RAHASIA

LAPORAN ONLINE ASSESSMENT INDEKS KEAMANAN INFORMASI 5.0

DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN MAMUJU

TAHUN 2025

Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
Deputi Bidang Keamanan Siber dan Sandi dan Pembangunan Manusia
Badan Siber dan Sandi Negara

RAHASIA

LAPORAN *ONLINE* ASSESSMENT
INDEKS KAMI 5.0

Instansi: Pemerintah Kabupaten Mamuju	**Pimpinan Unit Kerja:** Akhmad Taufiq Sip. Msi NIP. 19790102 201101 1 006
Unit Kerja: Dinas Komunikasi, Informatika, Statistika dan Persandian Kabupaten Mamuju	**Narasumber Instansi/ Asesi:** 1. Rahmanillah S. Sos 2. Muliadi, ST. MT. 3. Dewi Susanti SE 4. Yahya Permadi. SE 5. Andi Mulai Sulfiani 6. Baharuddin 7. Dedy Sutarna A. Mk, 8. Saparuddin Abd. Gani 9. Ade Sulhaj Anirah,S.Ak 10. Nur Alif
Alamat: Jl. KS Tubun No. 33, Kelurahan Rimuku, Kecamatan *Mamuju*, Kabupaten *Mamuju*, Sulawesi Barat 91511	
Email: diskominfosip@mamujukab.go.id	**Tim Asesor:** 1. Roybafih Sukisman S.Tr.TP. NIP. 19960503 201812 1 001 2. Siti Maryanti, A.Md. NIP. 19950504 202203 2 006
Telp: - **Fax:** -	

A. Ruang Lingkup:

1. Instansi/ Unit Kerja:

   Dinas Komunikasi, Informatika, Statistika dan Persandian Kabupaten Mamuju

2. Fungsi Kerja:

   Sesuai dengan Peraturan Bupati Nomor 36 Tahun 2016 tentang Kedudukan, Fungsi, Susunan Organisasi, dan Tata Kerja Perangkat Daerah Dinas Kominfo dan Persandian disebutkan merupakan unsur pelaksana urusan pemerintahan bidang komunikasi dan informatika.

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor	Jl. KS Tubun No. 33, Kelurahan Rimuku, Kecamatan *Mamuju*, Kabupaten *Mamuju*, Sulawesi Barat 91511
2	Data Center	Jl. KS Tubun No. 33, Kelurahan Rimuku, Kecamatan *Mamuju*, Kabupaten *Mamuju*, Sulawesi Barat 91511
3	DRC	-

4. Waktu Pelaksanaan:

   Kegiatan dilaksanakan secara daring selama 3 hari kerja, mulai Senin s.d Rabu, 8 – 10 Desember 2025.

B. Ruang Lingkup:

- Penyelenggara Sistem Elektronik : Dinas Komunikasi, Informatika, Statistika dan Persandian Kabupaten Mamuju
- Sistem Elektronik (SE) : Aplikasi Kehadiran Berbasis Kinerja Si Keren (https://sikeren.mamujukab.go.id)

C. Aset TI Kritikal:

1. Informasi/ Data:
   - Data Pribadi Pengguna (NIP, email, kepegawaian);
   - Data kredensial Pengguna (username, password).
2. Aplikasi/ Sistem Elektronik Utama/ Kritikal:
   - Absensi Kehadiran (https://sikeren.mamujukab.go.id)
3. Server Utama/ Kritikal:
   - Lenovo sr550, OS Debian 12, AaPanel
4. Infrastruktur Jaringan (ISP):
   - Utama : IconPlus
   - Cadangan : Icon Plus

D. Data Center (DC):

☒ Ada, dalam ruangan khusus (Ruang server dikelola internal organisasi)

☐ Ada, jadi satu dengan ruangan kerja
☐ Tidak Ada

E. Disaster Revovery Center (DRC):

☐ Ada ☒ Dikelola Internal ☒ Dikelola Vendor:

☒ Tidak Ada

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

Dokumen dan Bukti-bukti (Rekaman/ Arsip) Penerapan SMKI yang diperiksa:

1. Keputusan Bupati Mamuju Nomor 200 Tahun 2025 tentang Manajemen keamanan Informasi Sistem pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Mamuju.
2. Keputusan Kepala Dinas Komunikasi, Informatika dan Persandian Kabupaten Mamuju Nomor 43 Tahun 2024 tentang Pembentukan Struktur Manajemen Risiko Tahun 2025 pada Dinas Komunikasi, Informatika dan Persandoan Kabupaten Mamuju.
3. Formulir Penetapan Konteks Manajemen Risiko.
4. Daftar Identifikasi Risiko
5. Daftar Analisis Risiko
6. Daftar Risiko Prioritas Unit Kerja
7. Daftar Rencanan Tindak Pengendaian
8. Daftar Analisis Akar Masalah

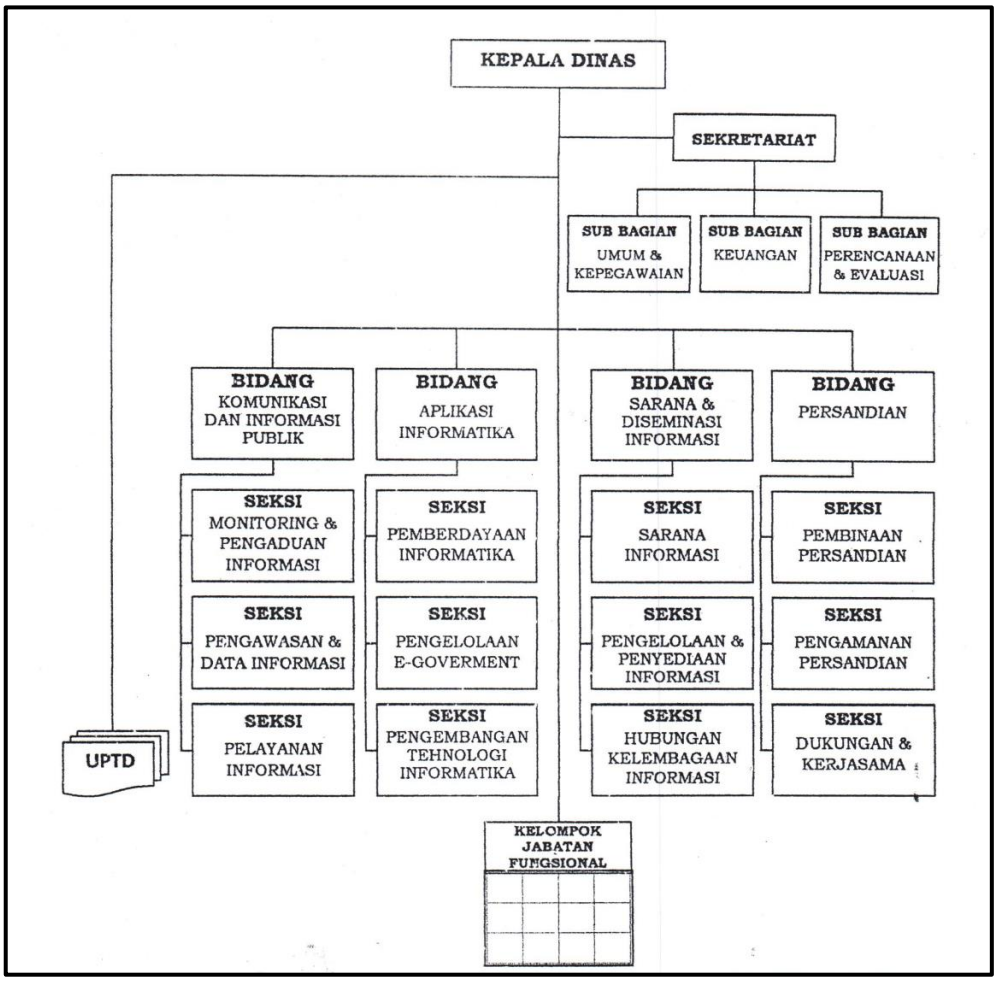
9. DPA Tahun 2022 Pengadaan Hardware dan Software Aplikasi Absensi
10. Laporan Kegiatan Tahun 2024 Bidang Sarana dan Diseminasi Informasi
11. SOP Penanganan Insiden Siber
12. SOP Pengamanan Jaringan
13. SOP Pengelolaan Keamanan Siber
14. Daftar Aset berdasrka Kartu Inventaris Barang (KIB)
15. Laporan Hasil Assesmen Penerapan Keamanan Informasi
16. Laporan Kegiatan Penyelenggara Persandian Untuk Pengamanan Informasi Pemerintah Daerah Kabupaten/ Kota (Indeks KAMI September 2025)
17. Laporan Kegiatan Operasional Email Sanapati Bulan September 2025 Sub Program Kegiatan Penetapan Hubungan Komunikasi Sandi Antar Perangkat Daerah Kabupaten/Kota – Bidang Persandian
18. Laporan Kegiatan Operasional Email Tanda Tangan Eletronik Tahun 2025 Program Kegiatan Penyelenggaraan Persandian Untuk Pengamanan Informasi Pemerintah Daerah Kabupaten/Kota - Bidang Persandian
19. Kebijakan Pelindungan Data Pribadi Nomor 15 Tahun 2025 tanggal 23 Oktober 2025
20. DPA Maintenance Aplikasi Presensi
21. Daftar Inventarisir Aset TIK
22. PKS Pemerintah Kabupaten Mamuju - BSSN
23. Laporan Pemeliharaan Server Diskominfosip Mamuju Juli - Agt
24. Laporan Pemeliharaan Server Diskominfosip Mamuju Maret-April 2025
25. Laporan Kegiatan Sosialisasi Penggunaan Aplikasi E-Kinerja dan Aplikasi Presensi
26. Surat Edaran Sikeren
27. Surat Pengusulan Operator Absen Si Keren
28. Dokumen Panduan Dan Syarat Pengelolaan Aset Diskominfosip 2025
29. Telaan Staf Usulan Peralatan Server
30. Alat Pengaman Ruang Server
31. Topologi Jaringan
32. Surat Tugas Tim PDP
33. Sosialisasi PDP Kominfosip Kab Mamuju
34. BKPP - Berita Acara Rekon Ta. 2023
35. SK SMKI 2025
36. Sk Tim Asessor Internal SPBE 2025
37. Sk Tim Koordinasi SPBE 2025
38. Peta Jabatan
39. Sk Jabatan Nutrisionis Marhayati
40. SK Adminsuper Admin Kabupaten
41. Evaluasi Renja 2025 Triwulan I
42. SK TTIS
43. Screenshot Aplikasi Pengguna Pribadi
44. Screenshot Aplikasi TTE Pengguna
45. Laporan Bulanan TTE Aktivasi Sep 2025
46. Laporan Kegiatan Operasional Email Sanapati Bulan September 2025
47. Laporan Monev Ururan Persandian 2024
48. Ekin Sep 2025
49. SK IKU
50. Perbup SOTK No. 74 Tahun 2019
51. SK Manajemen Resiko Tahun 2025
52. Laporan Tahunan 2024 Bidang Sarana Dan Diseminasi Informasi

53. Laporan TTE Bulan Sep 2025
54. SOP Absensi
55. SOP TTE Kab. Mamuju
56. Router
57. Versi OS Server
58. Versi Antivirus
59. Router NTP
60. Rekap Pengguna TTE 2024
61. SOP Pembaruan SE Kab. Mamuju
62. SOP Penerbitan Kab. Mamuju

Berdasarkan verifikasi Asesor BSSN terhadap dokumen, wawancara, dan observasi dengan Asesi Diskominfo Kabupaten Mamuju disimpulkan sebagai berikut:

I. KONDISI UMUM:

1. Diskominfosip Kabupaten Mamuju merupakan unsur pelaksana otonomi daerah yang dipimpin oleh seorang kepala dinas dan memiliki struktur sebagai berikut:
   a. sekretariat;
   b. bidang komunikasi dan informasi publik;
   c. bidang aplikasi informatika;
   d. bidang sarana dan diseminasi informasi;
   e. bidang persandian;
   f. UPTD; dan
   g. kelompok jabatan fungsional.



Gambar 1. Struktur Organisasi Diskominfosip Kabupaten Mamuju

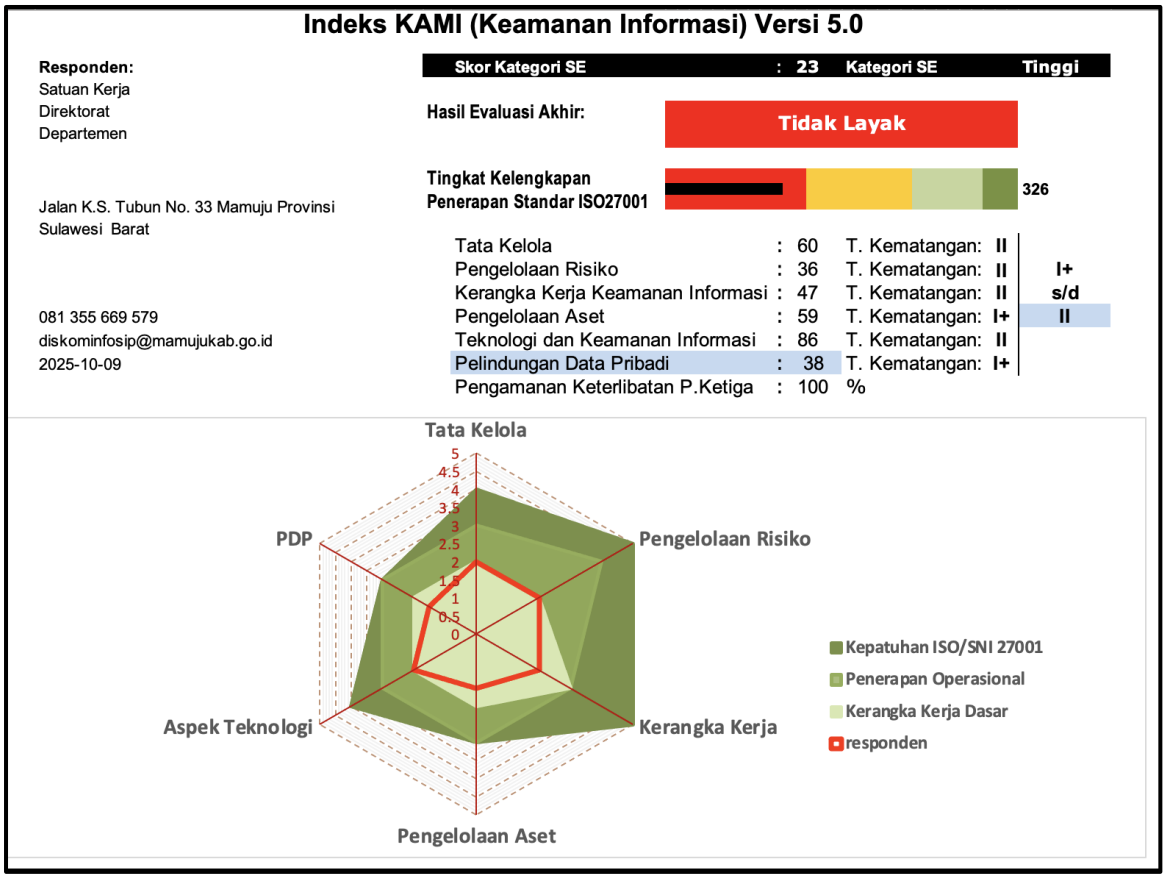
2. Komposisi Sumber Daya Manusia di Diskominfosip Kabupaten Mamuju sejumlah 41 orang, dengan rincian sebagai berikut.

Sandiman	:	3 orang	ASN	:	31 orang
Manggala Informatika	:	-	Non-ASN	:	10 orang
Pranata Komputer	:	4 orang			

3. Berdasarkan verifikasi terhadap hasil penilaian mandiri dari Indeks Keamanan Informasi (Indeks KAMI) versi 5.0, diperoleh hasil sebagai berikut:

Diskominfo Kabupaten Mamuju mengelola SE **Si Keren** yang merupakan aplikasi pelayanan absensi untuk ASN di lingkungan Pemerintah Daerah Kabupaten Mamuju dengan kategori **TINGGI (Skor Kategorisasi SE: 23)** dan hasil evaluasi akhir pada level **TIDAK LAYAK** dengan tingkat kelengkapan penerapan standar SNI/ISO 27001 sesuai kategori pada skor **326**.

Dashboard Hasil Verifikasi Indeks KAMI versi 5.0



Gambar 2 Dashboard Indeks KAMI versi 5.0

II. ASPEK TATA KELOLA

A. <u>Kekuatan/ Kematangan</u>

1. Pimpinan dari Organisasi sudah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen diantaranya sudah adanya penetapan kebijakan keamanan informasi. Salah satu hal ini adalah dengan dibuktikan terkait program keamanan informasi dalam ITSP atau inisiatif-inisiatif proyek terkait.

2. Fungsi yang mengelola dan mengimplementasikan program keamanan informasi sudah berjalan dalam organisasi namun belum spesifik diuraikan peranannya yang spesifik terkait keamanan informasi.
3. Pejabat/petugas pelaksana pengamanan informasi yang sudah ditunjuk sudah menjalankan fungsi keamanan informasi namun kewenangan yang sejalan dengan kepentingan dalam keamanan informasi belum diformalkan dalam suatu dokumentasi yang formal.
4. Alokasi sumber daya terkait pelaksanaan program keamanan informasi sudah direncanakan dan namun belum sepenuhnya disediakan dalam rangka memastikan pengelolaan keamanan informasi telah memadai dan dipastikan kepatuhannya.
5. Peran fungsi pelaksana pengamanan informasi belum semuanya telah dipetakan pada kebutuhan program keamanan informasi secara lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan.
6. Organisasi sudah mendefinisikan persyaratan/standar kompetensi dan keahlian khususnya terkait pelaksana pengelolaan keamanan informasi.
7. Semua pelaksana pengamanan informasi yang terlibat di Organisasi belum semuanya memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku khususnya terkait aspek kontrol teknis dan operasional keamanan informasi.
8. Manajemen Organisasi dan fungsi pengelola keamanan informasi sudah merencanakan dan menerapkan program sosialisasi dan peningkatan pemahaman terhadap keamanan informasi melalui beberapa media (seperti email, poster, training,dll) dan dievaluasi hasil penerapannya untuk memastikan kepatuhannya bagi semua pihak yang terkait.
9. Organisasi sudah menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi dengan merencanakan secara berkala minimal setiap tahun dalam rangka memastikan kebutuhan penerapan kontrol keamanan informasi telah terpenuhi.
10. Seluruh persyaratan keamanan informasi yang terdapat dalam standar yang berlaku sudah terintegrasi ke dalam proses kerja yang ada sehingga diharapkan kontrol keamanan informasi dapat berjalan secara konsisten.
11. Organisasi belum semuanya mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku.
12. Tanggung jawab pengelolaan keamanan informasi yang didelegasikan kepada fungsi pengelola keamanan informasi sudah mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, dan untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerja sama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada.
13. Koordinasi antara fungsi pengelola keamanan informasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak masih belum konsisten dan terlaksana secara memadai.
14. Fungsi pengelola keamanan informasi sudah secara rutin melaporkan kepada manajemen mengenai kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi harus secara rutin.
15. Setiap permasalahan keamanan informasi yang terjadi di Organisasi sudah menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis dalam melakukan tindakan perbaikan yang diperlukan untuk meningkatkan efektivitas pelaksanaan kontrol keamanan informasi.
16. Organisasi belum menerapkan sepenuhnya terkait program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya.

17. Metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi (misal: mekanisme, waktu pengukuran, pelaksananya) sudah didefinisikan namun belum dijabarkan secara lengkap. Sudah ada evaluasi pemantauannya perlu dilakukan namun belum diukur efektivitasnya dan tidak ada eskalasi pelaporan kepada manajemen untuk memastikan efektivitas dari proses pengelolaan program dan kontrol keamanan informasi yang diterapkan.
18. Manajemen Organisasi sudah mendefinisikan dan menerapkan program penilaian kinerja terkait penerapan proses keamanan informasi bagi individu (pejabat & petugas) pelaksananya sebagai bagian dari proses evaluasi tingkat pemahaman individu tersebut terhadap pengelolaan keamanan informasi di organisasi.
19. Target dan sasaran pengelolaan keamanan informasi sudah didefinisikan dan diformulasikan, serta dilakukan evaluasi dan mengkaji hasil pencapaiannya secara rutin. Laporan hasil evaluasi terhadap target dan sasaran tersebut telah dilaporkan statusnya kepada pimpinan organisasi.
20. Manajemen Organisasi belum sepenuhnya mendelegasikan pihak terkait / unit kerja / fungsi pengelola keamanan informasi pada internal Organisasi untuk mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi serta dipastikan untuk dipatuhi dengan menganalisis tingkat kepatuhannya..

B. Kelemahan/ Kekurangan

1. Organisasi belum menetapkan tanggung jawab untuk merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) termasuk pengalokasian kebutuhan sumber daya dan proses yang diperlukan dalam rangka menjamin kelangsungan bisnis ketika terjadi kondisi darurat.
2. Manajemen Organisasi belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

III. ASPEK RISIKO

A. Kekuatan/ Kematangan

1. Program kerja pengelolaan risiko keamanan informasi sudah terdokumentasi dan diterapkan secara memadai dalam proses penilaian dan evaluasi risiko.
2. Manajemen Organisasi sudah menentukan penanggung jawab proses manajemen risiko yang mempunyai wewenang dalam eskalasi terhadap pelaporan hasil analisa risiko keamanan informasi sampai ke tingkat pimpinan organisasi namun belum terdokumentasi secara resmi.
3. Ambang batas tingkat risiko yang dapat diterima ditetapkan oleh manajemen Organisasi dalam rangka melakukan evaluasi terhadap tingkatan risiko yang dianalisa tidak secara jelas dan terdokumentasi.
4. Dalam proses pengelolaan manajemen risiko, Organisasi sudah 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. Ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi.
6. Pada proses analisa risiko sudah ditetapkan mengenai dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sesuai dengan definisi yang ada.
7. Organisasi sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi).
8. Langkah-langkah mitigasi dan penanggulangan risiko yang ada sudah disusun secara sistematis dan memadai.

9. Langkah mitigasi risiko sudah disusun sesuai dengan tingkat prioritas dan target penyelesaiannya serta penanggungjawabnya dan telah terdapat mekanisme untuk memastikan efektivitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK.

B. Kelemahan/ Kekurangan

1. Kerangka kerja pengelolaan risiko keamanan informasi belum terdokumentasi dalam dokumen metodologi manajemen risiko sehingga belum dapat digunakan secara resmi.
2. Kerangka kerja pengelolaan risiko ini belum mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian di Organisasi.
3. Status penyelesaian langkah mitigasi risiko belum dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya.
4. Belum terdapat proses evaluasi yang obyektif/terukur terhadap penyelesaian langkah mitigasi yang telah diterapkan untuk memastikan konsistensi dan efektivitasnya.
5. Profil risiko berikut bentuk mitigasinya belum secara berkala dikaji ulang dalam rangka memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru.
6. Kerangka kerja pengelolaan risiko tidak dikaji untuk memastikan/meningkatkan efektivitasnya.
7. Pengelolaan risiko belum menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan.

IV. ASPEK KERANGKA KERJA

A. Kekuatan/ Kematangan

1. Kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya
2. Kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya
3. Tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?
4. Keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan

B. Kelemahan/ Kekurangan

1. Belum menerapkan aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga
2. Belum Tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini
3. Instansi/perusahaan belum menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch,* alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya
4. Instansi/perusahaan anda belum menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul

5. Instansi/perusahaan anda belum menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan
6. Belum ada penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya
7. Belum tersedianya kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsiderans keamanan informasi termasuk penjadwalan uji cobanya
8. Belum ada perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk
9. Instansi/perusahaan belum mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi
10. Instansi/perusahaan belummempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko
11. Instansi/perusahaan belum memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)
12. Instansi/perusahaan belum 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

V. ASPEK PENGELOLAAN ASET

A. <u>Kekuatan/ Kematangan</u>

1. Tersedia daftar inventaris sebagian besar aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara (termasuk kepemilikan aset).
2. Tersedia proses pengelolaan konfigurasi, namun belum diterapkan secara konsisten.
3. Tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional, namun belum sampai tahap memutakhirkan inventaris aset informasi.
4. Tersedia tata tertib penggunaan komputer, email, internet dan intranet, serta terimplementasi secara memadai.
5. Tersedia tata tertib pengamanan dan penggunaan aset organisasi terkait HAKI, serta terimplementasi secara memadai.
6. Tersedia peraturan terkait instalasi piranti lunak di aset TI milik organisasi, dan terimplementasi secara memadai.
7. Tersedianya kebijakan pengelolaan identitas elektronik dan proses otentikasi (username & password), namun belum termasuk kebijakan terhadap pelanggarannya.
8. Memiliki/ menerapkan prosedur back-up dan uji coba pengembalian data (restore) secara berkala.
9. Organisasi sudah mengevaluasi kelaikan keamanan layanan cloud termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001.
10. Sudah menerapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, belum berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang.

11. Memiliki dan melaksanakan proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik.
12. Infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya.
13. Memiliki dan melaksanakan proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting.
14. Memiliki dan melaksanakan peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya.(misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll).

B. Kelemahan/ Kekurangan

1. Definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku dalam proses penyusunan.
2. Tersedia konsep proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi organisasi dan keperluan pengamanannya.
3. Tersedia konsep definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut.
4. Tersedia konsep proses untuk mengidentifikasi dan menginventarisir syarat retensi asset informasi sesuai dengan peraturan perundangan yang ada dan menghapusnya jika sudah melewati batas retensi tersebut.
5. Tersedia konsep proses untuk mengevaluasi kepatuhan terhadap syarat retensi dan menghapus aset informasi jika sudah melewati batas retensi tersebut.
6. Tersedia konsep proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten.
7. Tersedia konsep definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di organisasi, namun belum diimplementasikan.
8. Belum tersedia peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.
9. Belum tersedianya persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi.
10. Belum memiliki dan melaksanakan ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data.
11. Belum memiliki ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya.
12. Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi dalam proses penyusunan.
13. Belum memiliki ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya.
14. Belum memiliki proses pengecekan latar belakang SDM.
15. Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib masih dalam proses penyusunan.
16. Belum memiliki proses dan metoda untuk penghancuran informasi yang belum tidak diperlukan dan sesuai dengan klasifikasi informasi (mis: secure delete, jenis/kerapatan shredder dll),termasuk didalamnya laporan bukti penghancuran informasi.
17. Belum memiliki prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidaksesuaian (non-conformity) terhadap kebijakan yang berlaku.

18. Belum memiliki prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
19. Belum tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya.
20. Belum tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
21. Belum diterapkan proses dan metoda untuk mengaburkan data (data masking) agar hanya dapat dilihat oleh pihak yang mempunyai otoritas sesuai regulasi atau kebijakan.
22. Belum tersedia 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.
23. Organisasi belum melakukan kajian risiko terkait penggunaan layanan berbasis cloud dan menyesuaikan kebijakan keamanan informasi terkait layanan ini.
24. Organisasi belum menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud.
25. Organisasi belum menetapkan kebijakan dan menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud.
26. Organisasi belum mengkaji, menetapkan pembagian tanggung jawab keamanan informasi antara organisasi dan penyelenggara layanan cloud .
27. Organisasi belum mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud.
28. Organisasi belum mengevaluasi penyelenggara layanan cloud terkait reputasi penyelenggaranya.
29. Organisasi belum menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal organisasi.
30. Proses pelaporan insiden terkait layanan cloud sedang dalam proses penyusunan.
31. Organisasi belum memiliki kebijakan, strategi dan proses untuk mengganti layanan cloud atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut.
32. Organisasi belum memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data).
33. Infrastruktur komputasi yang terpasang belum terlindungi dari gangguan pasokan listrik atau dampak dari petir dan masih dalam proses pengadaan/ penganggaran.
34. Infrastruktur komputasi yang terpasang direncanakan dapat dipantau melalui CCTV.
35. Belum tersedia peraturan pengamanan perangkat komputasi milik organisasi apabila digunakan di luar lokasi kerja resmi (kantor).
36. Belum tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang belum ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris).
37. Konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai.
38. Belum tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
39. Proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan organisasi dalam proses penyusunan.

VI. ASPEK TEKNOLOGI

A. Kekuatan/ Kematangan

1. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan.
2. Sebagian jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian organisasi, kebutuhan aplikasi, jalur akses khusus, dll).
3. Sebagian jaringan, sistem dan aplikasi yang digunakan secara rutin maupun tidak rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi.
4. Sebagian infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada.
5. Sebagian infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada dan efektivitas keamanannya.
6. Setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log.
7. Upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log.
8. Sebagian log dianalisa untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik), namun belum secara berkala.
9. Organisasi menerapkan enkripsi untuk melindungi sebagian aset informasi penting sesuai kebijakan pengelolaan yang ada.
10. Organisasi menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya.
11. Sebagian sistem dan atau aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, menon-aktifkan password, mengatur kompleksitas/panjangnya atau penggunaan kembali password lama.
12. Sebagian akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis.
13. Sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login,dan penarikan akses.
14. Organisasi menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi.
15. Organisasi menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar organisasi.
16. Sistem operasi untuk setiap perangkat desktop dan server dimutakhirkan dengan versi terkini.
17. Setiap desktop dan server dilindungi dari penyerangan virus (malware).
18. Terdapat rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis.
19. Keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada.
20. Organisasi menerapkan kontrol akses untuk source code apliksi .

B. Kelemahan/ Kekurangan

1. Konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, dalam proses penyusunan.
2. Proses pengelolaan konfigurasi perangkat komputasi (server, perangkat jaringan, sistem operasi dan aplikasi) yang direncanakan diterapkan secara konsisten dalam proses penyusunan.
3. Perangkat komputasi terpasang tersebut direncanakan dikaji ulang secara berkala sesuai dengan konfigurasi standard untuk keamanan sistem, dipantau efektivitasnya dan dimutakhirkan/disesuaikan konfigurasinya melalui proses Manajemen Perubahan (change management).

4. Organisasi dalam proses perancangan standar dalam menggunakan enkripsi pada jaringan, sistem dan aplikasi.
5. Organisasi belum laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan/ diselesaikan, namun belum konsisten.
6. Organisasi belum menganalisa dan menetapkan website yang membahayakan organisasi atau tidak seharusnya diakses karyawan, namun belum secara rutin. Untuk selanjutnya website tersebut diblok agar tidak dapat diakses.
7. Organisasi belum menetapkan prinsip pengembangan aplikasi yang aman (secure coding) yang digunakan untuk pengembangan aplikasi secara internal (in-house) maupun yang melibatkan pihak eksternal.misal: menggunakan standard OWASP 10
8. Organisasi belum menerapkan proses perencanaan pengembangan sistem.(Dengan mempertimbangkan hasil pemrograman yang tidak baik/laik pada sistem sebelumnya, konfigurasi software development tool yang aman (secure), kontrol terhadap lingkungan pengembangan, desain arsitektur yang aman)
9. Organisasi belum menerapkan proses source code review (baik secara manual atau menggunakan piranti lunak) sebelum dijalankan di lingkungan produksi.
10. Setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan belum diverifikasi/validasi pada saat proses pengembangan dan uji coba.
11. Organisasi belum menganalisa dan memperbaiki jika ditemukenali ancaman baru (misal adanya laporan kelemahan dan/atau teknik eksploit baru) yang berdampak pada keamanan sistem aplikasi.
12. Organisasi menerapkan lingkungan pengembangan dan uji coba, namun belum diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun.
13. Organisasi belum menerapkan proses atau mekanisme untuk mencegah terungkapnya informasi sensitif ke luar dari organisasi (misal membatasi/mengkarantina lampiran email atau memblokir pengiriman dokumen/data ke luar) .
14. Organisasi belum menerapkan teknologi (DLP Data Leakage Prevention) untuk mencegah terungkapnya informasi sensitif ke luar dari organisasi.
15. Organisasi belum melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin.

VII. ASPEK PERLINDUNGAN DATA PRIBADI

A. Kekuatan/ Kematangan

1. Organisasi sudah memiliki kebijakan terkait Pelindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku.
2. Organisasi sudah menunjuk fungsi/unit Pejabat Pelindung Data Pribadi yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Pelindungan Data Pribadi.
3. Organisasi sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku.

B. Kelemahan/ Kekurangan

1. Organisasi dalam proses penyusunan dokumentasi atas jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal.

2. Organisasi proses penyusunan untuk memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan/ dimana data pribadi tersebut diperoleh.
3. Proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di organisasi dalam proses pendokumentasian/ sedang disusun.
4. Organisasi dalam proses menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan/ dipertukarkan secara ilegal atau karena insiden lain.
5. Kajian risiko keamanan pada organisasi dalam proses untuk memasukkan aspek Pelindungan Data Pribadi.
6. Mekanisme pelindungan data pribadi dalam perecanaan diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku.
7. Organisasi dalam proses untuk mendapatkan persetujuan pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut .
8. Organisasi sedang menyusun proses untuk melaporkan insiden terkait terungkapnya data pribadi.
9. Organisasi dalam penyusunan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut.
10. Organisasi sedang menyusun proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan.
11. Organisasi dalam penyusunan proses terkait periode penyimpanan data pribadi dan/ penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data.
12. Organisasi dalam penyusunan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut.
13. Organisasi dalam penyusunan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum.

VIII. REKOMENDASI

Berikut ini rekomendasi yang disusun berdasarkan prioritas yang dapat segera ditindaklanjuti dalam rangka mengoptimalkan penerapan pengamanan data dan informasi:

A. ASPEK TATA KELOLA

1. Melakukan pemetaan dan pendokumentasian peran pelaksana pengamanan informasi secara lebih komprehensif, termasuk penegasan dukungan terhadap fungsi audit internal yang independen serta penerapan segregasi kewenangan yang jelas, guna mengurangi risiko konflik kepentingan, meningkatkan akuntabilitas, dan memperkuat tata kelola keamanan informasi.
2. Menyusun dan melaksanakan program peningkatan kompetensi dan keahlian pengelolaan keamanan informasi secara terencana dan berkelanjutan, termasuk melalui pelatihan berkala dan sertifikasi yang relevan bagi pejabat serta petugas pelaksana, guna memastikan kemampuan yang memadai sesuai peran, tanggung jawab, dan tingkat risiko yang dihadapi.

B. ASPEK RISIKO

1. Menyusun, menetapkan, dan menerapkan program kerja pengelolaan risiko keamanan informasi yang terdokumentasi secara lengkap dan disahkan secara resmi, serta digunakan secara konsisten sebagai dasar identifikasi, analisis, evaluasi, dan pengendalian risiko, guna memastikan pengelolaan risiko keamanan informasi berjalan efektif dan selaras dengan tujuan organisasi.
2. Menetapkan penanggung jawab manajemen risiko keamanan informasi secara jelas dan terdokumentasi, serta membangun mekanisme eskalasi dan pelaporan status pengelolaan risiko

keamanan informasi secara berkala hingga ke tingkat pimpinan, guna memastikan pengambilan keputusan yang tepat, pengawasan yang efektif, dan akuntabilitas pengelolaan risiko.

3. Menyempurnakan kerangka kerja pengelolaan risiko keamanan informasi agar secara jelas mencakup definisi dan keterkaitan antara klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman, serta dampak kerugian terhadap organisasi, sehingga proses penilaian dan pengendalian risiko dapat dilakukan secara konsisten, terukur, dan dapat dipertanggungjawabkan.
4. Mendefinisikan dan mendokumentasikan secara jelas kepemilikan (asset owner) dan pihak pengelola (custodian) seluruh aset informasi, termasuk aset utama/penting serta proses kerja utama yang memanfaatkan aset tersebut, guna memastikan kejelasan tanggung jawab, perlindungan aset yang memadai, dan pengelolaan risiko keamanan informasi yang efektif.
5. Melaksanakan analisa atau kajian risiko keamanan informasi secara terstruktur dan terdokumentasi terhadap seluruh aset informasi, sebagai dasar dalam mengidentifikasi, menetapkan, dan memprioritaskan langkah mitigasi atau penanggulangan risiko yang selanjutnya diintegrasikan ke dalam program pengelolaan keamanan informasi.
6. Melakukan evaluasi secara berkala dan terdokumentasi terhadap penyelesaian langkah mitigasi risiko keamanan informasi melalui proses yang objektif dan terukur, guna memastikan konsistensi penerapan, efektivitas pengendalian, serta sebagai dasar perbaikan berkelanjutan dalam pengelolaan keamanan informasi.

C. ASPEK KERANGKA KERJA

1. Memastikan aspek keamanan informasi, termasuk kewajiban pelaporan insiden, perlindungan kerahasiaan informasi, Hak Kekayaan Intelektual (HAKI), tata tertib penggunaan, serta pengamanan aset dan layanan TIK, dicantumkan secara jelas dan mengikat dalam kontrak atau perjanjian kerja sama dengan pihak ketiga, guna meminimalkan risiko dan memastikan kepatuhan terhadap kebijakan keamanan informasi.
2. Menyusun, menetapkan, dan menerapkan prosedur resmi pengelolaan pengecualian terhadap penerapan keamanan informasi, termasuk mekanisme persetujuan, pencatatan, penilaian risiko, serta proses tindak lanjut atas konsekuensi yang timbul, guna memastikan pengecualian dikelola secara terkontrol, transparan, dan tidak meningkatkan risiko yang tidak dapat diterima.
3. Menyusun dan menerapkan kebijakan serta prosedur operasional pengelolaan security patch yang terdokumentasi, termasuk penetapan tanggung jawab untuk memonitor rilis patch keamanan, memastikan pemasangan tepat waktu, melakukan verifikasi keberhasilan implementasi, serta melaporkan statusnya secara berkala, guna meminimalkan kerentanan dan meningkatkan postur keamanan sistem informasi.
4. Mengintegrasikan aspek keamanan informasi secara sistematis dalam manajemen proyek sesuai dengan ruang lingkup proyek, termasuk pada tahap perencanaan, pelaksanaan, dan penutupan proyek, guna memastikan risiko keamanan informasi telah diidentifikasi, dikendalikan, dan dipertimbangkan sejak awal hingga akhir siklus proyek.
5. Menerapkan proses evaluasi risiko keamanan informasi secara terstruktur terhadap rencana pembelian atau implementasi sistem baru, termasuk mekanisme penanganan dan mitigasi atas permasalahan yang teridentifikasi, guna memastikan sistem yang diadopsi telah memenuhi persyaratan keamanan dan tidak menimbulkan risiko yang tidak dapat diterima bagi organisasi.
6. Menerapkan proses pengembangan sistem yang aman (Secure SDLC) secara konsisten dengan mengacu pada prinsip dan metode yang sesuai dengan standar platform teknologi yang digunakan, termasuk pengintegrasian aspek keamanan sejak tahap perencanaan, pengembangan, pengujian, hingga implementasi, guna mengurangi kerentanan dan memastikan keandalan serta keamanan sistem informasi.

D. ASPEK PENGELOLAAN ASET

1. Menetapkan definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku.
2. Menetapkan proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi organisasi dan keperluan pengamanannya.
3. Menetapkan definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut
4. Menetapkan proses untuk mengidentifikasi dan menginventarisir syarat retensi asset informasi sesuai dengan peraturan perundangan yang ada dan menghapusnya jika agar melewati batas retensi tersebut
5. Menetapkan proses untuk mengevaluasi kepatuhan terhadap syarat retensi dan menghapus aset informasi jika agar melewati batas retensi tersebut
6. Menetapkan proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten.
7. Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di organisasi
8. Menetapkan peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi
9. Menetapkan persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
10. Menetapkan kebijakan waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data
11. Menetapkan kebijakan pertukaran data dengan pihak eksternal dan pengamanannya
12. Menetapkan proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi
13. Menetapkan ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya
14. Menetapkan proses pengecekan latar belakang SDM
15. Menetapkan proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
16. Menetapkan proses dan metoda untuk penghancuran informasi yang agar tidak diperlukan dan sesuai dengan klasifikasi informasi (mis: secure delete, jenis/kerapatan shredder dll),Termasuk didalamnya laporan bukti penghancuran informasi .
17. Menetapkan prosedur kajian penggunaan akses (user access review) dan hak aksesnya (user access rights) berikut langkah pembenahan apabila terjadi ketidaksesuaian (non-conformity) terhadap kebijakan yang berlaku
18. Menetapkan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
19. Menetapkan daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya.
20. Menetapkan daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
21. Menetapkan proses dan metoda untuk mengaburkan data (data masking) agar hanya dapat dilihat oleh pihak yang mempunyai otoritas sesuai regulasi atau kebijakan.Mis: pengamanan data pribadi, data sensitif
22. Menetapkan 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.

23. Organisasi agar melakukan kajian risiko terkait penggunaan layanan berbasis cloud dan menyesuaikan kebijakan keamanan informasi terkait layanan ini.
24. Organisasi agar menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis cloud.
25. Organisasi agar menetapkan kebijakan dan menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan cloud.
26. Organisasi agar mengkaji, menetapkan pembagian tanggung jawab keamanan informasi antara organisasi dan penyelenggara layanan cloud .
27. Organisasi agar mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis cloud.
28. Organisasi agar mengevaluasi penyelenggara layanan cloud terkait reputasi penyelenggaranya.
29. Organisasi agar menetapkan standar keamanan teknis penggunaan layanan cloud, termasuk aspek penggunaannya oleh pengguna di internal organisasi.
30. Organisasi agar memiliki proses pelaporan insiden terkait layanan cloud.
31. Organisasi agar memiliki kebijakan, strategi dan proses untuk mengganti layanan cloud atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut.
32. Organisasi agar memiliki proses untuk menghentikan layanan cloud, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data).
33. Menetapkan perlindungan pada infrastruktur komputasi yang terpasang dari gangguan pasokan listrik atau dampak dari petir.
34. Menetapkan perlindungan pada infrastruktur komputasi yang terpasang dapat dipantau melalui CCTV .
35. Menetapkan peraturan pengamanan perangkat komputasi milik organisasi apabila digunakan di luar lokasi kerja resmi (kantor).
36. Menetapkan proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang agar ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris).
37. Konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai.
38. Tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
39. Tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan organisasi .

E. ASPEK TEKNOLOGI

1. Tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan.
2. Tersedia proses pengelolaan konfigurasi perangkat komputasi (server, perangkat jaringan, sistem operasi dan aplikasi) yang diterapkan secara konsisten.
3. Perangkat komputasi terpasang tersebut agar dikaji ulang secara berkala sesuai dengan konfigurasi standard untuk keamanan sistem, dipantau efektivitasnya dan dimutakhirkan/disesuaikan konfigurasinya melalui proses Manajemen Perubahan (change management).
4. Organisasi mempunyai standar dalam menggunakan enkripsi.
5. Adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan.

6. Organisasi secara rutin menganalisa dan menetapkan website yang membahayakan organisasi atau tidak seharusnya diakses karyawan.Untuk selanjutnya website tersebut diblok agar tidak dapat diakses.
7. Organisasi agar menetapkan prinsip pengembangan aplikasi yang aman (secure coding) yang digunakan untuk pengembangan aplikasi secara internal (in-house) maupun yang melibatkan pihak eksternal.misal: menggunakan standard OWASP 10
8. Organisasi agar menerapkan proses perencanaan pengembangan sistem.(Dengan mempertimbangkan hasil pemrograman yang tidak baik/laik pada sistem sebelumnya, konfigurasi software development tool yang aman (secure), kontrol terhadap lingkungan pengembangan, desain arsitektur yang aman)
9. Organisasi menerapkan proses source code review (baik secara manual atau menggunakan piranti lunak) sebelum dijalankan di lingkungan produksi.
10. Setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba.
11. Organisasi secara rutin menganalisa dan memperbaiki jika ditemukenali ancaman baru (misal adanya laporan kelemahan dan/atau teknik eksploit baru) yang berdampak pada keamanan sistem aplikasi.
12. Organisasi menerapkan lingkungan pengembangan dan uji coba yang agar diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun.
13. Organisasi agar menerapkan proses atau mekanisme untuk mencegah terungkapnya informasi sensitif ke luar dari organisasi (misal membatasi/mengkarantina lampiran email atau memblokir pengiriman dokumen/data ke luar) .
14. Organisasi agar menerapkan teknologi (DLP Data Leakage Prevention) untuk mencegah terungkapnya informasi sensitif ke luar dari organisasi .
15. Organisasi melibatkan pihak independen untuk mengkaji kehlan keamanan informasi secara rutin.

F. ASPEK PELINDUNGAN DATA PRIBADI

1. Organisasi agar mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal.
2. Organisasi agar memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh.
3. Proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di organisasi agar didokumentasikan.
4. Organisasi agar menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain.
5. Kajian risiko keamanan pada organisasi agar memasukkan aspek Pelindungan Data Pribadi.
6. Mekanisme pelindungan data pribadi agar diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku.
7. Organisasi agar mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut .
8. Organisasi agar memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi.
9. Organisasi agar menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut.
10. Organisasi agar menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan.

11. Organisasi agar menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data.
12. Organisasi agar menerapkan proses terkait penghapusan/pemusnahan data apabila agar tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut.
13. Organisasi agar menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum.

Penutup

Demikian Laporan *Online Assessment* Indeks KAMI 5.0 Pemerintah Daerah Kabupaten Mamuju Tahun 2025, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan informasi Pemerintah Daerah Kabupaten Mamuju.

Depok, 5 Januari 2026

Diskominfosip Kabupaten Mamuju
Tim Asesi:

Kepala Diskominfosip Kabupaten Mamuju

Ditandatangani secara elektronik oleh :
Plt. KEPALA DINAS KOMINFOSIP MAMUJU

Akhmad Taufiq, S.Ip., M.Si.
NIP : 19790102 201101 1 006

Kepala Bidang Persandian

Ditandatangani secara elektronik oleh :
Plt. KEPALA BIDANG PERSANDIAN KOMINFOSIP MAMUJU

RAHMANILLAH, S.Sos
NIP. 19790119 200701 2 010

Badan Siber dan Sandi Negara
Asesor Indeks KAMI:

Sandiman Ahli Pertama

Dokumen Ini ditandatangani secara elektronik oleh:
Sandiman Ahli Pertama

ROYBAFIH SUKISMAN, S.Tr.TP.
Penata Muda Tingkat I (III/b)

Pengolah Data dan Infromasi

Dokumen Ini ditandatangani secara elektronik oleh:
Pengolah Data Keamanan Siber dan Sandi

SITI MARYANTI, A.Md
Pengatur (II/c)

Dr. Roebiono Kertopati

Ingatlah Kechilafan Satu Orang Sahaja
Tjukup Sudah Menjebabkan Keruntuhan
Negara

Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
Deputi Bidang Keamanan Siber dan Sandi dan Pembangunan Manusia
Badan Siber dan Sandi Negara

Jalan Raya Muchtar 70
Bojong Sari, Depok, Jawa Barat – 16516