

Indikator 8 (evaluasi spbe 2024)

Indikator 8. Tingkat Kematangan Kebijakan Internal Manajemen Keamanan Informasi KABUPATEN MURUNG RAYA SUDAH MENCAPAI TINGKAT 3

Tingkat	Kriteria	Capaian Tahun 2023	Capaian Tahun 2024
1	Konsep kebijakan internal terkait Manajemen Keamanan Informasi belum atau telah tersedia.		
2	Kebijakan internal terkait Manajemen Keamanan Informasi telah ditetapkan. Kondisi: Kebijakan internal terkait Manajemen Keamanan Informasi belum mengatur secara lengkap mengenai cakupan Manajemen Keamanan Informasi (penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap Keamanan Informasi).		

Tingkat	Kriteria	Capaian Tahun 2023	Capaian Tahun 2024
3	Kriteria tingkat 2 telah terpenuhi dan kebijakan internal terkait Manajemen Keamanan Informasi mengatur seluruh cakupan Manajemen Keamanan Informasi secara lengkap (penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap Keamanan Informasi).	?	?
4	Kriteria tingkat 3 telah terpenuhi, dan kebijakan internal terkait Manajemen Keamanan Informasi telah mengatur penerapan untuk seluruh unit kerja/perangkat daerah di Instansi Pusat/Pemerintah Daerah. Selain itu, kebijakan internal terkait Manajemen Keamanan Informasi telah direviu dan dievaluasi secara periodik.		
5	Kriteria tingkat 4 telah terpenuhi serta hasil reviu dan evaluasi kebijakan internal terkait Manajemen Keamanan Informasi telah ditindaklanjuti dengan kebijakan baru.		

Data Dukung

Tingkat 1

Konsep kebijakan Terkait Manajemen Keamanan Informasi Sudah Tersedia

Tingkat 2

Kebijakan Terkait Manajemen Keamanan Informasi Sudah Tersedia dan sudah di tetapkan

Tingkat 3

Kebijakan Terkait Manajemen Keamanan Informasi Sudah Tersedia dan sudah di tetapkan dan mengatur cakupan Manajemen Keamanan Informasi secara lengkap pada Pasal 24, 25, 26 dan Pasal 34 Perbub SPBE Kabupaten Murung Raya

Pasal 24,25,26

Bagian Kedelapan Keamanan SPBE

Pasal 24

- (1) Keamanan SPBE sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf h ditujukan untuk melindungi aset Data dan Informasi, Infrastruktur SPBE, dan Aplikasi SPBE dari pihak yang tidak bertanggung jawab.

- (2) Keamanan SPBE sebagaimana dimaksud pada ayat (1) meliputi penjaminan terhadap:
 - a. kerahasiaan;
 - b. keutuhan;
 - c. ketersediaan; dan
 - d. kenirsangkalan.
- (3) Penjaminan kerahasiaan sebagaimana dimaksud pada ayat (2) huruf a dilakukan melalui penetapan klasifikasi keamanan, pembatasan akses, dan pengendalian keamanan lainnya.
- (4) Penjaminan keutuhan sebagaimana dimaksud pada ayat (2) huruf b dilakukan melalui pendeteksian modifikasi.
- (5) Penjaminan ketersediaan sebagaimana dimaksud pada ayat (2) huruf c dilakukan melalui penyediaan mekanisme verifikasi dan validasi.
- (6) Penjaminan kenirsangkalan sebagaimana dimaksud pada ayat (2) huruf d dilakukan melalui penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital.
- (7) Kepala Dinas menetapkan standar operasional prosedur dalam penerapan keamanan SPBE di daerah sesuai dengan ketentuan yang ditetapkan oleh Badan Siber Sandi Negara.

Pasal 25

- (1) Setiap data dan informasi yang dikelola oleh PD wajib dilakukan *backup* secara terpusat dan berkala sesuai dengan frekuensi dan tingkat keamanan data dan informasi.
- (2) Dinas melakukan pengujian secara teratur terhadap mekanisme *backup* dan *restore* data dan informasi untuk memastikan integritas dan validitas prosedur.
- (3) Tata cara *backup* dan *restore* data dan informasi ditetapkan oleh Kepala Dinas.
- (4) Dalam rangka memastikan keamanan data dan informasi, 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 SPBE.
- (5) Manajemen keamanan informasi dilaksanakan berdasarkan pedoman manajemen keamanan informasi SPBE yang ditetapkan oleh Badan Siber Sandi Negara.

Pasal 26

- (1) Dalam memastikan keamanan Infrastruktur SPBE, dilakukan audit keamanan Infrastruktur SPBE.
- (2) Audit keamanan Infrastruktur SPBE dilaksanakan minimal 1 (satu) kali dalam setahun oleh Dinas dengan berdasarkan standar dan tata cara pelaksanaan audit keamanan infrastruktur SPBE yang ditetapkan oleh Badan Siber Sandi Negara.

Pasal 27

- (1) Dalam rangka memastikan keamanan Aplikasi SPBE, dilakukan audit keamanan Aplikasi SPBE.
- (2) Audit keamanan Aplikasi SPBE, terdiri atas:
 - a. audit aplikasi sejenis Aplikasi Umum;
 - b. audit Aplikasi Khusus;
- (3) Audit aplikasi sejenis dilaksanakan dalam 1 (satu) tahun sekali oleh Dinas dengan berpedoman pada standar dan tata cara pelaksanaan audit keamanan Aplikasi SPBE yang ditetapkan oleh Badan Siber Sandi Negara.
- (4) Audit keamanan Aplikasi Khusus dilaksanakan dalam 2 (dua) tahun sekali oleh Dinas dengan berpedoman pada standar dan tata cara pelaksanaan audit keamanan Aplikasi SPBE yang ditetapkan oleh Badan Siber Sandi Negara.

Pasal 28

- (1) Kepala Dinas melakukan evaluasi terhadap pelaksanaan keamanan SPBE setiap 1 (satu) tahun sekali.
- (2) Tata cara pelaksanaan evaluasi keamanan SPBE ditetapkan oleh Kepala Dinas.

PASAL 34

Bagian Kedua
Manajemen Keamanan Informasi

Pasal 34

- (1) Manajemen keamanan informasi sebagaimana dimaksud dalam Pasal 32 huruf b bertujuan untuk melindungi data/informasi milik Pemerintah Daerah dalam keberlangsungan SPBE serta meminimalisir kerugian akibat perilaku kriminal di dunia siber yang dilakukan oleh pihak yang tidak bertanggung jawab.
- (2) Manajemen keamanan informasi dilakukan oleh seluruh PD di daerah.
- (3) Ruang lingkup keamanan informasi sebagaimana dimaksud pada ayat (1) meliputi :
 - a. keamanan pada sistem elektronik; dan
 - b. keamanan pada transaksi elektronik
- (4) Keamanan pada sistem elektronik sebagaimana dimaksud pada ayat (3) huruf a bertujuan untuk mengatur keamanan sumberdaya teknologi informasi dan komunikasi yang tidak terbatas pada data, informasi, perangkat ataupun sumber daya manusia.

17

- (5) Keamanan pada sistem elektronik mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan dan kerugian.
- (6) Keamanan pada transaksi elektronik sebagaimana dimaksud pada ayat (3) huruf b bertujuan untuk mengatur keamanan pada setiap transaksi elektronik yang dilakukan oleh PD.
- (8) Sumber daya manusia pelaksana transaksi elektronik pada PD wajib memiliki Sertifikat Elektronik.
- (9) Dinas memonitor Sertifikat Elektronik yang digunakan oleh setiap PD.

Tautan Pendukung

1. [Tautan Menuju Ke simpan.murungrayakab.go.id Untuk Indikator 8](https://simpan.murungrayakab.go.id)
2. [Peraturan Bupati No. 12 Tahun 2023 Tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Murung Raya](#)