SALINAN

BUPATI MURUNG RAYA
PROVINSI KALIMANTAN TENGAH

PERATURAN BUPATI MURUNG RAYA
NOMOR 10 TAHUN 2025

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK
DI LINGKUNGAN PEMERINTAH DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI MURUNG RAYA,

Menimbang : a. bahwa pemanfaatan teknologi informasi dan komunikasi diharapkan dapat meningkatkan efesiensi, efektifitas, transparansi, dan akuntabilitas dalam penyelenggaraan pemerintahan dan pelayanan publik dalam rangka mewujudkan salah satu tujuan nasional untuk memajukan kesejahteraan umum berdasarkan Pembukaan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

b. bahwa dalam rangka memastikan keamanan data dan informasi perlu dilakukan manajemen keamanan informasi melalui serangkaian proses yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja dan perbaikan berkelanjutan terhadap keamanan informasi dalam Sistem Pemerintahan Berbasis Elektronik;

c. bahwa berdasarkan Pasal 3 ayat (2) Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik serta Pasal 25 ayat (4) Peraturan Bupati Murung Raya Nomor 12 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Murung Raya, proses manajemen kemanan informasi ditetapkan oleh Kepala Daerah;

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

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

2. Undang-Undang Nomor 5 Tahun 2002, tentang Pembentukan Kabupaten Katingan, Kabupaten Seruyan, Kabupaten Sukamara, Kabupaten Lamandau, Kabupaten Gunung Mas, Kabupaten Pulang Pisau, Kabupaten Murung Raya dan Kabupaten Barito Timur di Provinsi Kalimantan Tengah (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 18, Tambahan Lembaran Negara Republik Indonesia Nomor 4180);

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 beberapakali 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);

3. 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);

4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapakali terakhir dengan Undang-undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);

5. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);

6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

7. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);

8. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);

9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
10. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
11. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
12. Peraturan Daerah Kabupaten Murung Raya Nomor 9 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Murung Raya (Lembaran Daerah Tahun 2016 Nomor 169, Tambahan Lembaran Daerah Kabupaten Murung Raya Nomor 38), sebagaimana telah beberapakali diubah terkahir dengan Peraturan Daerah Kabupaten Murung Raya Nomor 6 Tahun 2024 tentang Perubahan Kedua Atas Peraturan Daerah Kabupaten Murung Raya Nomor 9 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Murung Raya (Lembaran Daerah Kabupaten Murung Raya Tahun 2020 Nomor 28, Tambahan Lembaran Daerah Kabupaten Murung Raya Nomor 28);
13. Peraturan Bupati Murung Raya Nomor 12 Tahun 2023 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Murung Raya (Berita Daerah Kabupaten Murung Raya Tahun 2023 Nomor 145);

MEMUTUSKAN :

Menetapkan : **PERATURAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH DAERAH.**

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:
1. Daerah adalah Kabupaten Murung Raya.
2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Murung Raya.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Murung Raya.
5. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.

6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
7. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
8. Keamanan Informasi adalah suatu kondisi untuk melindungi aset yang dimiliki organisasi dari berbagai ancaman pihak internal maupun eksternal untuk menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, serta terjaganya aspek kerahasiaan, keutuhan dan ketersediaan dari informasi.
9. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
10. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
11. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
12. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan system, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrase/penghubung, dan perangkat Elektronik lainnya.
13. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah.
(2) Kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud ayat (1) meliputi :
    a. penetapan ruang lingkup;
    b. penetapan penanggung jawab;
    c. perencanaan;
    d. dukungan pengoperasian;
    e. evaluasi kinerja; dan
    f. perbaikan berkelanjutan terhadap keamanan informasi.
(3) Ketentuan lain untuk mendukung kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) dapat menerapkan pengendalian teknis keamanan yang meliputi :
    a. manajemen risiko;
    b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
    c. pengelolaan pihak ketiga.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Pasal 3

(1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf a meliputi:
    a. data dan informasi SPBE;
    b. aplikasi SPBE; dan
    c. aset infrastruktur SPBE.
(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Daerah yang harus diamankan dalam SPBE.

Pasal 4

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf b dilaksanakan oleh Bupati.
(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
(3) Dalam melaksanakan tugas sebagai penanggung jawab keamanan SPBE, Sekretaris Daerah disebut juga koordinator SPBE.

Pasal 5

(1) Dalam melaksanakan tugas sebagai penanggung jawab keamanan SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 4 ayat (3) menetapkan pelaksana teknis Keamanan SPBE.
(2) Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. ketua tim; dan
    b. anggota tim.
(3) Ketua Tim sebagaimana dimaksud pada ayat (2) huruf a dijabat oleh pimpinan perangkat daerah yang membidangi urusan komunikasi dan informatika.
(4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh pimpinan perangkat daerah lainnya yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di Daerah.

Pasal 6

(1) Ketua tim sebagaimana dimaksud dalam pasal 5 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah yang meliputi:
    a. menetapkan prosedur pengendalian keamanan informasi SPBE Pemerintah Daerah;
    b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di lingkungan Pemerintah Daerah;
    c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundangundangan;
    d. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
    e. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen kelangsungan bisnis dan perencanaan pemulihan bencana; dan
    f. melaporkan pelaksanaan manajemen keamanan informasi SPBE pada koordinator SPBE.
(2) Anggota tim sebagaimana dimaksud dalam Pasal 5 ayat (2) huruf b mempunyai tugas:
    a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada perangkat daerah;
    b. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan;
    c. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen business continuity dan disaster recovery plans; dan
    d. berkoordinasi dengan ketua tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 7

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

Pasal 8

(1) Program kerja Keamanan SPBE sebagaimana dimaksud dalam pasal 7 ayat (2) huruf a paling sedikit meliputi:
    a. edukasi kesadaran Keamanan SPBE;
    b. penilaian kerentanan Keamanan SPBE;
    c. peningkatan Keamanan SPBE;
    d. penanganan insiden Keamanan SPBE; dan
    e. audit Keamanan SPBE.
(2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud dalam pasal 7 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 9

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf d dilakukan oleh koordinator SPBE.
(2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
    a. sumber daya manusia Keamanan SPBE;
    b. teknologi keamanan SPBE; dan
    c. anggaran keamanan SPBE.
(3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen keamanan informasi SPBE diberikan alokasi sumber daya yang sesuai.

Pasal 10

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam pasal 9 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:
    a. keamanan TIK; dan
    b. keamanan aplikasi.
(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus adanya dukungan kegiatan:
    a. pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi dan TIK; dan/atau
    b. bimbingan teknis mengenai standar teknis dan prosedur Keamanan SPBE.
(3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia Keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan SPBE.
(4) Teknologi keamanan informasi sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap perangkat daerah.
(5) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 11

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf e dilakukan oleh koordinator SPBE.
(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan keamanan SPBE di lingkungan Pemerintah Daerah.
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
    a. menganalisis efektifitas pelaksanaan Keamanan SPBE; atau
    b. mendukung dan merealisasikan program audit Keamanan SPBE.
(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Pasal 12

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

BAB III
PENGENDALIAN TEKNIS KEAMANAN

Pasal 13

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf a dilakukan oleh setiap perangkat daerah.
(2) Manajemen risiko sebagaimana dimaksud pada ayat (1) paling sedikit menyusun daftar risiko dengan ketentuan subtansi meliputi:
    a. inventarisasi aset SPBE;
    b. identifikasi ancaman dan kerentanan keamanan terhadap aset SPBE;
    c. penilaian risiko keamanan terhadap aset SPBE;
    d. penentuan prioritas risiko;
    e. analisa dampak jika terjadi risiko;
    f. analisa kontrol keamanan yang bisa diterapkan; dan/atau
    g. rekomendasi kontrol keamanan.
(3) Prosedur pelaksanaan manajemen risiko mengacu sesuai dengan ketentuan peraturan perundangundangan.

Pasal 14

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf b ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.
(2) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah dengan cakupan aspek, meliputi :
    a. keamanan perangkat teknologi informasi komunikasi;
    b. keamanan jaringan;
    c. keamanan pusat data;
    d. keamanan perangkat end point;
    e. keamanan remote working;
    f. keamanan penyimpanan elektronik;

g. pengelolaan akses kontrol;
h. pengendalian keamanan dari ancaman virus dan malware;
i. persayaratan keamanan terkait pembangunan dan pengembangan aplikasi SPBE;
j. pengelolaan aset;
k. keamanan migrasi data;
l. konfigurasi perangkat IT Security;
m. perlindungan data pribadi;
n. keamanan komunikasi;
o. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
p. pengendalian keamanan informasi terhadap pihak ketiga;
q. penerapan kriptografi;
r. penanganan insiden keamanan informasi;
s. kelangsungan bisnis atau layanan TIK;
t. perencanaan pemulihan bencana terhadap layanan;
u. audit internal keamanan SPBE; dan/atau
v. aspek prosedur pengendalian keamanan informasi SPBE lainnya.

(3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk keputusan bupati atau surat edaran sekretaris daerah atau kebijakan teknis lainnya.

Pasal 15

(1) Setiap perangkat daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 14 ayat (3).
(2) Setiap perangkat daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian keamanan informasi SPBE.

Pasal 16

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf c dilakukan oleh setiap perangkat daerah.
(2) Perangkat daerah harus memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan.
(3) Perangkat daerah harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
(4) Perangkat daerah harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama dengan pihak ketiga.
(5) Perangkat daerah harus membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
KETENTUAN PENUTUP

Pasal 17

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Puruk Cahu
pada tanggal 19 Maret 2025

BUPATI MURUNG RAYA,

ttd

HERIYUS

Diundangkan di Puruk Cahu
pada tanggal 19 Maret 2025

SEKRETARIS DAERAH
KABUPATEN MURUNG RAYA,

ttd

HERMON

BERITA DAERAH KABUPATEN MURUNG RAYA TAHUN 2025 NOMOR 227.

SALINAN SESUAI DENGAN ASLINYA
Ditandatangani Secara Elektronik Oleh :
Kepala Bagian Hukum Sekretariat Daerah
Kabupaten Murung Raya,

RHONI KLAWA TUMON, S.H., M.H.