



# LAPORAN ONLINE ASSESSMENT INDEKS KAMI



INDEKS  
KEAMANAN  
INFORMASI

<b>Instansi/Perusahaan:</b>  PEMERINTAH DAERAH PROVINSI MALUKU	<b>Narasumber Instansi/Perusahaan:</b>  1. Dra. Nureny Tuarita, MSi. 19660312 199203 2 011  2. Joseph S.Anakotta,S.Sos 19690814 199203 1 015  3. Luky Soukotta, S.Sos 19710306 199103 1 007  4. Gysbert Haumahu 19880520 201101 1 003  5. Merie.J A Lawalata 19651008 198503 2 005  6. Jenny Putiray, A.Md. 19790717 201001 2 017  7. Samuel Nikijuluw, S.Kom 19870910 201503 1 003
<b>Unit Kerja:</b>  DINAS KOMUNIKASI DAN INFORMATIKA	
<b>Alamat:</b>  Jl. Dr. Latumenten, Ambon - 97112	Tel/ Fax : (0911) 342460
<b>Email:</b>  kominfo@malukuprov.go.id	<b>Pimpinan Unit Kerja:</b>  Drs. Semuel. E. Huwae, MH 19691111 199510 1 001

## A. Ruang Lingkup:

### 1. Instansi / Unit Kerja:

Layanan Ruang Server dan Sistem Informasi yang dikelola oleh Dinas Komunikasi dan Informatika Provinsi Maluku (Diskominfo Provinsi Maluku).

### 2. Fungsi Kerja:

Sebagaimana Peraturan Gubernur Maluku Nomor 33 Tahun 2017 tentang Uraian Tugas Jabatan Pimpinan Tinggi Pratama, Administrator dan Pengawas di Lingkungan Dinas Komunikasi dan Informatika Provinsi Maluku, Diskominfo Provinsi Maluku memiliki tugas melaksanakan urusan pemerintahan bidang komunikasi dan informatika dan di bidang persandian serta tugas pembantuan yang ditugaskan kepada daerah provinsi sesuai dengan ketentuan yang berlaku untuk meningkatkan pelayanan kepada masyarakat/ publik. Dalam menyelenggarakan tugas tersebut, Diskominfo Provinsi Maluku memiliki fungsi sebagai berikut :

- a. Perumusan kebijakan di bidang komunikasi dan informatika, persandian dan statistik;
- b. Pelaksanaan kebijakan di bidang komunikasi dan informatika, persandian dan statistik;
- c. Pelaksanaan evaluasi dan pelaporan di bidang komunikasi dan informatika, persandian dan statistik; dan
- d. Pembinaan teknis dan fasilitasi di bidang komunikasi dan informatika, persandian dan statistik.

3. Lokasi:

No	Nama Lokasi	Alamat
1	Diskominfo Provinsi Maluku	Jl. Dr. Latumeten, Ambon - 97112
2	Ruang Server	Jl. Dr. Latumeten, Ambon - 97112

B. Nama /Jenis Layanan Publik:

Layanan informasi website malukuprov.go.id dan mediacenter.malukuprov.go.id.

C. Aset TI yang kritikal:

1. Informasi:
  - Data konfigurasi sistem
2. Aplikasi:
 

Kurang lebih memiliki 20 aplikasi, namun yang dikelola Diskominfo di antaranya:

  - malukuprov.go.id
  - mediacenter.malukuprov.go.id
3. Server :
  - Tidak memiliki server utama, menggunakan penyedia *hosting* (niagahoster.com).
  - Memiliki server yang berada di Diskominfo, namun hanya untuk proses *development* dan uji coba sebelum *production*.
4. Infrastruktur Jaringan/Network:
  - Asti Net, tidak ada redundan.

D. DATA CENTER (DC):

- ADA, dalam ruangan khusus (Ruang server dikelola internal)
- 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)
	<b>Kebijakan, Sasaran, Rencana, Standar</b>			
1	Kebijakan Keamanan Informasi	Ya		D
2	Organisasi, Peran dan Tanggungjawab Keamanan Informasi	Ya		D
3	Panduan Klasifikasi Informasi	Ya		D
4	Kebijakan Manajemen Risiko TIK	Ya		D
5	Kerangka Kerja Manajemen Kelangsungan Usaha ( <i>Bussiness Continuity Management</i> )		Tdk	-
6	Kebijakan Penggunaan Sumberdaya TIK		Tdk	-
	<b>Prosedur/ Pedoman:</b>			-
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 <i>Removable Media</i> & Disposal Media		Tdk	-
7	Pemantauan ( <i>Monitoring</i> ) Penggunaan Fasilitas TIK		Tdk	-
8	<i>User Access Management</i>		Tdk	-
9	<i>Teleworking</i>		Tdk	-
10	Pengendalian instalasi <i>software</i> & HAKI		Tdk	-
11	Pengelolaan Perubahan ( <i>Change Management</i> ) TIK		Tdk	-
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi	Ya		R

**Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)**

**Dokumen yang diperiksa:**

1. Peraturan Daerah Provinsi Maluku Nomor 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Maluku;
2. Peraturan Gubernur Maluku Nomor 33 Tahun 2017 tentang Uraian Tugas Jabatan Pimpinan Tinggi Pratama, Administrator dan Pengawas di Lingkungan Dinas Komunikasi dan Informatika Provinsi Maluku;
3. Peraturan Gubernur Nomor 73 Tahun 2020 tentang Pelaksanaan Persandian untuk Pengamanan Informasi;
4. Keputusan Gubernur Maluku Nomor 228 Tahun 2021 tentang Pembentukan Tim Tanggap Insiden Siber Pemerintah;

5. Surat Keputusan Kepada Diskominfo Nomor 800/61/SK/IV/2021 tentang Pembentukan Tim Penanggung Jawab Aset Kritis;
6. BA Audit Penyelenggaraan Persandian Tahun 2020;
7. Dokumen Pelaksanaan Anggaran Tahun 2021;
8. Lampiran Rencana Program Kegiatan Sub Kegiatan dan Pendaan 2020-2024;
9. Laporan Kegiatan *Hardening* Tahun 2021;
10. Laporan Kegiatan ITSA Tahun 2020;
11. Laporan Hasil Pemantauan dan Evaluasi Penyelenggaraan Urusan Persandian 2020;
12. Laporan Hasil Pemantauan dan Evaluasi Penyelenggaraan Urusan Persandian 2018;
13. Laporan Kegiatan Penyediaan Layanan Keamanan Informasi Pemerintah Daerah Provinsi (*Bimtek IT Security dan Assessment*) Tahun 2021;
14. Laporan Kegiatan Penyediaan Layanan Keamanan Informasi Pemerintah Daerah Provinsi (*Sosialisasi Keamanan Siber*) Tahun 2021;
15. Usulan Pemusnahan Barang Milik Daerah Tahun 2021;
16. Perjanjian Kinerja Eselon II, III dan IV Tahun 2021;
17. SOP Penerimaan Berita Naskah Surat Biasa Melalui Email Sanapati;
18. SOP Penerimaan Naskah yang dikecualikan;
19. SOP Pengiriman Surat Elektronik (Email Sanapati);
20. SOP Pengiriman Naskah Dinas Dikecualikan;
21. SOP *Back Up* Data Elektronik Eksternal Naskah Dinas Biasa/Dikecualikan;
22. SOP *Back Up* Data Elektronik Internal Naskah Dinas Biasa/Dikecualikan;
23. SOP Pemulihan Insiden Keamanan Informasi *Hosting Server*;
24. SOP Penanganan Insiden Keamanan Informasi;
25. SOP Pendaftaran Insiden pada *Ticketing System*;
26. Telaahan Staf Hasil *IT Assessment* dari BSSN untuk aplikasi lingkup Pemerintah Provinsi Maluku;
27. Kontrak Berlangganan Penyediaan Layanan Astinet;
28. Form Bukti Pinjam Pakai Barang Inventaris Tahun 2021;
29. Buku Inventaris Gabungan Tahun 2020;
30. Draf Peraturan Gubernur tentang Tata Kelola SPBE;
31. Draf Peraturan Gubernur tentang Daftar Informasi yang Dikecualikan;
32. Draf Lampiran Sistem Manajemen Keamanan Informasi (SMKI).

**Bukt-bukti (rekaman/arsip) penerapan SMKI:**

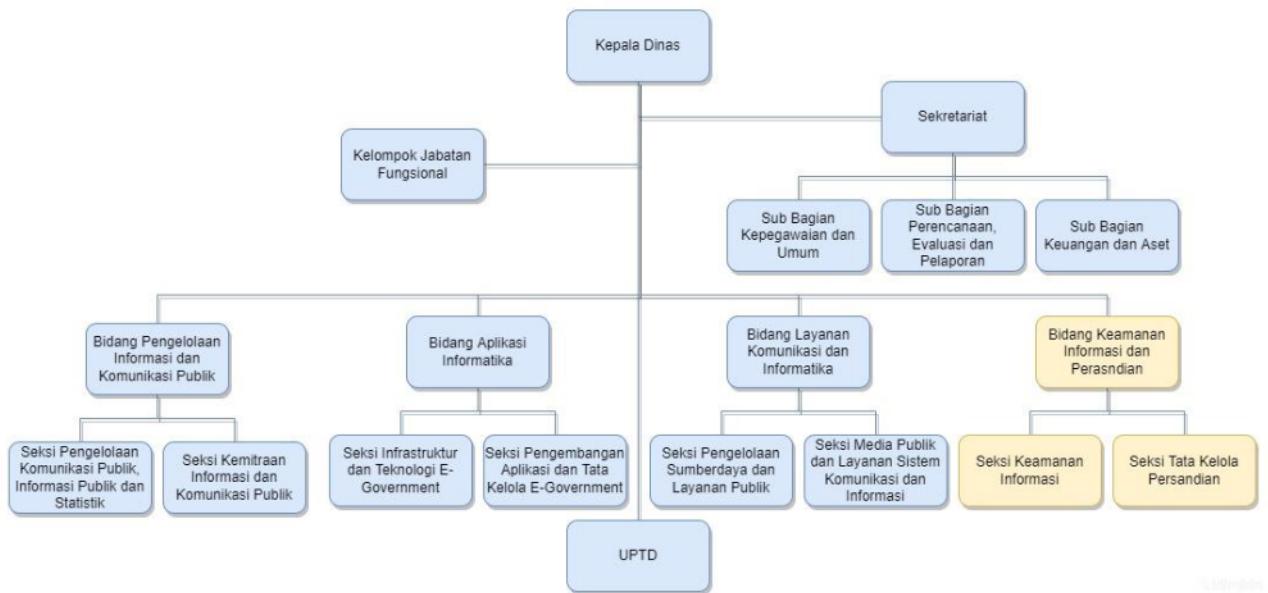
1. *Screenshot cPanel – email accounts*;
2. *Screenshot modul pengecekan kompleksitas password*;
3. *Screenshot antivirus – imunify360*;
4. *Screenshot konfigurasi mikrotik*;
5. *Screenshot log menggunakan log viewer*;
6. *Screenshot penggunaan fungsi hash pada database untuk penyimpanan password*;
7. *Screenshot server proxmox*;
8. *Screenshot SSL*;
9. *Screenshot SIEM – Wazuh*;
10. Topologi jaringan kantor gubernur.

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

**I. KONDISI UMUM:**

1. Struktur organisasi satuan kerja dalam ruang lingkup Diskominfo Provinsi Maluku dibentuk berdasarkan Peraturan Daerah Provinsi Maluku Nomor 6 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Maluku dan menjalankan tugas dan fungsinya berdasarkan Peraturan Gubernur Maluku Nomor 33 Tahun 2017 tentang Uraian Tugas Jabatan Pimpinan Tinggi Pratama, Administrator dan Pengawas

di Lingkungan Dinas Komunikasi dan Informatika Provinsi Maluku. Adapun struktur Diskominfo Provinsi Maluku adalah sebagai berikut:



2. SDM pengelola terdiri dari:

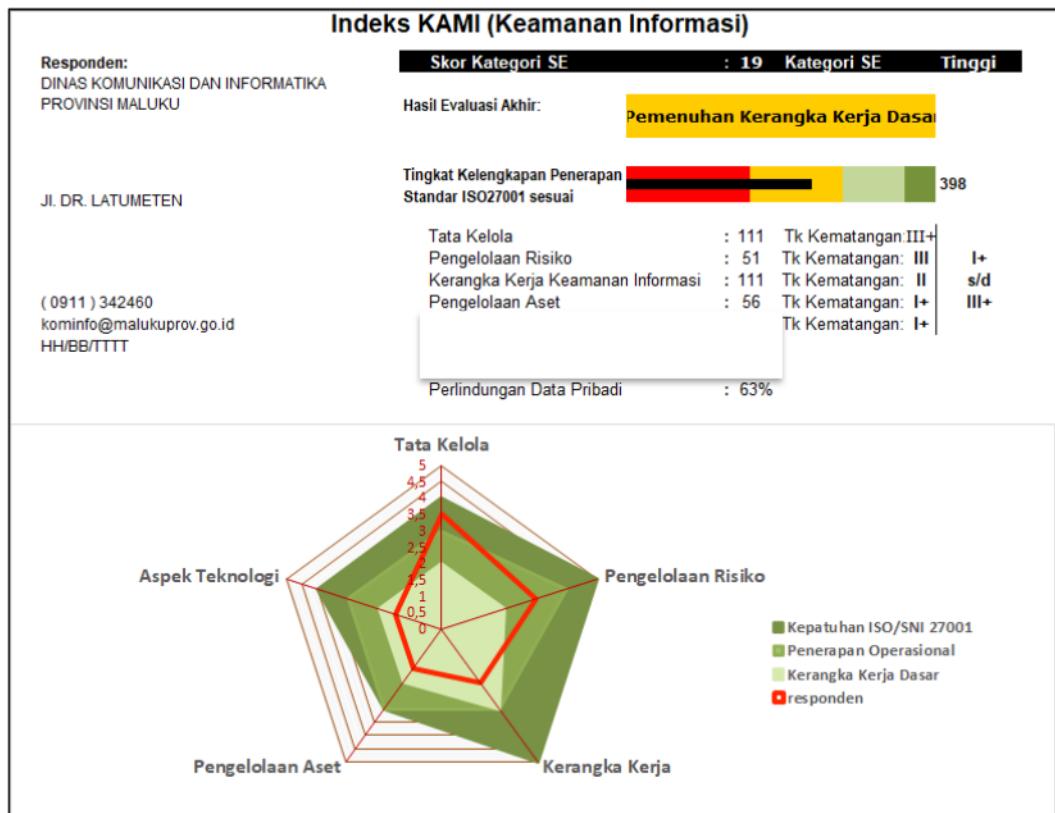
Jumlah pegawai Diskominfo Provinsi Maluku adalah 45 personil ASN dan 22 personil Non ASN (PTT). Sedangkan jumlah pegawai pada Bidang Keamanan Informasi dan Persandian sebanyak 7 personil ASN dan 1 orang personil Non ASN, serta pada Bidang Aplikasi dan Informatika sebanyak 5 personil ASN dan 3 orang personil Non ASN.

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

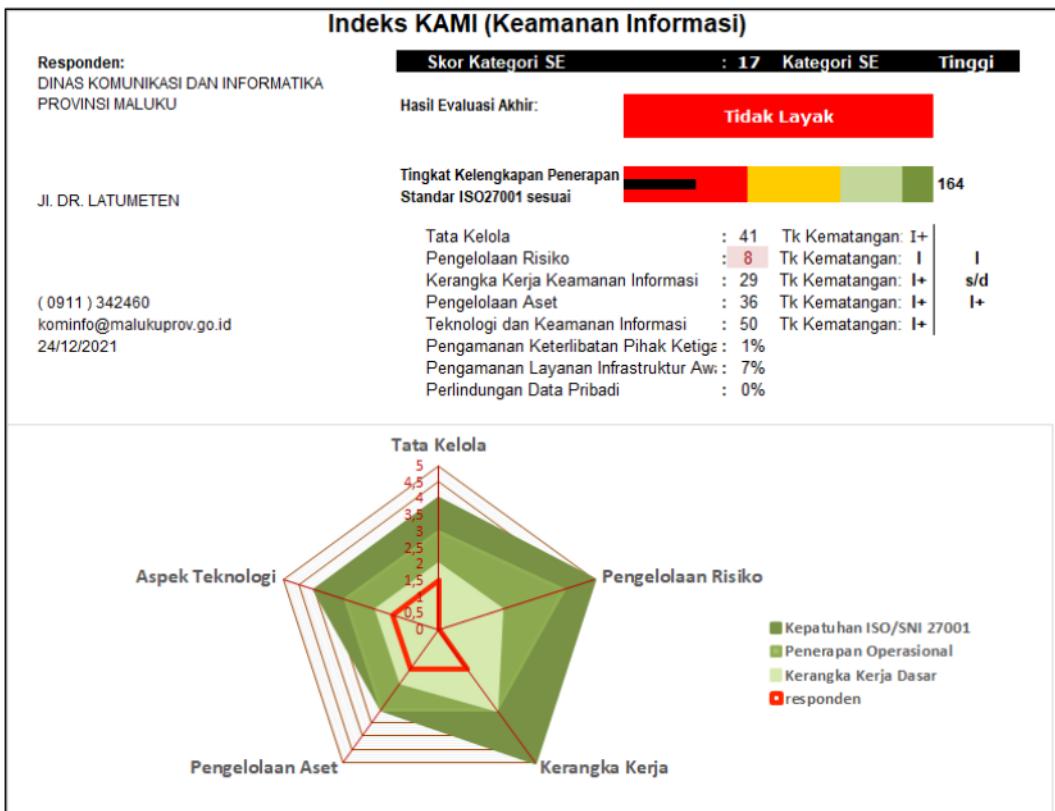
Tahun 2021 ini Penilaian Mandiri Indeks KAMI dilakukan dengan ruang lingkup Ruang Server dan Sistem Informasi yang dikelola oleh Dinas Komunikasi dan Informatika Provinsi Maluku (Diskominfo Provinsi Maluku) dengan kategori **TINGGI** dan hasil evaluasi akhir **TIDAK LAYAK** dengan total nilai **164**.

Pada tahun 2021 merupakan periode pertama kali bagi Diskominfo Provinsi Maluku dalam melakukan penilaian mandiri dengan menggunakan Indeks KAMI yang dilakukan verifikasi oleh Tim BSSN, 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, Tata Kelola, Pengelolaan Risiko, Aset, Teknologi dan Keamanan Informasi serta Suplemen. Pada pelaksanaan verifikasi, Tim Asesor berupaya untuk membantu dan mengarahkan Diskominfo Provinsi Maluku untuk dapat memperbaiki dan meningkatkan implementasi Keamanan Informasi sesuai ruang lingkup Diskominfo melalui penyiapan data dukung/ *evidence* berikut penerapan dan perbaikannya secara berkelanjutan dalam rangka meningkatkan proses penerapan Sistem Manajemen Keamanan Informasi yang secara langsung berdampak pada meningkatnya fungsi Persandian di Provinsi Maluku secara lebih optimal.

**Total Score Sebelum Verifikasi: 398 (ref. file Indeks KAMI pra Verifikasi)**



**Total Score Setelah Verifikasi: 164 (ref. file Indeks KAMI pasca Verifikasi)**



## **II. ASPEK TATA KELOLA:**

### A. Kekuatan/Kematangan

1. Dinas Kominfo Pemprov Maluku telah menetapkan fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab dalam mengelola dan mengimplementasikan program keamanan informasi dan memastikan kepatuhannya.
2. Dinas Kominfo Pemprov Maluku dan fungsi pengelola keamanan informasi telah 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 serta hal ini perlu dijadikan agenda rutin untuk meningkatkan pemahaman keamanan informasi.
3. Memiliki dasar hukum dalam pelaksanaan tugas dan fungsi organisasi dalam pengamanan informasi yang tertuang pada Peraturan Gubernur Maluku Nomor 33 Tahun 2017 dan Peraturan Gubernur Nomor 73 Tahun 2020 tentang Pelaksanaan Persandian untuk Pengamanan Informasi.
4. Sudah Menyusun draf Sistem Manajemen Keamanan Informasi, namun belum disahkan.
5. Menjadikan aspek keamanan informasi pada sebagian proses kegiatan yang dilakukan, namun belum menjadikan aspek keamanan informasi sebagai bahan pengambilan keputusan pimpinan.
6. Memiliki penanggung jawab pengelolaan keamanan informasi untuk berkoordinasi dengan pihak internal maupun eksternal, meskipun belum terdokumentasi dengan baik dan belum proaktif dalam berkoordinasi.

### B. Kelemahan/Kekurangan

1. Pimpinan dari Dinas Kominfo Pemprov Maluku belum menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen di antaranya belum adanya penetapan kebijakan keamanan informasi. Salah satu hal ini adalah dengan dibuktikan terkait program keamanan informasi dalam *IT Strategic Plan (ITSP)* atau inisiatif-inisiatif proyek terkait.
2. Pejabat/petugas pelaksana pengamanan informasi belum ditunjuk di dalam organisasi yang mempunyai wewenang untuk mengimplementasikan program keamanan informasi yang akan dilaksanakan.
3. Alokasi sumber daya terkait pelaksanaan program keamanan informasi belum direncanakan dan disediakan dalam rangka memastikan pengelolaan keamanan informasi telah memadai dan dipastikan kepatuhannya.
4. Peran fungsi pelaksana pengamanan informasi belum dipetakan terkait pengelolaan program keamanan informasi secara lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan.
5. Dinas Kominfo Pemprov Maluku belum mendefinisikan persyaratan/standar kompetensi dan keahlian khususnya terkait pelaksana pengelolaan keamanan informasi.
6. Semua pelaksana pengamanan informasi yang terlibat di Dinas Kominfo Pemprov Maluku belum memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku khususnya terkait aspek kontrol teknis dan operasional keamanan informasi.
7. Dinas Kominfo Pemprov Maluku belum 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.
8. Beberapa persyaratan keamanan informasi yang terdapat dalam standar yang berlaku sudah terintegrasi ke dalam proses kerja yang ada namun sebagian lainnya masih bersifat aktivitas kontrol tambahan yang dilakukan.
9. Persyaratan keamanan informasi yang terdapat dalam standar yang berlaku belum terintegrasi ke dalam proses kerja yang ada.

10. Dinas Kominfo Pemprov Maluku belum mengidentifikasi data pribadi yang digunakan dalam proses kerja dan belum menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku.
11. 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.
12. Tanggung jawab pengelolaan keamanan informasi yang didelegasikan kepada fungsi pengelola keamanan informasi belum mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, dan untuk mengidentifikasi persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada.
13. Fungsi pengelola keamanan informasi sudah melaporkan kepada manajemen mengenai sebagian dari kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi namun belum secara rutin namun masih dalam perencanaan.
14. Setiap permasalahan keamanan informasi yang terjadi menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis dalam melakukan tindakan perbaikan yang diperlukan untuk meningkatkan efektivitas pelaksanaan kontrol keamanan informasi, masih dalam perencanaan.
15. Dinas Kominfo Pemprov Maluku akan menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggung jawabnya, masih dalam perencanaan.
16. Metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi akan didefinisikan yang mencakup mekanisme, waktu pengukuran, pelaksananya, dan harus diukur dan dievaluasi pemantauannya secara berkala serta dilakukan eskalasi pelaporan kepada manajemen untuk memastikan efektivitas dari proses pengelolaan program dan kontrol keamanan informasi yang diterapkan, masih dalam perencanaan
17. Tanggung jawab terhadap pengelolaan langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) belum dirancang dalam dokumentasi yang ada. Hal ini termasuk pengalokasian kebutuhan sumber daya dan proses yang diperlukan dalam rangka menjamin kelangsungan bisnis ketika terjadi kondisi darurat yang telah ditetapkan oleh manajemen.
18. Dinas Kominfo Pemprov Maluku belum 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 belum didefinisikan dan diformulasikan, serta dilakukan evaluasi dan mengkaji hasil pencapaian secara rutin. Laporan hasil evaluasi terhadap target dan sasaran tersebut belum dilaporkan statusnya kepada pimpinan organisasi.
20. Dinas Kominfo Pemprov Maluku belum mendelegasikan pihak terkait / unit kerja / fungsi pengelola keamanan informasi pada internal Dinas Perhubungan Kota Malang untuk mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi serta dipastikan untuk dipatuhi dengan menganalisis tingkat kepatuhannya.
21. Dinas Kominfo Pemprov Maluku belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

### **III. ASPEK RISIKO:**

- A. Kekuatan/Kematangan
1. Pemerintah Provinsi Maluku telah mendefinisikan kepemilikan dan pihak pengelola (*custodian*) aset informasi yang dimiliki berupa inventaris aset yang telah tercantum dalam buku inventaris gabungan maupun keluaran dari aplikasi Sistem Informasi Manajemen Barang Daerah (SIMBADA) dengan tingkat kepemilikan aset dilakukan pada

tiap bidang pada Dinas Komunikasi dan Informatika. Namun berdasarkan inventaris tersebut, belum terdapat pengelompokan aset utama/penting yang akan menjadi modal dasar dalam melindungi keamanan informasi di dalamnya dan belum terdapat penanggung jawab yang akan melakukan pengelolaan terhadap aset saat terjadi kerusakan atau kehilangan.

2. Telah membentuk tim penanggung jawab aset kritis yang bertugas melakukan serangkaian upaya pengamanan dan perlindungan terhadap aset kritis yang dimiliki sesuai keputusan Kepala Dinas Komunikasi dan Informatika Pemerintah Provinsi Maluku Nomor 800/61/SK/IV/2021.
3. Telah menetapkan dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset yang tercantum dalam kolom aspek bisnis dan strategis pada tabel aset infrastruktur jaringan Diskominfo Pemerintah Provinsi Maluku namun belum dilakukan secara menyeluruh terhadap keseluruhan identifikasi aset utama yang telah dimiliki.

#### B. Kelemahan/Kekurangan

1. Pemerintah Provinsi Maluku belum memiliki program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan, saat ini saat ini terkait dengan kebijakan pengelolaan risiko tercantum dalam konsep dokumen Sistem Manajemen Keamanan Informasi.
2. Pemerintah Provinsi Maluku belum memiliki kerangka kerja pengelolaan risiko, menetapkan penanggung jawab manajemen risiko, ambang batas tingkat risiko yang dapat diterima. Pada saat ini konsep kerangka risiko telah tercantum dalam dokumen konsep Sistem Manajemen Keamanan Informasi Provinsi Maluku.
3. Belum memiliki identifikasi ancaman dan kelemahan yang terkait dengan aset informasi, terutama aset utama dan belum menetapkan dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama termasuk belum menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang telah dimiliki.
4. Belum memiliki *risk register* dan belum terdapat upaya dalam melakukan pemantauan, evaluasi terhadap penyelesaian langkah mitigasi risiko berikut proses kaji ulang terhadap adanya perubahan kerangka kerja pengelolaan risiko.
5. Belum menjadikan pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan.

#### **IV. ASPEK KERANGKA KERJA:**

##### A. Kekuatan/Kematangan

1. Pemerintah Provinsi Maluku telah memiliki beberapa kebijakan dan prosedur keamanan informasi dan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang dalam keamanan informasi yang tertuang dalam penjabaran tugas dan fungsi pada Dinas Komunikasi dan Informatika, Pelaksanaan Persandian untuk Pengamanan Informasi dan konsep SMKI.
2. Telah memiliki proses identifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi dalam suatu prosedur/SOP Penanganan Insiden.
3. Telah mencantumkan aspek keamanan informasi dalam kontrak dengan pihak ketiga berupa menjaga kerahasiaan pada pasal 14 dengan merujuk pada data dukung surat pernyataan kontrak dengan Telkomsat dan PT Telekomunikasi Indonesia.
4. Pemprov Maluku telah menjadikan aspek keamanan informasi menjadi bagian dari manajemen proyek, mekanisme tersebut ter gambarkan dalam proses *hardening* yang dilakukan sesuai dengan hasil pelaporan kegiatan yang telah dilakukan.
5. Telah memiliki strategi penerapan keamanan informasi namun belum disinkronisasikan dengan hasil analisa risiko organisasi. Kondisi saat ini masih mengacu pada laporan ITSA yang dilakukan secara periodik. Strategi penerapan keamanan informasi juga telah direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi namun belum dilakukan secara menyeluruh terhadap rencana penerapan SMKI yang telah disusun.

6. Telah mempunyai rencana dan program peningkatan keamanan informasi untuk jangka pendek maupun menengah yang telah diupayakan pencapaian realisasinya sesuai dengan durasi pencapaian target yang telah ditetapkan.

**B. Kelemahan/Kekurangan**

1. Kebijakan keamanan informasi terkait SMKI masih berupa *draft*/ konsep belum ditetapkan secara formal dan belum ada upaya secara berkelanjutan dalam mempublikasikan kepada pihak internal maupun eksternal.
2. Belum memiliki mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
3. Belum tersedia proses yang mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya dan upaya untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga, kebijakan SMKI masih dalam konsep dan penyelenggaraan keamanan informasi belum diterapkan secara menyeluruh meskipun telah memiliki peraturan terkait dengan penyelenggaraan persandian untuk pengamanan informasi. (belum adanya sinkronisasi penerapan SMKI secara berkelanjutan baik pihak internal maupun eksternal)
4. Pemprov Maluku belum memiliki kebijakan dan prosedur keamanan informasi yang dibutuhkan berdasarkan hasil kajian risiko keamanan informasi maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan dimana kajian tersebut menghasilkan mitigasi tertentu yang dituangkan dalam kebijakan dan prosedur.
5. Dalam kontrak dengan pihak ketiga telah mencantumkan pentingnya menjaga aspek kerahasiaan, namun belum terdapat klausul keamanan informasi lainnya seperti perlunya menambahkan mekanisme pelaporan insiden, HAKI, tata tertib penggunaan dan pengamanan aset.
6. Konsekuensi dari pelanggaran kebijakan keamanan informasi masih belum didefinisikan, dikomunikasikan dan ditegakkan, baik di internal maupun eksternal Pemprov Maluku, saat ini ketentuan tersebut telah tercantum dalam dokumen konsep SMKI.
7. Belum memiliki prosedur resmi dalam mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi yang dihadapi.
8. Belum melakukan penerapan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, hingga memastikan pemasangan dan melaporkannya.
9. Belum menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian atau implementasi sistem baru serta menjadi upaya dalam menanggulangi permasalahan yang ada.
10. Belum adanya penerapan proses pengembangan sistem yang aman (*Secure SDLC*) dengan menggunakan prinsip atau metode sesuai standar platform teknologi, yang dilakukan saat ini masih sebatas kustomisasi terhadap pihak ketiga, pelaksanaannya masih secara sporadis dan belum ditetapkan dalam kebijakan/prosedur yang perlu dilakukan secara berkesinambungan dan konsisten.
11. Belum adanya prosedur/mekanisme penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, termasuk proses untuk menanggulangi dan penerapan pengamanan baru (*compensating control*) serta jadwal penyelesaiannya.
12. Belum memiliki kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning/BCP*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya.
13. Belum memiliki perencanaan pemulihan bencana terhadap layanan TIK (*Disaster Recovery Plan/DRP*) yang terdapat komposisi, peran, wewenang dan tanggungjawab tim serta belum dilakukan uji coba dan evaluasi sebagai tahap langkah perbaikan atau pembenahan yang diperlukan.
14. Belum melakukan evaluasi kelayakan secara berkala terhadap seluruh kebijakan dan prosedur keamanan informasi yang dimiliki.

15. Belum memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada serta belum melakukan evaluasi tingkat kepatuhan secara konsisten dan berkelanjutan maupun kaji ulang dan penyampaian kepada pimpinan terkait dengan langkah peningkatan kinerja keamanan informasi.
16. Belum ada proses yang dilakukan untuk merevisi kebijakan dan prosedur yang berlaku, termasuk analisa untuk menilai aspek finansial ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya.
17. Belum melakukan pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada secara periodik.

## **V. ASPEK PENGELOLAAN ASET:**

### A. Kekuatan/Kematangan

1. Memiliki daftar inventaris aset, namun masih terbatas pada asset persandian dan asset infrastruktur jaringan, belum mendata aset sampai dengan *end user*, misalkan laptop, PC, perlengkapan ruang server, dan lain sebagainya.
2. Sudah mendefinisikan klasifikasi asset informasi pada draf SMKI, namun belum di sahkan sehingga belum dapat diterapkan.
3. Sudah memiliki definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses pada draf Pergub tentang informasi yang dikecualikan, namun belum disahkan.
4. Sudah melakukan proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten, namun belum memiliki kebijakan yang mengaturnya.
5. Telah melakukan proses pengelolaan konfigurasi yang diterapkan secara konsisten, hal ini diimplementasikan pada konfigurasi mikrotik.
6. Telah melakukan proses untuk merilis suatu aset baru ke dalam lingkungan operasional, namun belum memutakhirkan inventaris aset informasi.
7. Telah melakukan pengelolaan identitas elektronik dan proses otentikasi (*username & password*) pada komputer dan email, namun belum memiliki kebijakan terhadap penyelenggaranya.
8. Telah melakukan pertukaran data dengan pihak eksternal dan pengamanannya, namun belum memiliki prosedur yang menjadi turunan dari draf SMKI.
9. Telah memiliki prosedur dalam penanganan insiden terkait kegagalan keamanan informasi.
10. Telah secara rutin melakukan *back-up* pada beberapa aset yang dikelola, namun belum pernah melakukan uji coba pengembalian data (*restore*) secara berkala.
11. Telah melakukan proses penghancuran data/aset yang sudah tidak diperlukan.

### B. Kelemahan/Kekurangan

1. Belum melakukan evaluasi dan mengklasifikasikan aset informasi seusai dengan tingkat kepentingan aset, hal ini dapat dituangkan dalam dokumen *risk register*.
2. Belum menetapkan definisi tanggungjawab pengamanan informasi secara individual untuk semua personil, hal ini dapat dituangkan pada Berita Acara (BA) ketika penyerahan aset organisasi atau dapat dimasukkan dalam klausul pada draf SMKI.
3. Memiliki tata tertib penggunaan komputer, email, internet dan intranet, tata tertib pengamanan dan penggunaan aset instansi terkait HAKI, serta peraturan instalasi piranti lunak di aset TI milik instansi, namun masih dalam draf SMKI dan belum diimplementasikan.
4. Belum memiliki peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.
5. Belum mengimplementasikan persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi yang tertuang pada draf SMKI.

6. Belum mengimplementasikan ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data yang tertuang pada draf Pergub tentang informasi yang dikecualikan.
7. Belum melakukan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya, hal ini tertuang pada draf SMKI.
8. Belum melakukan proses pengecekan latar belakang SDM sebagaimana yang tertuang pada draf SMKI.
9. Belum memiliki prosedur/ proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib, prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya (*user access rights*) berikut langkah pemberahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku, serta prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.
10. Belum memiliki data/informasi yang harus *di-backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya, daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
11. Belum memiliki 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.
12. Belum melakukan secara maksimal pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang, hal ini tertuang pada draf SMKI dan perlu diturunkan dalam bentuk kebijakan baik SOP maupun juknis. Pengamanan baru pada tingkatan penguncian pintu ruangan server dengan kunci fisik dan pemasangan cctv di luar ruangan server.
13. Belum memiliki proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik.
14. Infrastruktur komputasi belum terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya.
15. Infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik karena menggunakan UPS yang dapat digunakan selama kurang lebih 15 menit ketika kondisi darurat, namun belum ada perlindungan dari dampak petir.
16. Belum memiliki peraturan sah pengamanan perangkat komputasi milik organisasi apabila digunakan di luar lokasi kerja resmi (kantor), hal ini terdapat pada draf SMKI namun sudah diimplementasikan pada penggunaan VPN pada Disdukcapil.
17. Belum memiliki proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris).
18. Konstruksi ruang penyimpanan perangkat pengolah informasi penting belum 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.
19. Belum memiliki proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting.
20. Belum memiliki mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
21. Belum memiliki 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). Hal ini terdapat pada draf SMKI dan perlu diimplementasikan.
22. Belum memiliki proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan organisasi.

**VI. ASPEK TEKNOLOGI:****A. Kekuatan/Kematangan**

1. Pengamanan pada layanan TIK yang menggunakan internet sudah dilakukan lebih dari satu lapis. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll). Hal ini dapat dilihat dari topologi jaringan pada Diskominfo Provinsi Maluku.
2. Telah melakukan pemindaian untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi, namun belum konsisten dilaksanakan.
3. Setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log.
4. Sistem operasi telah dimutakhirkan dengan versi terkini namun belum secara menyeluruhan.
5. Telah memiliki kebijakan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, namun belum diimplementasikan.
6. Melakukan pemutakhiran versi terkini pada setiap perangkat server ketika ada rekomendasi dan menerapkan antivirus/ *antimalware bundling* dengan cpanel (imunify).
7. Melibatkan pihak independen untuk mengkaji keandalan keamanan informasi, namun belum secara konsisten penerapannya.

**B. Kelemahan/Kekurangan**

1. Keseluruhan infrastruktur jaringan, sistem dan aplikasi belum dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada.
2. Belum melalukan analisa secara berkala pada log untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik).
3. Belum memiliki kebijakan standar dalam penerapan enkripsi untuk melindungi aset informasi penting.
4. Belum seluruh sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama, serta pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*, dan penarikan akses.
5. Belum menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi.
6. Belum memiliki laporan penyerangan virus/*malware* yang gagal/sukses ditindaklanjuti dan diselesaikan.
7. Belum memastikan keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada.
8. Pada proses pengembangan dan uji coba aplikasi, belum melakukan verifikasi terhadap spesifikasi dan fungsi keamanan.
9. Belum menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun.

**VII. ASPEK SUPLEMEN:****A. Kekuatan/Kematangan**

1. Telah memiliki draf kebijakan SMKI yang memuat kebijakan keamanan informasi bagi pihak ketiga.
2. Telah memiliki kebijakan penetapan data apa saja yang dapat disimpan/ diolah/ dipertukarkan melalui layanan berbasis *cloud* yang dikelola oleh Diskominfo Provinsi Maluku.

**B. Kelemahan/Kekurangan**

1. Belum memiliki kebijakan terkait manajemen risiko dan pengelolaan keamanan pihak ketiga, pengelolaan sub-kontraktor/alih daya pada pihak ketiga, pengelolaan layanan dan keamanan pihak ketiga, pengelolaan perubahan layanan dan kebijakan pihak ketiga, penanganan aset, pengelolaan insiden oleh pihak ketiga, dan rencana kelangsungan layanan pihak ketiga.
2. Belum memiliki kebijakan pengamanan layanan infrastruktur awan (*cloud service*).
3. Belum memiliki kebijakan perlindungan data pribadi.

### **VIII. REKOMENDASI**

1. Pimpinan Dinas Kominfo Pemprov Maluku perlu secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait.
2. Dalam rancangan dokumen Kebijakan Umum dan Prosedur Sistem Manajemen Keamanan Informasi Dinas Kominfo Pemprov Maluku, dapat disusun mengacu ISO 27001 : 2013.
3. Dalam rancangan dokumen Kebijakan Manajemen Risiko Dinas Kominfo Pemprov Maluku, dapat disusun mengacu ISO 27001 : 2013.
4. Peran pelaksana pengamanan informasi yang mencakup semua keperluan perlu dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan.
5. Dinas Kominfo Pemprov Maluku perlu menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait.
6. Dinas Kominfo Pemprov Maluku perlu menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi.
7. Dinas Kominfo Pemprov Maluku perlu mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada.
8. Pengelola keamanan informasi perlu secara proaktif berkoordinasi 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.
9. Tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) Perlu didefinisikan dan dialokasikan.
10. Penanggung jawab pengelolaan keamanan informasi Perlu melaporkan kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi.
11. Pimpinan satuan kerja di Dinas Kominfo Pemprov Maluku perlu menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggung jawabnya.
12. Dinas Kominfo Pemprov Maluku perlu mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya.
13. Dinas Kominfo Pemprov Maluku perlu menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya.
14. Dinas Kominfo Pemprov Maluku perlu menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi.
15. Dinas Kominfo Pemprov Maluku perlu mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisis tingkat kepatuhannya.
16. Dinas Kominfo Pemprov Maluku perlu mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

17. Pemerintah Provinsi Maluku perlu memiliki program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan sebagai dasar dalam meminimalisir terjadinya peristiwa/insiden yang dapat mempengaruhi kinerja organisasi.
18. Perlunya memiliki pengelompokan aset utama/penting (inventaris aset kritis) sesuai yang tercantum pada Keputusan Kadiskominfo tentang tugas, kewajiban dan tanggung jawab aset kritis di mana salah satunya adalah melakukan pendataan aset kritis di Dinas Kominfo Provinsi Maluku serta menambahkan pihak yang akan bertanggung jawab dalam melakukan pengelolaan terhadap aset saat terjadi kerusakan atau kehilangan.
19. Perlu menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan dengan tujuan adalah dapat dilakukan langkah antisipasi dalam menangani risiko yang akan terjadi sesuai dengan level kewenangan yang ditetapkan sehingga meminimalisir terjadinya efek risiko sistemik.
20. Perlunya memiliki kerangka kerja pengelolaan risiko yang mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian, serta menetapkan ambang batas tingkat risiko yang dapat diterima dalam kebijakan yang ditetapkan oleh pimpinan Provinsi Maluku dan digunakan sebagai dasar dalam melakukan serangkaian upaya dalam menghindari terjadinya insiden yang berdampak pada kelangsungan bisnis maupun merusak reputasi organisasi. Implementasi kerangka kerja pengelolaan risiko dapat merujuk pada peraturan maupun standar manajemen risiko yang telah ada seperti Peraturan Menteri PAN RB nomor 5 tahun 2020 tentang Manajemen Risiko SPBE atau ISO 27005, NIST SP 800-30 di mana di dalamnya terdapat kerangka kerja yang dapat digunakan dalam manajemen risiko sistem informasi, di mana ada 3 tahapan dalam proses manajemen risiko, yaitu *risk assessment*, *risk mitigation*, dan *risk evaluation*.
21. Perlunya melakukan identifikasi ancaman dan kelemahan terhadap aset informasi, terutama aset utama dan menetapkan dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama.
22. Perlu melakukan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang telah dimiliki dan dilakukan secara berkala serta berkelanjutan guna mengetahui secara *realtime* perlunya *update* perubahan terhadap adanya perkembangan teknologi berikut ancaman keamanan yang menyertainya.
23. Perlu menyusun *risk register* (daftar inventarisasi risiko yang berisikan sejumlah risiko yang akan membantu organisasi dalam melakukan identifikasi, penilaian, dan pengelolaan risiko hingga tingkat yang dapat diterima melalui proses peninjauan dan pembaruan secara periodik).
24. Mengacu dokumen *risk register* tersebut perlu dilakukan pemantauan, evaluasi terhadap penyelesaian langkah mitigasi risiko serta proses kaji ulang terhadap adanya perubahan apabila terdapat perubahan aset maupun level risiko yang ada karena terjadinya suatu kondisi tertentu yang mengakibatkan terjadinya perubahan terhadap *risk register* tersebut.
25. Pentingnya menjadikan pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan melalui serangkaian proses sistematis dan terstruktur dengan membudayakan sadar risiko pada seluruh komponen di dalamnya sesuai dengan pembagian kerja dan kewenangan yang telah ditetapkan.
26. Perlunya melakukan identifikasi kebijakan dan prosedur keamanan informasi secara lengkap dan detail dengan melihat pada penjabaran dokumen SMKI yang telah dikonsepkan sebagai upaya dalam menjalankan penerapan SMKI secara utuh di mana dalam pelaksanaannya terdapat pembagian peran dan wewenang secara jelas mulai dari tahap perencanaannya sampai dengan evaluasi dan perbaikan proses keamanan informasi.
27. Perlu menyusun mekanisme pengelolaan dokumen kebijakan dan prosedur keamanan informasi yang tertuang dalam SOP di mana di dalamnya memuat tentang penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
28. Perlunya prosedural sistematis yang akan menggambarkan pelaksanaan pengamanan informasi secara menyeluruh dengan melibatkan/mengkomunikasikan kebijakan yang telah disusun baik pada pihak internal maupun eksternal sehingga akan lebih merasakan manfaat dengan keberadaan Dinas Kominfo sebagai *lead* dan penanggung jawab pelaksanaan keamanan informasi di Pemprov Maluku.

29. Perlunya melakukan identifikasi, penyusunan kebijakan dan prosedur keamanan informasi sesuai kebutuhan berdasar hasil mitigasi dari proses kajian risiko keamanan informasi maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan.
30. Perlunya penetapan dari adanya konsekuensi yang diterima terhadap pelanggaran kebijakan keamanan informasi, saran dapat ditambahkan dan diperkuat dalam konsep SMKI khususnya dalam Bab terkait dengan Kepatuhan.
31. Perlunya memiliki prosedur resmi dalam mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi yang akan dihadapi.
32. Perlunya menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, termasuk alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, dan memastikan pemasangan dan pelaporannya.
33. Perlunya peningkatan kegiatan *hardening* secara terjadwal dan berkelanjutan baik oleh internal dan eksternal Pemprov Maluku serta perlunya penambahan SOP Manajemen Proyek dimana di dalamnya memuat aspek keamanan informasi.
34. Perlunya menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian atau implementasi sistem baru serta menjadi upaya dalam menanggulangi permasalahan yang ada. Pentingnya mendokumentasikan proses tersebut sebagai bagian dari evaluasi dan tindak lanjut pelaksanaan keamanan informasi pada periode mendatang.
35. Perlunya penambahan penerapan SDLC pada konsep SMKI dengan pengayaan pada peraturan yang telah ada misalkan Peraturan BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE.
36. Perlunya prosedur/mekanisme penerapan suatu sistem yang mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, termasuk proses untuk menanggulangi dan penerapan pengamanan baru (*compensating control*) serta jadwal penyelesaiannya. (Proses kaji ulang *risk register* keamanan TIK).
37. Perlu menyusun BCP yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk perjadwalan uji cobanya.
38. Perlu memiliki rencana pemulihan bencana berupa DRP yang akan menjadi dokumen yang mendefinisikan setiap aktivitas, tindakan serta prosedur yang harus dilakukan oleh seluruh komponen untuk dapat melindungi/menyelamatkan aset. DRP berisikan *response plan* (rencana tanggap) terhadap bencana, satu hal yang perlu diperhatikan sebelum menyusun DRP adalah menerapkan pengelolaan risiko.
39. Pentingnya untuk melakukan evaluasi kelayakan secara berkala terhadap seluruh kebijakan dan prosedur keamanan informasi yang dimiliki sebagai strategi dalam pemantauan berkala tentang kontrol/tahapan yang perlu diperbarui atau *di-update* dengan menyesuaikan kebutuhan organisasi atau perkembangan teknologi.
40. Perlu menyusun strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko organisasi.
41. Perlunya melakukan *cascading* strategi penerapan keamanan informasi dengan menyelaraskan pembagian tugas pada tiap level koordinator/jabatan sampai dengan pelaksana, sehingga akan terlihat penerapan keberlangsungan SMKI yang akan menjadi bagian dari pelaksanaan program kerja keamanan informasi pada organisasi secara utuh dan menyeluruh.
42. Perlu memiliki audit internal secara independen yang akan melakukan evaluasi tingkat kepatuhan, pengkajian ulang terhadap perbaikan dan penyampaian kepada pimpinan terhadap peningkatan kinerja program keamanan informasi.
43. Perlu adanya mekanisme keperluan untuk merevisi kebijakan dan prosedur yang berlaku, serta analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya serta perlu melakukan pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pemberian yang diperlukan, telah diterapkan secara efektif.
44. Menginventarisasi seluruh asset tidak terbatas pada aset persandian, namun juga aset infrastruktur jaringan sampai dengan *end user*.

45. Menerapkan klasifikasi asset informasi, tingkatan akses yang berbeda dari setiap klasifikasi asset informasi dan matriks yang merekam alokasi akses dan melakukan evaluasi terhadapnya.
46. Menyusun kebijakan terkait proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi).
47. Melakukan pemutakhiran inventaris asset informasi setelah merilis suatu asset baru ke dalam lingkungan operasional.
48. Melakukan uji coba pengembalian data (*restore*) secara berkala setelah melakukan *back-up* pada asset yang dikelola.
49. Menyusun tata tertib pengamanan dan penggunaan asset yang di dalamnya tertuang penggunaan komputer, email, internet dan intranet, peraturan HAKI serta instalasi piranti lunak di asset TI.
50. Menyusun peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.
51. Mengimplementasikan ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data.
52. Melakukan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi asset yang ada di dalamnya.
53. Mendata data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya, daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
54. Menyusun 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.
55. Melakukan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi asset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang.
56. Melindungi infrastruktur komputasi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya, melindungi dari gangguan pasokan listrik dan petir.
57. Konstruksi ruang penyimpanan perangkat pengolah informasi penting belum 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.
58. Melakukan inspeksi dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan asset informasi penting.
59. Menyusun mekanisme pengamanan dalam pengiriman asset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
60. Memusatkan jaringan komunikasi di Diskominfo KSB dan melakukan segmentasi sesuai dengan kepentingannya (pembagian instansi, kebutuhan aplikasi, jalur akses khusus, dll).
61. Menyusun konfigurasi standar untuk keamanan sistem bagi keseluruhan asset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan dan kebutuhan serta belum secara rutin menganalisis kepatuhan penerapan konfigurasinya.
62. Mengimplementasikan *Security Information and Event Management* (SIEM) yang dapat berfungsi sebagai analisis keamanan, pendekripsi gangguan, analisis data log, pemantauan integritas file, pendekripsi kerentanan, penilaian konfigurasi, membantu dalam tanggap insiden, kepatuhan terhadap kebijakan, pemantauan keamanan cloud.
63. Menerapkan pengamanan untuk mendekripsi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi, misalnya membuat SSID yang tersegmentasi khusus bagi pengunjung atau pihak ketiga.
64. Melakukan penerapan pengamanan fisik pada lingkungan *data center* dengan mekanisme pengamanan kunci digital seperti *fingerprint*, *biometrik* atau sensor RFID, serta diimbangi dengan adanya kebijakan/prosedurnya.
65. Melakukan pemindaian terhadap sistem elektronik yang meliputi jaringan, sistem dan seluruh aplikasi yang dimiliki secara berkala.
66. Melakukan pemasangan antivirus dan *antimalware* pada sistem elektronik yang dimiliki dan dikelola.

67. Memastikan keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada.
68. Menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun
69. Mencantumkan standar dalam menggunakan enkripsi (penerapan kriptografi) di kebijakan SMKI, serta membuat dokumen turunan dari kebijakan tersebut.
70. Semua sistem dan aplikasi menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama. Pengaturan tersebut disarankan untuk dituangkan dalam prosedur penggunaan *password*.
71. Menyusun dan mengimplementasikan kebijakan pengamanan keterlibatan pihak ketiga penyedia layanan, pengamanan layanan infrastruktur awan (*cloud service*) dan perlindungan data pribadi.

Ambon, 29 Desember 2021

Depok, 29 Desember 2021

**Narasumber Instansi/Perusahaan:**

Dinas Komunikasi dan Informatika Provinsi Maluku

1. Dra. Nureny Tuarita, MSi.  
19660312 199203 2 011

2. Joseph S.Anakotta,S.Sos.  
19690814 199203 1 015

3. Luky Soukotta, S.Sos.  
19710306 199103 1 007

4. Gysbert Haumahu, S.Kom  
19880520 201101 1 003

5. Merie.J A Lawalata  
19651008 198503 2 005

6. Jenny Putiray, A.Md.  
19790717 201001 2 017

7. Samuel Nikijuluw, S.Kom  
19870910 201503 1 003

**Asessor Indeks KAMI:**

1. Lead Asesor:  
Firman Maulana, S.E.



2. Asesor Pendamping:  
Diah Sulistyowati, S.Kom.



3. Asesor Pendamping:  
Irma Nurfitri Handayani, S.ST.



4. Asesor Pendamping:  
Ivan Bashofi, S.S.T.TP.



5. Asesor Pendamping:  
Mochamad Jazuly, S.S.T.TP.

