LAPORAN
ONLINE ASSESSMENT
INDEKS KAMI

Instansi/Perusahaan: PEMERINTAH KABUPATEN MAMUJU	**Pimpinan Unit Kerja:** Akhmad Taufiq, S.IP.,M.Si NIP. 19790102 201101 1 006
Unit Kerja: DINAS KOMUNIKASI, INFORMATIKA, DAN PERSANDIAN KABUPATEN MAMUJU	**Narasumber Instansi/Perusahaan:** 1. Ilham, S.IP NIP. 19810329 200801 1 012 2. Muliadi, S.T.,M.T. NIP. 19742104 200701 1 020 3. Yayat Permadi, S.E. NIP. 19791123 200701 1 011 4. Dewi Susanti, S.E. NIP. 19680208 200112 2 002 5. Rahmanillah, S.Sos. NIP. 19790119 200701 2 010 6. Baharuddin NIP. 19840710 201212 1 003 7. Dedi Sutarna, A.Mk. NIP. 19840215 200501 1 003 8. Hasaruddin, A.Md.Kom 9. Hasran, S.T.
Alamat: Jl. K.S.Tubun Rimuku Kecamatan Mamuju 91511 Kabupaten Mamuju Provinsi Sulawesi Barat	
Email: diskominfosandi@mamujukab. go.id	**Asesor:** 1. Jabang Aru Saputro, S.Tr.Kom NIP. 19960209 202012 1 013 2. Rosdiana Lukitawati, A.Md. NIP. 19930606 202203 2 002
Telp/Fax: 081355669579	

A. Ruang Lingkup:
   1. Instansi / Unit Kerja:
      Dinas Komunikasi, Informatika dan Persandian Kabupaten Mamuju.
   2. Fungsi Kerja:
      -

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor	Jl. K.S.Tubun Rimuku Kecamatan Mamuju 91511, Kabupaten Mamuju, Provinsi Sulawesi Barat
2	Data Center	Jl.K.S.Tubun Nomor 33, Mamuju, Provinsi Sulawesi Barat.

B. Nama /Jenis Layanan Publik:

Kartu Mamuju Keren (kmk.mamujukab.go.id)

C. Aset TI yang kritikal:

- Kartu Keluarga.
- KTP.

2. Infrastruktur Jaringan/Network:
   - Server Utama

D. DATA CENTER (DC):

☒ ADA, dalam ruangan khusus (pada lantai yang sama dengan ruang kerja)

☐ ADA, jadi satu dengan ruang kerja

☐ TIDAK ADA

E. DISASTER RECOVERY CENTER (DRC):

☒ ADA ☒ Dikelola Internal ☐ Dikelola Vendor :

☐ TIDAK ADA

Status Ketersediaan Dokumen Kerangka Kerja
Sistem Manajemen Keamanan Informasi (SMKI)

No	Nama Dokumen	Ya	Tdk	Keterangan (D: Draf, R:Rilis, T:Tersosialisasikan)
	Kebijakan, Sasaran, Rencana, Standar			
1	Kebijakan Keamanan Informasi	Ya		R
2	Organisasi, Peran dan Tanggungjawab Keamanan Informasi	Ya		R

3	Panduan Klasifikasi Informasi	Ya		R
4	Kebijakan Manajemen Risiko TIK	Ya		R
5	Kerangka Kerja Manajemen Kelangsungan Usaha (*Bussiness Continuity Management*)	Ya		R
6	Kebijakan Penggunaan Sumberdaya TIK		Tdk	-
	Prosedur/ Pedoman:			-
1	Pengendalian Dokumen		Tdk	-
2	Pengendalian Rekaman/ Catatan		Tdk	-
3	Audit Internal SMKI		Tdk	-
4	Tindakan Perbaikan & Pencegahan		Tdk	-
5	Pelabelan, Pengamanan, Pertukaran & Disposal Informasi		Tdk	-
6	Pengelolaan *Removable* Media & Disposal Media		Tdk	-
7	Pemantauan (*Monitoring*) Penggunaan Fasilitas TIK		Tdk	-
8	*User Access Management*		Tdk	-
9	*Teleworking*		Tdk	-
10	Pengendalian instalasi *software* & HAKI		Tdk	-
11	Pengelolaan Perubahan (*Change Management*) TIK		Tdk	-
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi		Tdk	-

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

Dokumen yang diperiksa:

1. Keputusan Bupati Mamuju Nomor 32 Tahun 2024 Tentang Pembentukan Tim Koordinasi Sistem Pemerintah Berbasis Elektronik Pemerintah Kabupaten Mamuju Tahun 2024;
2. Keputusan Bupati Mamuju Nomor 33 Tahun 2024 Tentang Pembentukan Tim Asesor Internal Sistem Pemerintahan Berbasis Elektronik Pemerintah Kabupaten Mamuju Tahun 2024;

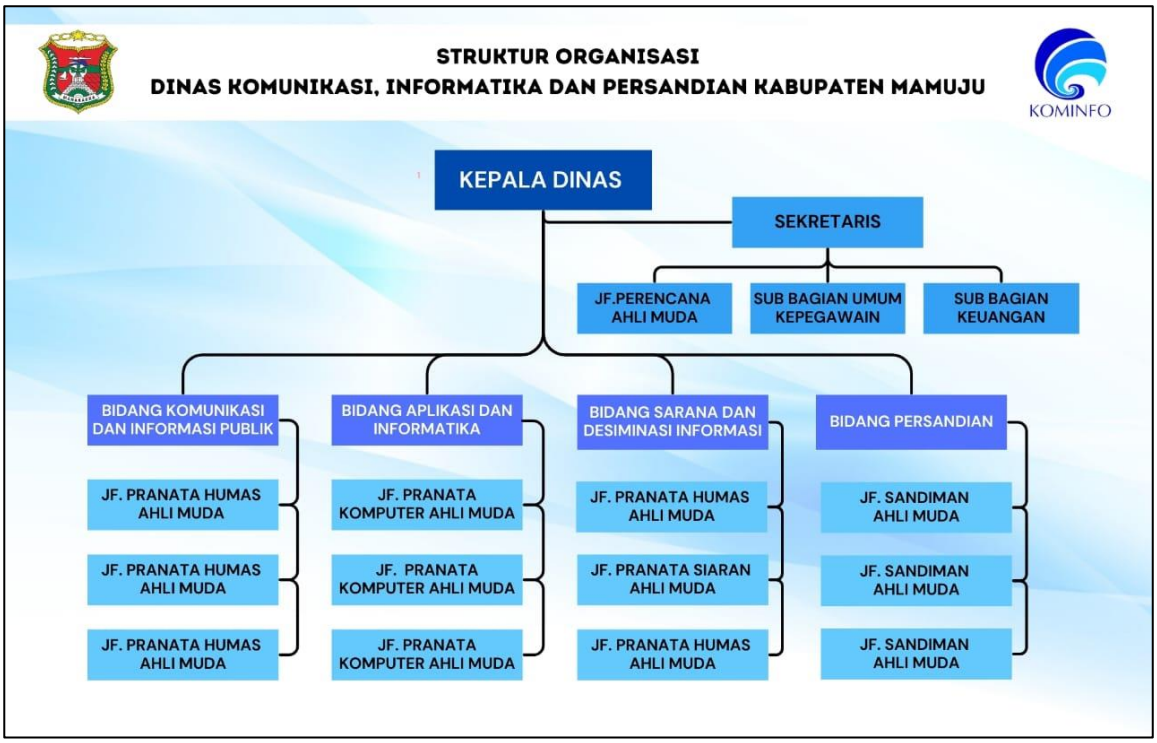
3. Keputusan Bupati Mamuju Nomor 188 Tahun 2024 Tentang Pembentukan Tim Pengelola dan Penunjukkan Pejabat Penghubung Layanan Pengaduan Masyarakat melalui Aplikasi Sp4n Lapor Pemerintah Kabupaten Mamuju Tahun Anggaran 2024;
4. Keputusan Bupati Mamuju Nomor 455 Tahun 2024 Tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Mamuju;
5. Keputusan Bupati Mamuju Nomor: 188.45/647/KPTS/XII/2022 Tentang Penyesuaian Jabatan Fungsional Hasil Penyeteraan Jabatan di Lingkungan Pemerintah Kabupaten Mamuju;
6. Keputusan Sekretaris Daerah Kabupaten Mamuju Nomor: 52 Tahun 2024 Tentang Pembentukan Tim Pengelola Website Dinas Komunikasi, Informatika dan Persandian Kabupaten Mamuju Tahun Anggaran 2024;
7. Keputusan Kepala Dinas Komunikasi, Informatika dan Persandian Kabupaten Mamuju Nomor:188.45/15/KPTS/I/2024/Diskominfosandi Tentang Pembentukan Struktur Manajemen Risiko pada Dinas Komunikasi, Informatika dan Persandian Kabupaten Mamuju;
8. Surat Sekretariat Daerah Nomor: B/100.3.4/4/2024 perihal Tindak Lanjut Surat Edaran Bupati Mamuju terkait pemulihan Aplikasi Srikandi;
9. Rencana Strategis Diskominfosandi Kabupaten Mamuju Tahun 2021-2026;
10. Buku Inventaris Aset Pemerintah Kabupaten Mamuju;
11. Rekapitulasi Data Kartu Mamuju Keren;
12. DPA Kabupaten Mamuju Tahun Anggaran 2024;
13. Berita Acara Sumpah Jabatan Sandiman Ahli Muda;
14. Analisis Jabatan Pemerintah Kabupaten Mamuju Tahun 2024;
15. Daftar OPD aktivasi TTE bulan Januari s/d September 2024;
16. Perjanjian Kerja Sama antara Pemerintah Daerah Kabupaten Mamuju dengan BSRE tentang Pemanfaatan Sertifikat Elektronik pada Sistem Elektronik di Lingkungan Pemerintah Daerah Kabupaten Mamuju;
17. SKP Sandiman Ahli Muda;
18. IKU Diskominfosandi Kabupaten Mamuju;
19. *Screenshot* Fortinet Firewall;
20. *Screenshot setting port rule* mikrotik;
21. *Screenshot* upaya akses yg masuk dalam log mikrotik;

Berdasarkan verifikasi terhadap dokumen dan wawancara terhadap narasumber instansi/lembaga disimpulkan sebagai berikut :

I. KONDISI UMUM:

1. Struktur organisasi satuan kerja dalam ruang lingkup

   Adapun struktur Diskominfo Kabupaten Mamuju adalah sebagai berikut:



2. SDM pengelola terdiri dari:

No	Status Kepegawaian	Jumlah	Prosentase
1	ASN	30	**100%**
2	PTT	0	**0%**
Jumlah			**100%**

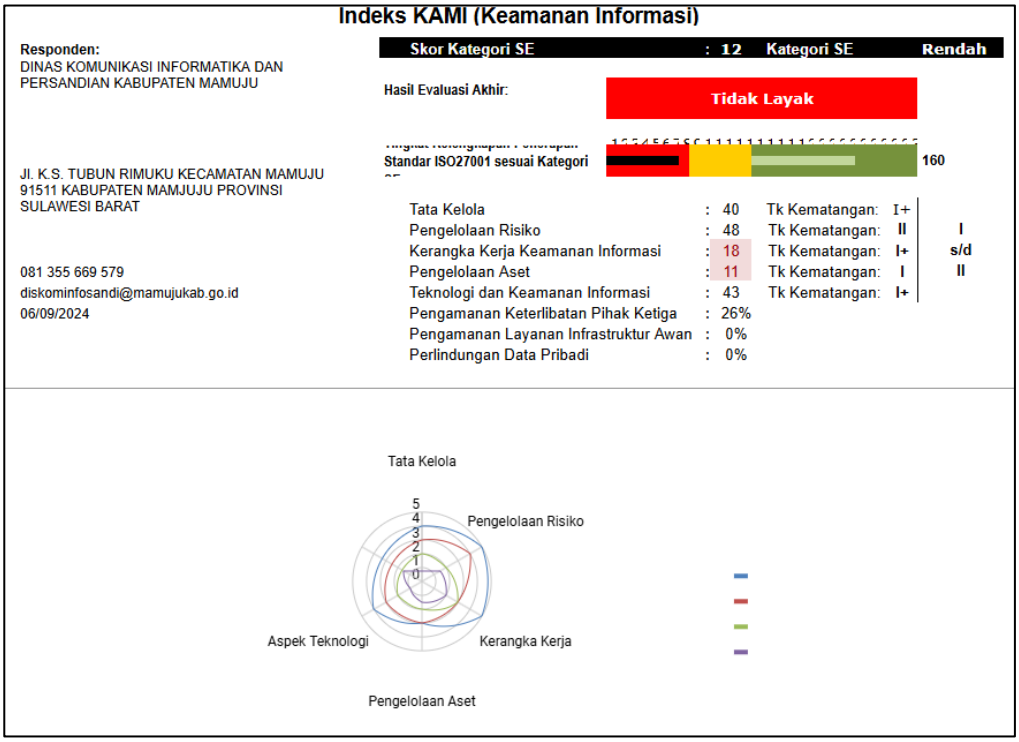
3. Berdasarkan verifikasi terhadap hasil *Self Assessment* isian *file* Indeks KAMI diperoleh hasil sebagai berikut:

   Penilaian Mandiri Indeks KAMI dilakukan dengan ruang lingkup Ruang Server (jaringan) dan Sistem Informasi/website yang dikelola oleh Dinas Komunikasi, Informatika dan Persandian Kabupaten Mamuju dengan kategori RENDAH dan hasil evaluasi akhir Tidak Layak dengan total nilai sementara adalah 160. Berdasarkan hasil verifikasi, maka diperoleh penilaian sistem elektronik untuk Aplikasi **Kartu Mamuju Keren** dengan kategori **TINGGI** dan hasil hasil evaluasi akhir **Tidak Layak** dengan total nilai **101.**

Catatan:

Pada tahun 2024 ini merupakan pertama kali Dinas Komunikasi, Informatika dan Persandian Kabupaten Mamuju melakukan verifikasi oleh Tim BSSN dalam penilaian mandiri Indeks KAMI, sehingga sesuai mekanisme kebijakan yang ada untuk pelaksanaan kegiatan verifikasi adalah dengan melakukan pengecekan keseluruhan kelengkapan kebijakan dan/atau prosedur dan penerapan dokumen kebijakan dan/atau prosedur pada area Kategori SE, Tata Kelola, Pengelolaan Risiko, Aset, Teknologi dan Keamanan Informasi serta Suplemen. Pada pelaksanaan verifikasi, Tim Asesor berupaya untuk membantu dan mengarahkan Dinas Komunikasi, Informatika dan Persandian Kabupaten Mamuju untuk dapat memperbaiki dan meningkatkan implementasi Keamanan Informasi sesuai ruang lingkup melalui penyiapan data dukung/ *evidence* berikut penerapan dan perbaikannya secara berkelanjutan dalam rangka meningkatkan proses penerapan Sistem Manajemen Keamanan Informasi yang langsung berdampak pada meningkatnya fungsi Persandian di Kabupaten Mamuju secara lebih optimal.

Total Score Sebelum Verifikasi: 160 (ref. file Indeks KAMI pra Verifikasi)



Indeks KAMI (Keamanan Informasi)

Responden:
DINAS KOMUNIKASI INFORMATIKA DAN PERSANDIAN KABUPATEN MAMUJU

Jl. K.S. TUBUN RIMUKU KECAMATAN MAMUJU 91511 KABUPATEN MAMJUJU PROVINSI SULAWESI BARAT

081 355 669 579
diskominfosandi@mamujukab.go.id
06/09/2024

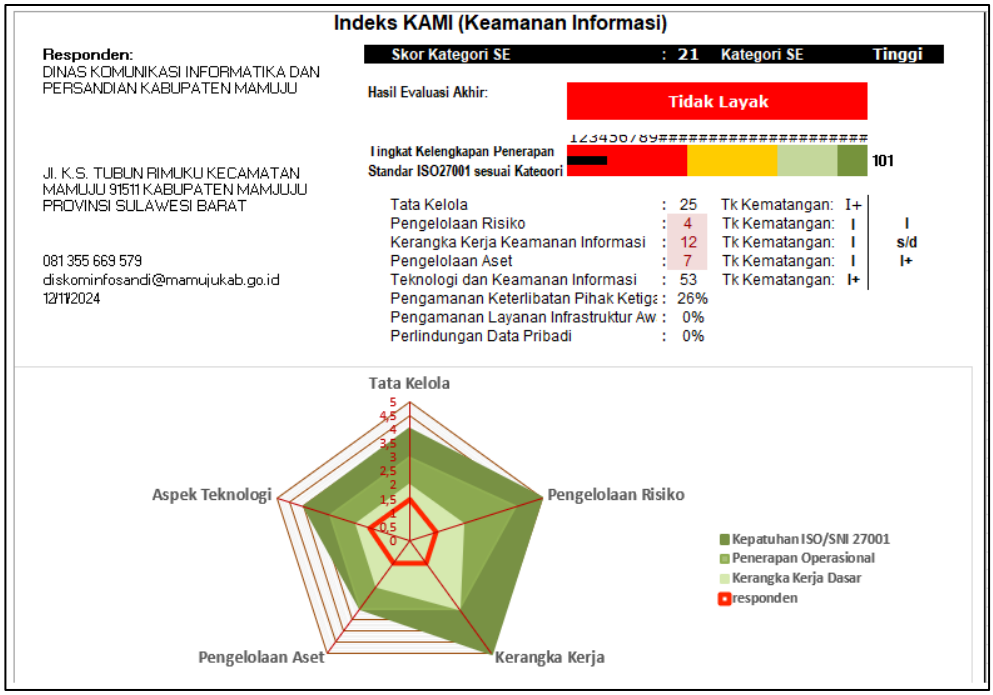
Skor Kategori SE	: 12	Kategori SE	Rendah

Hasil Evaluasi Akhir: Tidak Layak

Standar ISO27001 sesuai Kategori 160

Tata Kelola	: 40	Tk Kematangan:	I+	
Pengelolaan Risiko	: 48	Tk Kematangan:	II	I
Kerangka Kerja Keamanan Informasi	: 18	Tk Kematangan:	I+	s/d
Pengelolaan Aset	: 11	Tk Kematangan:	I	II
Teknologi dan Keamanan Informasi	: 43	Tk Kematangan:	I+	
Pengamanan Keterlibatan Pihak Ketiga	: 26%			
Pengamanan Layanan Infrastruktur Awan	: 0%			
Perlindungan Data Pribadi	: 0%			

Total Score Setelah Verifikasi: 101 (ref. file Indeks KAMI pasca Verifikasi)



II. ASPEK TATA KELOLA:

A. Kekuatan/Kematangan

1. Diskominfosandi Kabupaten Mamuju telah secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi, namun belum memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya.
2. Diskominfosandi Kabupaten Mamuju sudah menetapkan fungsi yang secara spesifik keseluruhannya mempunyai tugas dan tanggungjawab dalam mengelola dan implementasi program keamanan informasi dan memastikan kepatuhan.
3. Pejabat/petugas pelaksana informasi Diskominfosandi Kabupaten Mamuju telah memiliki wewenang yang sesuai untuk menjamin keseluruhan kepatuhan tehadap program keamanan informasi.
4. Penanggungjawab pelaksana pengamanan informasi di Diskominfosandi Kabupaten Mamuju sudah diberikan alokasi sumber daya namun baru sebagian belum secara keseluruhan demi mengelola dan menjamin kepatuhan program keamanan informasi.
5. Peran pelaksana pengamana informasi yang ada di Diskominfosandi Kabupaten Mamuju telah mencakup sebagian keperluan yang dipetakan termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan.
6. Sebagian pelaksana pengamanan informasi di Diskominfosandi Kabupaten Mamuju memiliki kompetensi dan keahlian sesuai persyaratan yang berlaku.

7. Diskominfosandi Kabupaten Mamuju telah menerapkan sosialisasi dan peningkatan pemahaman untuk keamanan informasi bagi sebagian pihak terkait.
8. Diskominfosandi Kabupaten Mamuju menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi.
9. Diskominfosandi Kabupaten Mamuju telah mendefinisikan metrik, parameter dan proses pengukuran kinerja bagi sebagian dalam pengelolaan keamanan informasi.
10. Diskominfosandi Kabupaten Mamuju sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat dan petugas) pelaksana.
11. Diskominfosandi Kabupaten Mamuju sudah mengintegrasikan sebagian keperluan/persyaratan keamanan informasi dalam proses kerja yang ada.

B. Kelemahan/Kekurangan

1. Diskominfosandi Kabupaten Mamuju belum menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelola keamanan informasi.
2. Diskominfosandi Kabupaten Mamuju belum mendefinisikan secara keseluruhan persyaratan/standar kompeteni dan keahlian pelaksana pengelola keamanan informasi.
3. Diskominfosandi Kabupaten Mamuju belum memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*bussiness continuity* dan *disaster recovery plans*).
4. Kondisi dan permasalahan keamanan informasi di Diskominfosandi Kabupaten Mamuju belum menjadi konsiderans penuh dari proses pengambilan keputusan strategis.
5. Diskominfosandi Kabupaten Mamuju belum menerapkan target dan sasaran pengelolaan keamanan informasi untuk seluruh area relevan, mengevaluasi capaian secara rutin dan menerapkan langkah perbaikan untuk mencapai sasaran yang ada termasuk laporan status kepada pimpinan.
6. Tanggungjawab pengelola keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal untuk identifikasi persyaratan/kebutuhan pengamanan belum ditetapkan Diskominfosandi Kabupaten Mamuju dalam menyelesaikan permasalahan yang ada.
7. Penanggungjawab pengelola keamanan informasi belum melaporkan kondisi, kinerja dan kepatuhan program keamanan informasi pada pimpinan secara rutin dan resmi.
8. Diskominfosandi Kabupaten Mamuju belum mengidentifikasi legislasi, perangkat hukum dan standar lain terkait keamanan informasi.
9. Diskominfosandi Kabupaten Mamuju belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (perdata dan pidana).

III. ASPEK RISIKO:

A. Kekuatan/Kematangan

1. Diskominfosandi Kabupaten Mamuju sudah sebagian menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi hingga ke tingkat pimpinan.

B. Kelemahan/Kekurangan

1. Belum adanya dokumentasi secara resmi terkait program kerja pengelolaan risiko keamanan informasi di Diskominfosandi Kabupaten Mamuju.
2. Kerangka kerja pengelolaan risiko belum mencakup definisi dam hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian di Diskominfosandi Kabupaten Mamuju.
3. Ambang batas tingkat risiko yang dapat diterima belum ditetapkan oleh Pimpinan Diskominfosandi Kabupaten Mamuju dalam rangka evaluasi terhadap tingkatan risiko yang dianalisa.
4. Dalam proses pengelolaan manajemen risiko, Diskominfosandi Kabupaten Mamuju belum terdapat pendefinisian mengenai kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
5. Diskominfosandi Kabupaten Mamuju telah mengidentifikasi ancaman dan kelemahan terkait aset informasi terutama untuk setiap aset utama ke dalam form *risk register* (daftar risiko).
6. Diskominfosandi Kabupaten Mamuju belum menetapkan kerugian terkait hilangnya/terganggunya fungsi aset utama dalam form *risk register* (daftar risiko).
7. Diskominfosandi Kabupaten Mamuju tidak menjalankan analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada.
8. Status penyelesaian langkah mitigasi risiko tidak dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya.
9. Diskominfosandi Kabupaten Mamuju belum menyusun langkah mitigasi dan penanggulangan risiko ke dalam *risk treatment plan.*
10. Diskominfosandi Kabupaten Mamuju telah menyusun langkah mitigasi sesuai tingkat prioritas dengan target penyelesaian dan penanggungjawabnya, dengan memastikan efektifitas pengguna sumber daya yang dapat menurunkan tingkat ke ambang batas yang bisa diterima.
11. Belum terdapat proses evaluasi yang obyektif/terukur terhadap penyelesaian langkah mitigasi yang telah diterapkan untuk memastikan konsistensi dan efektifitasnya.

12. Profil risiko berikut bentuk mitigasinya tidak secara berkala dikaji ulang dalam rangka memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru.
13. Kerangka kerja pengelolaan risiko tidak dikaji untuk memastikan/meningkatkan efektifitasnya.
14. Pengelolaan risiko belum menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan.

IV. ASPEK KERANGKA KERJA:

A. Kekuatan/Kematangan
   1. Kebijakan dan prosedur yang diperlukan terkait keamanan informasi sebagian sudah disusun dan dituliskan dengan jelas, termasuk peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya.
   2. Strategi penerapan keamanan informasi direalisasikan sebagai pelaksanaan program kerja Diskominfosandi Kabupaten Mamuju.
   3. Rencana dan program peningkatan keamanan informasi untuk jangka menengah/Panjang (1-3-5) tahun sudah direalisasikan secara konsisten.

B. Kelemahan/Kekurangan
   1. Kebijakan keamanan informasi belum ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oelh pihak yang membutuhkannya.
   2. Belum tersedia mekanisme untuk mengelola sebagian dokumen kebijakan dan prosedur keamana informasi.
   3. Belum tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi dan sasaran) untuk mengkomunikasikan kebijakan keamanan informasi kepada semua pihak termasuk pihak ketiga.
   4. Belum adanya keseluruhan kebijakan dan prosedur keamanan informasi yang merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi.
   5. Belum tersedia sebagian proses untuk identifikasi kondisi yang membahayakan keamanan informasi dan menetapkan sebagai insiden keamanan informasi untuk ditindaklanjuti.
   6. Belum terdapat aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI dan tata tertib penggunaan dan pengamanan aset maupun layanan TIK dalam kontrak pihak ketiga.
   7. Konsekwensi dari pelanggaran kebijakan keamanan informasi belum didefinisikan, dikomunikasikan dan ditegakkan.

8. Diskominfosandi Kabupaten Mamuju belum memiliki prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi.
9. Diskominfosandi Kabupaten Mamuju belum membahas aspek keamanan informsi dalam manajemen proyek.
10. Diskominfosandi Kabupaten Mamuju belum menerapkan proses untuk evaluasi risiko terkait rencana pembelian sistem baru dan menanggulangi permasalahan yang muncul.
11. Diskominfosandi Kabupaten Mamuju belum menerapkan proses pengembangan sistem yang aman (*secure SDLC*) dengan menggunakan prinsip sesuai standar platform teknologi yang digunakan.
12. Penerapan suatu sistem mengakibatkan timbulnya risiko dengan proses sebagai penanggulangan belum diterapkan pengamanan baru dan jadwal penyelesaian.
13. Belum tersedia kerangka kerja pengelolaan perencanaan layanan TIK (*business continuity plan*) namun belum dengan jadwal uji coba.
14. Seluruh kebijakan dan prosedur keamanan informasi belum dievaluasi kelayakan secara berkala.
15. Diskominfosandi Kabupaten Mamuju belum mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko.
16. Diskominfosandi Kabupaten Mamuju belum memiliki strategi penggunaan teknologi keamanan informasi yang penerapannya sesuai dengan perubahan profil risiko.
17. Diskominfosandi Kabupaten Mamuju belum menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggung jawab untuk monitor rilis *security patch* baru serta pelaporan.
18. Diskominfosandi Kabupaten Mamuju belum mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim dalam perencanaan pemulihan bencana terhadap layanan TIK (*business continuity planning*).
19. Belum dilakukan uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sesuai jadwal.
20. Belum dilakukan evaluasi dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) untuk menerapkan langkah perbaikan.
21. Diskominfosandi Kabupaten Mamuju belum memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi.
22. Belum dilakukan audit internal untuk evaluasi tingkat kepatuhan, konsistensi, dan efektivitas penerapan keamanan informasi.
23. Belum dilakukan evaluasi untuk identifikasi langkah pembenahan dan pencegahan serta belum dilakukan pelaporan kepada pimpinan organisasi.
24. Belum dilakukan analisa untuk menilai aspek finansial dalam keperluan untuk merevisi kebijakan dan prosedur yang berlaku.

25. Belum dilakukan pengujian dan evaluasi secara periodik tingkat/status kepatuhan program keamanan informasi.

V. ASPEK PENGELOLAAN ASET:

A. Kekuatan/Kematangan

1. Daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi sudah didokumentasikan namun belum seluruhnya tercatat secara lengkap, akurat dan terpelihara (termasuk kepemilikan aset).
2. Beberapa penerapan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko sudah tersedia. Hal ini seperti:
   a. Terdapat beberapa sebagian ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya.

B. Kelemahan/Kekurangan

1. Belum tersedianya definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku.
2. Belum ada proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi dan keperluan pengamanannya, syarat penghancuran data yang sudah tidak diperlukan, serta definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi namun belum ada dokumentasinya.
3. Belum tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut.
4. Diskominfosandi Kabupaten Mamuju tidak memiliki proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) namun tidak semuanya tercatat secara sistematis.
5. Diskominfosandi Kabupaten Mamuju tidak melakukan proses pengelolaan konfigurasi namun belum diterapkan secara konsisten.
6. Belum tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
7. Beberapa penerapan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko belum tersedia. Hal ini seperti:
   a. Tidak terdapat definisi tanggung jawab pengamanan informasi secara individual untuk personil di Diskominfosandi Kabupaten Mamuju.
   b. Diskominfosandi Kabupaten Mamuju tidak memiliki tata tertib penggunaan komputer, email, internet dan intranet.
   c. Belum ditetapkannya tata tertib pengamanan dan penggunaan aset Diskominfosandi Kabupaten Mamuju terkait HAKI.

d. Belum ada aturan terkait instalasi piranti lunak di aset TI milik Diskominfosandi Kabupaten Mamuju.
e. Tidak terdapat peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.
f. Tidak ada proses mengenai pengelolaan identitas elektronik dan proses otentikasi (*username* dan *password*) termasuk kebijakan terhadap pelanggarannya.
g. Tidak terdapat persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi.
h. Tidak ada ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data.
i. Tidak terdapat proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi.
j. Masih belum ada prosedur *back-up* dan uji coba pengembalian data (*restore*) dan belum secara berkala dilakukan.
k. Belum adanya ketentuan mengenai pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya.
l. Tidak terdapat proses pengecekan latar belakang SDM.
m. Tidak terdapat proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
n. Tidak terdapat prosedur penghancuran data/aset yang sudah tidak diperlukan.
o. Tidak terdapat prosedur kajian penggunaaan akses (*user access review*) dan hak akses (*user access right)*
p. Tidak ada prosedur untuk user mutasi/keluar atau tenaga kontrak yang habis masa kerjanya.

8. Belum tersedia daftar data/informasi yang di back-up namun belum dengan laporan analisa kepatuhan terhadap prosedur back-up.
9. Belum terdokumentasinya daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanannya yang sesuai dengan klasifikasinya.
10. Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan belum ditetapkan dan didokumentasikan.

Beberapa kelemahan dalam pengamanan fisik antara lain:

11. Pengamanan fasilitas fisik (lokasi kerja) masih belum diterapkan sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang.
12. Belum ada proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik.

13. Belum ada infrastruktur komputasi telah terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya.
14. Tidak terdapat infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan Listrik atau dampak dari petir.
15. Belum tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi, dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris) serta pengamanannya yang melibatkan pihak ketiga.
16. Belum adanya proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untukmenempatkan aset informasi penting.
17. Belum adanya mekanisme pengamanan dalam pengiriman aset informasi(perangkat dan dokumen) yang melibatkan pihak ketiga.
18. Belum adanya proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Diskominfosandi Kabupaten Mamuju.
19. Belum tersedia peraturan pengamanan perangkat komputasi milik Diskominfo KSB apabila digunakan di luar lokasi kerja resmi.
20. Diskominfosandi Kabupaten Mamuju belum menyesuaikan konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung.
21. Belum tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi di dalamnya.

VI. ASPEK TEKNOLOGI:

A. Kekuatan/Kematangan

1. Layanan TIK (beberapa sistem komputer) di Diskominfosandi Kabupaten Mamuju menggunakan internet yang dilindungi dengan lebih dari 1 lapis pengamanan.
2. Jaringan internet telah dilakukan segmentasi sesuai dengan kebutuhan, hal ini diimplementasikan dengan pembatasan akses jaringan, memudahkan pemantauan dan identifikasi jika terjadi adanya insiden keamanan siber.
3. Tersedia konfigurasi standar untuk keamanan sistem bagi sebagian aset jaringan, sistem, dan aplikasi.
4. Beberapa jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk identifikasi kemungkinan celah kelemahan.
5. Beberapa infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup sesuai kebutuhan yang ada.

6. Setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log, dan diimplementasikan kepada seluruh sistem elektronik.
7. Akses yang digunakan untuk mengelola sistem (administrasi sistem) sudah menggunakan bentuk pengamanan khusus yang berlapis.
8. Diskominfosandi Kabupaten Mamuju telah menerapkan enkripsi untuk melindungi beberapa aset informasi sesuai kebijakan pengelolaan yang ada.
9. Sebagian log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya.
10. Diskominfosandi Kabupaten Mamuju menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan yang tidak resmi.
11. Sistem operasi untuk setiap perangkat *dekstop* dan *server* dimutakhirkan dengan versi terkini.
12. Setiap *desktop* dan *server* telah dilindungi dari penyerangan virus (*malware*).
13. Terdapat hasil rekaman yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin.
14. Terdapat laporan penyerangan virus/*malware* yang ditindaklanjuti dan diselesaikan.
15. Keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada.

B. Kelemahan/Kekurangan

1. Diskominfosandi Kabupaten Mamuju telah menganalisa kepatuhan penerapan konfigurasi standar namun belum secara rutin.
2. Keseluruhan infrastruktur jaringan, sistem dan aplikasi belum dirancang untuk memastikan ketersediaan sesuai kebutuhan yang ada.
3. Diskominfosandi Kabupaten Mamuju belum menerapkan lingkungan pengembangan dan uji coba yang diamankan sesuai dengan standar platform teknologi yang ada.
4. Diskominfosandi Kabupaten Mamuju belum melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin.
5. Diskominfosandi Kabupaten Mamuju belum menerapkan standar dalam menggunakan enkripsi serta menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) dan siklus penggunaan.
6. Seluruh sistem dan aplikasi belum secara otomatis mendukung penerapan penggantian *password* secara otomatis, menonaktifkan *password* serta mengatur kompleksitas dan penggunaan kembali *password* lama.
7. Akses yang digunakan dalam mengelola sistem belum menggunakan bentuk pengamanan khusus berlapis.

8. Sistem dan aplikasi yang digunakan di Diskominfosandi Kabupaten Mamuju belum menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeout, lockout* setelah kegagalan login dan penarikan akses.
16. Diskominfosandi Kabupaten Mamuju belum menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Diskominfosandi Kabupaten Mamuju.
17. Aplikasi yang ada belum memiliki spesifikasi dan fungsi keamanan yang diverifikasi pada saat proses pengembangan dan uji coba.

VII. REKOMENDASI

Fondasi keberhasilan dalam penyelenggaraan pengamanan informasi terdiri dari 3 (tiga) faktor, yaitu **Sumber Daya Manusia** yang cukup dalam segi kuantitas dan kualitas, **Implementasi Teknologi** yang mendukung pengamanan, serta perlu adanya **Komitmen Pimpinan Berupa Dukungan Anggaran dan Penetapan Kebijakan/Regulasi** yang dapat menjadi payung dalam pelaksanaan pengamanan informasi. Berdasarkan ketentuan tersebut diperlukan penguatan pada 3 (tiga) faktor tersebut untuk mendukung pelaksanaan pengamanan informasi, meminimalisir risiko kegagalan pengamanan informasi, dan memastikan keamanan layanan SPBE Pemerintah Kabupaten Mamuju berjalan dengan maksimal.

Berikut ini rekomendasi yang disusun sesuai segementasi SDM, Kebijakan/Dukungan Pimpinan serta Penerapan Teknologi berdasarkan prioritas yang perlu segera ditindaklanjuti dalam rangka penerapan keamanan informasi SPBE di Pemerintah Kabupaten Mamuju:

1. **Sumber Daya Manusia (SDM)**, terdapat beberapa hal yang harus segera ditindaklanjuti, di antaranya :

   a. Perlu dilakukan peningkatan kuantitas dan kualitas SDM keamanan informasi di Diskominfosandi Kabupaten Mamuju, karena berdasarkan assessmen yang telah dilakukan, Diskominfosandi Kabupaten Mamuju dinilai masih memiliki keterbatasan SDM spesialis keamanan informasi khususnya untuk melakukan kegiatan terkait identifikasi kerentanan, peningkatan keamanan, monitoring Mamujuan siber, *threat intelligence* dan kegiatan manajemen penanganan insiden terhadap seluruh aplikasi SPBE di Pemkab Mamuju.

   b. Sebagaimana poin a di atas, perlu dilakukan identifikasi kebutuhan kapasitas ideal personil keamanan informasi disesuaikan dengan beban kerja organisasi khususnya di bidang keamanan informasi atau keamanan SPBE. Selanjutnya perlu adanya spesialisasi SDM, spesialisasi tersebut dapat dikategorikan sebagai berikut:

      1) SDM khusus menangani Keamanan Aplikasi;
      2) SDM khusus menangani Keamanan Jaringan; dan
      3) SDM khusus menangani Keamanan Pusat Data.

c. Diskominfosandi Kabupaten Mamuju diharapkan dapat melakukan koordinasi dan konsultasi dengan BKD dan/atau BSSN terkait dengan pengajuan SDM (Pemenuhan kebutuhan jabatan fungsional sandiman dan manggala informatika) yang disesuaikan dengan ruang lingkup tugas yang dapat mengawaki keseluruhan pelaksanaan tugas dan fungsi dalam penyelenggaraan keamanan informasi.

d. SDM yang sudah ada perlu dilakukan pengembangan pengetahuan dan keahlian secara kontinu melalui *workshop*, bimbingan teknis, pelatihan, *sharing knowledge*, dan peningkatan keahlian khususnya spesifik terkait secure SDLC atau *Secure Programming*.

e. Selain itu terkait program edukasi dan *awareness* terhadap pimpinan dan seluruh pegawai Pemkab Mamuju maupun masyarakat pada umumnya, diperlukan kegiatan yang dapat meningkatkan pemahaman akan pentingnya keamanan informasi dan pelindungan data pribadi di era siber saat ini, dimana bahaya kejahatan siber dapat merugikan berbagai pihak baik dari sisi finansial, layanan operasional, hingga korban jiwa.

f. Terkait poin e di atas kegiatan yang dapat dilakukan oleh Diskominfosandi Kabupaten Mamuju adalah literasi keamanan informasi secara masif dan terukur, baik melalui media *online* (seperti webinar keamanan informasi, workshop keamanan informasi, mem-*posting* himbauan keamanan informasi di media sosial, maupun media elektronik lainnya) dan secara *offline* (seperti sosialisasi keamanan informasi baik kepada PD s.d. kecamatan, sektor pendidikan, dan sektor lainnya).

2. **Pada faktor regulasi/ kebijakan** serta komitmen dan dukungan Pimpinan terdapat beberapa hal yang harus segera ditindaklanjuti, di antaranya:

a. Dalam proses implementasi Sistem Manajemen Keamanan Informasi pada Sistem Pemerintahan Berbasis Elektronik (SMKI SPBE) pada Pemkab Mamuju, diperlukan dukungan dari Pimpinan berkaitan dengan peningkatan anggaran untuk mendukung pelaksanaan program keamanan SPBE, pemenuhan dan pengembangan SDM serta peningkatan perangkat teknologi keamanan.

b. Menetapkan Kebijakan Internal Manajemen Keamanan Informasi SPBE atau Kebijakan SMKI dalam bentuk Peraturan Kepala Daerah sebagai pedoman legal dan resmi dalam mendukung pelaksanaan program keamanan SPBE di lingkungan Pemkab Mamuju.

c. Selanjutnya menyusun turunan Kebijakan Internal Manajemen Keamanan Informasi SPBE atau Kebijakan SMKI baik berupa prosedur teknis maupun surat edaran yang akan digunakan sebagai panduan dalam implementasi keamanan informasi secara menyeluruh dengan melibatkan/ mengkomunikasikan kebijakan terkait pada pihak internal maupun eksternal sehingga akan lebih merasakan manfaat dengan

keberadaan Diskominfosandi Kabupaten Mamuju sebagai *lead* dan penanggung jawab pelaksanaan keamanan informasi di Pemkab Mamuju.

d. Selanjutnya meningkatkan pengelolaan dokumen kebijakan dan prosedur keamanan informasi dengan cara menyusun daftar induk dokumen kebijakan dan prosedur keamanan informasi dan memonitor pengelolaan dokumennya pada kegiatan distribusi, penarikan dan penyimpanannya. Serta melakukan evaluasi untuk seluruh kebijakan dan prosedur keamanan informasi. Selain itu, juga secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif.

e. Perlu adanya penyusunan, pelaksanaan dan pengelolaan *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP) sebagai upaya dalam menjaga kelangsungan TIK dan menjadi bagian rencana tindakan (*response plan*) dalam mengantisipasi terjadinya bencana. Dalam penyusunannya, dapat menggunakan standar SNI ISO 22301 maupun *best practice* lainnya. Penyusunan DRP memerlukan beberapa proses seperti pencatatan seluruh aset (layanan TI) yang dimiliki oleh organisasi, pencatatan risiko-risiko negatif yang berpotensi menjadi sebuah bencana bagi organisasi, serta analisis dampak bisnis sebagai pertimbangan keputusan dalam penyusunan dokumen DRP. Selanjutnya DRP akan menjadi panduan yang dipersiapkan Diskominfosandi Kabupaten Mamuju dalam menghadapi bencana sehingga proses bisnis/layanan tetap dilanjutkan dan dapat menjaga konsistensi data apabila akibat bencana berdampak pada gangguan maupun kerusakan terhadap layanan teknologi informasi.

f. Perlu melaksanakan kegiatan monitoring keamanan informasi pada seluruh aset SPBE secara *realtime* dan terlapor kepada pimpinan dalam bentuk tinjauan manajemen secara rutin.

g. Perlu melaksanakan kegiatan audit internal keamanan SPBE dengan berkolaborasi dengan unit kerja Inspektorat. Selanjutnya menetapkan tim audit internal untuk bersama mempelajari untuk meningkatkan pemahaman terhadap Perpres No.95 tahun 2018 tentang SPBE khususnya pada pasal 55 s.d pasal 58 tentang audit TIK SPBE, Pemerkominfo No.16 tahun 2022 tentang Kebijakan Umum Audit TIK SPBE serta peraturan BSSN nomor 4 tahun 2021 khususnya pasal yang mengatur terkait standar teknis keamanan SPBE yang menjadi objek yang akan di audit terkait keamanan aplikasi dan infrastruktur SPBE.

h. Selanjutnya, tidak kalah pentingnya adalah urgensi penerapan manajemen risiko sebagai salah satu bagian dari tugas dan fungsi serta menjadi budaya keamanan informasi yang tidak terpisahkan dalam bisnis proses organisasi dengan tujuan untuk mengurangi dampak yang merugikan dari adanya suatu kejadian yang membahayakan atau insiden keamanan informasi. Manajemen risiko akan membantu mengawal pencapaian tujuan Diskominfosandi Kabupaten Mamuju tanpa harus menanggung kerugian yang tidak diinginkan baik secara personil maupun organisasi. Penerapannya dilakukan dengan ketentuan sebagai berikut:

1) Menjadikan manajemen risiko menjadi bagian dari tugas dan fungsi di Diskominfosandi Kabupaten Mamuju.
2) Identifikasi risiko dilakukan berdasarkan kritikalitas aset untuk setiap kategori aset yaitu Perangkat Keras, Perangkat Lunak, Sistem Aplikasi, Jaringan Komunikasi, Personil (pegawai tetap dan non tetap serta pihak ketiga yang terlibat), Data/Informasi, dan Sarana Pendukung yang digunakan dalam penyelenggaraan layanan TI oleh Diskominfosandi Kabupaten Mamuju.
3) Melakukan review dan evaluasi secara berkala terhadap risk register yang sudah disusun pada tahun 2024.
4) Perlu penyusunan Kartu Inventaris pada Aset TI dan Aset Informasi terkait pemilik dan pengelola aset, misal terjadi kerusakan atau kehilangan aset, maka perlu penanggung jawab dan penerapan kebijakan manajemen risiko yang akan diimplementasikan.
5) Melakukan monitoring terhadap rencana mitigasi yang telah ditetapkan dari risk register secara periodik atau menyusun *risk treatment plan* sebagai dasar dalam memetakan kelemahan dan mengetahui kekurangan sehingga dapat meminimalisir adanya eksploitasi dari pihak - pihak tertentu (ancaman yang timbul).

3. Pemenuhan dan Peningkatan Teknologi terdapat beberapa hal yang harus segera ditindaklanjuti, di antaranya:

a. Peningkatan dan perawatan perangkat teknologi keamanan informasi pada infrastruktur dan aplikasi SPBE untuk memperkuat ketahanan dari Mamujuan siber, di antaranya implementasi IDS/IPS, Security Information and Event Management (SIEM), Antivirus/Anti-*Malware*, ataupun penambahan dukungan teknologi Next Generation Firewall.
b. Perlu dengan segera menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya sesuai dengan kebijakan. Sehingga setiap pegawai di lingkungan Pemkab Mamuju dapat menggunakan dan mengelola kunci enkripsi dengan baik.

c. Perlu menetapkan dengan segera pada sistem dan aplikasi agar dapat secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menonaktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama. Hal ini sejalan dan mendukung dengan poin di atas, sehingga keamanan pada people, sistem dan aplikasi dapat meningkat.

d. Evaluasi dan implementasi teknologi keamanan informasi pada perangkat TI (PC, Laptop, dan Smartphone) pada seluruh pegawai Diskominfo pada khususnya dan sebagian besar pegawai Diskominfosandi Kabupaten Mamuju pada umumnya, untuk dapat menerapkan sistem operasi versi terkini dan antivirus/antimalware dan Diskominfosandi Kabupaten Mamuju memastikan penerapannya apakah efektif dalam meminimalisir ancaman atau risiko dari Mamujuan virus dan malware.

e. Memperhatikan selalu lisensi yang terupdate terhadap perangkat keamanan teknologi informasi.

f. Perlu menganalisa kepatuhan penerapan konfigurasi standar secara rutin, dan melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin.

VIII. PENUTUP

Demikian Laporan *Online Assessment* Indeks KAMI Pemerintah Daerah Kabupaten Mamuju Tahun 2024 ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan informasi Pemerintah Daerah Kabupaten Mamuju. Laporan *Online Assessment* Indeks KAMI Pemerintah Daerah Kabupaten Mamuju Tahun 2024 ini disampaikan kepada:

1. Direktur Keamanan Siber dan Sandi Pemerintah Daerah
2. Bupati Kabupaten Mamuju;
3. Sekretaris Daerah Kabupaten Mamuju.

Depok, 09 Desember 2024

Kepala Bidang Persandian
Dinas Komunikasi Informatika, Persandian
Dan Statistik Kabupaten Mamuju

Ditandatangani secara elektronik oleh :
KEPALA BIDANG PERSANDIAN
Ilham, S.IP
NIP : 19810329 200801 1 012

Asesor Indeks KAMI BSSN

Ditandatangani secara elektronik oleh:
SANDIMAN AHLI PERTAMA
Jabang Aru Saputro, S.Tr. Kom
Penata Muda (III/a)

Dokumen Ini ditandatangani secara elektronik oleh:
Pengolah Data Keamanan Siber dan Sandi
ROSDIANA LUKITAWATI, A Md
Pengatur (II/c)

Mengetahui,
Dinas Komunikasi Informatika, Persandian Dan Statistik
Kabupaten Mamuju

Ditandatangani secara elektronik oleh :
Plt. KEPALA DINAS KOMINFOSANDI MAMUJU
Akhmad Taufiq, S.Ip., M.Si.
NIP : 19790102 201101 1 006