuk pengamanan informasi lingkup Pemerintah Daerah;
- b. meningkatkan komitmen, efektivitas, dan kinerja pelaksanaan kebijakan, program dan kegiatan penyelenggaraan persandian untuk pengamanan informasi; dan
- c. memberikan pedoman dalam menetapkan pola hubungan komunikasi sandi antar Perangkat Daerah.

Pasal 4

Ruang lingkup pengaturan dalam Peraturan Bupati ini meliputi:

- a. penyelenggaraan Persandian untuk Pengamanan Informasi;
- b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah;
- c. pemantauan, evaluasi dan pelaporan;
- d. pembinaan dan pengawasan teknis; dan
- e. Pendanaan.

BAB II
PENYELENGGARAAN PERSANDIAN
UNTUK PENGAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 5

- (1) Pemerintah Daerah menyusun perencanaan Penyelenggaraan Persandian untuk Pengamanan Informasi.
- (2) Penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) diintegrasikan dengan RPJMD.

Pasal 6

- (1) Bupati bertanggung jawab terhadap penyelenggaraan persandian untuk Pengamanan Informasi.
- (2) 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 Non elektronik; dan
 - d. penyediaan layanan Keamanan Informasi.

Bagian Kedua
Penyusunan Kebijakan Pengamanan Informasi

Pasal 7

Penyusunan Kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf a dilaksanakan dengan:

- a. menyusun Rencana Strategis Pengamanan Informasi;
- b. menetapkan arsitektur Keamanan Informasi; dan
- c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

Pasal 8

- (1) Penyusunan Rencana Strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 7 huruf a disusun oleh Bupati sesuai dengan kewenangannya.
- (2) Penyusunan Rencana Strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.
- (3) Rencana strategis sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. tujuan, sasaran, program, kegiatan, dan target pelaksanaan Pengamanan Informasi setiap tahun untuk jangka waktu 5 (lima) tahun; dan
 - b. peta rencana penyelenggaraan Pengamanan Informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun untuk jangka waktu 5 (lima) tahun.
- (4) Rencana Strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Bupati.

Pasal 9

- (1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 7 huruf b ditetapkan oleh Bupati atas usulan Kepala Dinas.
- (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) Arsitektur Keamanan Informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.
- (4) Arsitektur Keamanan Informasi dilakukan evaluasi pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu waktu sesuai dengan kebutuhan.

Pasal 10

- (1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 7 huruf c ditetapkan oleh Bupati.
- (2) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) minimal 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
- h. keamanan komunikasi.

Pasal 11

- (1) Dalam melakukan penyusunan rencana strategis, Arsitektur Keamanan Informasi, dan aturan mengenai tata Kelola Keamanan Informasi, Bupati dapat melakukan koordinasi dan konsultasi kepada BSSN.
- (2) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (1) Bupati dapat menunjuk Dinas.

Bagian Ketiga Pengelolaan Sumber Daya Keamanan Informasi

Pasal 12

- (1) Pengelolaan Sumber Daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf b dilaksanakan oleh Dinas.
- (2) Pengelolaan Sumber Daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
 - a. pengelolaan aset keamanan teknologi informasi dan komunikasi;
 - b. pengelolaan sumber daya manusia; dan
 - c. manajemen pengetahuan.

Pasal 13

- (1) Pengelolaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.
- (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 14

- (1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf b dilakukan oleh Dinas dan berkoordinasi dengan Perangkat Daerah yang membidangi urusan kepegawaian dan urusan pengembangan sumber daya manusia.
- (2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses sebagai berikut:
 - a. pengembangan kompetensi;
 - b. pembinaan karir;
 - c. pendayagunaan; dan
 - d. pemberian tunjangan pengamanan persandian.

Pasal 15

- (1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf a dilaksanakan dengan ketentuan:
 - a. melalui tugas belajar, pendidikan dan pelatihan pembentukan dan penjurangan 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 seorang pegawai untuk meningkatkan kompetensi di bidang Keamanan Informasi.
- (2) Pembinaan karir sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf b dilaksanakan dengan ketentuan:
 - a. pembinaan jabatan fungsional di bidang Keamanan Informasi; dan
 - b. pengisian formasi jabatan pimpinan tinggi, jabatan administrator, dan jabatan pengawas sesuai dengan standar kompetensi yang ditetapkan.
- (3) Pendayagunaan sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf c dilaksanakan dengan ketentuan seluruh sumber daya manusia yang bertugas di bidang Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan.

Pasal 16

- (1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 12 ayat (2) huruf c dilakukan oleh Dinas.
- (2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan 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) Manajemen pengetahuan sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi pemerintah daerah.
- (5) Dalam pelaksanaan manajemen pengetahuan, Pemerintah Daerah berkoordinasi dan dapat melakukan konsultasi dengan BSSN.

Bagian Keempat
Pengamanan Sistem Elektronik dan
Pengamanan Informasi Nonelektronik

Pasal 17

Pengamanan Sistem Elektronik dan pengamanan Informasi Non Elektronik sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf c dilaksanakan oleh Dinas sesuai ketentuan peraturan perundang-undangan.

Pasal 18

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 17 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 19

- (1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 18, 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 dengan kegiatan mitigasi risiko dan penerapan pelindungan 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 20

- (1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 17, Pemerintah Daerah 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) Sertifikat Elektronik sebagaimana dimaksud pada ayat (2) bertujuan:
 - a. meningkatkan kapabilitas dan tata kelola Keamanan Informasi dalam penyelenggaraan Sistem Elektronik;
 - b. meningkatkan Keamanan Informasi dalam Sistem Elektronik;
 - c. meningkatkan kepercayaan, kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan terhadap implementasi Sistem Elektronik; dan
 - d. meningkatkan efisiensi dan efektifitas penyelenggaraan pemerintahan dan pelayanan publik.

- (4) Untuk mendapatkan Sertifikat elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan oleh Otoritas Pendaftaran yang bertanggung jawab melakukan pemeriksaan, pemberian persetujuan atau penolakan atas setiap permintaan penerbitan, pembaruan, dan pencabutan Sertifikat Elektronik yang diajukan oleh pemilik atau calon Pemilik Sertifikat Elektronik.

Pasal 21

- (1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik sebagaimana dimaksud dalam Pasal 20 ayat (1), Pemerintah Daerah 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 22

- (1) Pengamanan Informasi Non Elektronik sebagaimana dimaksud dalam Pasal 17 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan Informasi Non Elektronik.
- (2) Pengamanan Informasi Non Elektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 23

- (1) Dinas berkoordinasi dengan BSSN melaksanakan audit Keamanan Informasi di lingkup Pemerintah Daerah.
- (2) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (1) meliputi audit keamanan Sistem Elektronik dan audit pelaksanaan sistem manajemen.
- (3) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima

Penyediaan Layanan Keamanan Informasi

Pasal 24

- (1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf d dilaksanakan oleh Dinas berkoordinasi dengan BSSN.
- (2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
 - a. Bupati dan Wakil Bupati;
 - b. Perangkat Daerah;
 - c. pegawai atau aparatur sipil negara pada Pemerintah Daerah; dan
 - d. Pengguna Layanan, yaitu:
 1. masyarakat umum;

2. stakeholder Non ASN; dan
3. pihak ketiga.

Pasal 25

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 24 ayat (1) meliputi:

- a. identifikasi kerentanan dan penilaian risiko 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 JKS;
- 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 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 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; dan/atau
- o. konsultasi Keamanan Informasi bagi Pengguna Layanan.

Pasal 26

- (1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 24, 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 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 PERANGKAT DAERAH

Pasal 27

- (1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah ditetapkan oleh Bupati.

- (2) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah 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 Perangkat Daerah;
 - b. jaring komunikasi sandi internal Perangkat Daerah; dan
 - c. jaring komunikasi sandi pimpinan Daerah.
- (4) Jaring komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh Perangkat Daerah.
- (5) Jaring komunikasi sandi internal Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar Pengguna Layanan di lingkup internal Perangkat Daerah.
- (6) Jaring komunikasi sandi pimpinan daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Bupati, Wakil Bupati, dan Kepala Perangkat Daerah.

Pasal 28

- (1) Penetapan pola hubungan komunikasi sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 27 ayat (1) dilaksanakan 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 Perangkat Daerah dan internal Perangkat Daerah;
 - 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 sebagaimana dimaksud pada ayat (2).
- (4) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3) 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, infrastruktur komunikasi, serta fasilitas lainnya yang dibutuhkan; dan
 - d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.
- (5) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (4) sebagai pola hubungan komunikasi sandi antar Perangkat Daerah ditetapkan dengan Keputusan Bupati.

- (6) Keputusan Bupati sebagaimana dimaksud pada ayat (5) minimal 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.
- (7) Keputusan Bupati sebagaimana dimaksud pada ayat (6) disampaikan oleh Bupati kepada Gubernur sebagai wakil Pemerintah Pusat dan ditembuskan kepada Kepala BSSN.

BAB IV PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 29

- (1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah.
- (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.
- (4) Bupati menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (3) kepada Gubernur sebagai wakil Pemerintah Pusat.

Pasal 30

Pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB V PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 31

Pembinaan dan pengawasan teknis terhadap penyelenggaraan persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dilaksanakan oleh BSSN dan Gubernur sebagai wakil Pemerintah Pusat.

Pasal 32

Pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar Perangkat Daerah dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI
PENDANAAN

Pasal 33

Pendanaan penyelenggaraan persandian yang diatur dalam Peraturan Bupati ini dibebankan pada Anggaran Pendapatan dan Belanja Daerah dan sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan dengan memperhatikan kemampuan kapasitas fiskal Daerah.

BAB VII
KETENTUAN PENUTUP

Pasal 34

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Tanjung
pada tanggal 13 November 2025

BUPATI TABALONG,

ttd.

MUHAMMAD NOOR RIFANI

Diundangkan di Tanjung
pada tanggal 13 November 2025

SEKRETARIS DAERAH KABUPATEN TABALONG,

ttd.

HAMIDA MUNAWARAH

BERITA DAERAH KABUPATEN TABALONG TAHUN 2025 NOMOR 39

Salinan Sesuai dengan Aslinya
KEPALA BAGIAN HUKUM,



NORMA ZAHRIATI, S.H.
NIP. 19730704 199903 2 004