


	<b>LAPORAN ONSITE ASSESSMENT INDEKS KAMI</b>	 <b>INDEKS KEAMANAN INFORMASI</b>
<b>Instansi/Perusahaan:</b>  PEMERINTAH DAERAH PROVINSI SULAWESI BARAT	<b>Pimpinan Unit Kerja :</b>  Mustari Mula, S.Sos., M.A.P. Kepala Dinas Komunikasi, Informatika, Persandian, dan Statistik Daerah Provinsi Sulawesi Barat.	
<b>Unit Kerja:</b>  DINAS KOMUNIKASI DAN INFORMATIKA (DISKOMINFO)	<b>Narasumber Instansi/Perusahaan :</b>  1. Abdul Azis, S.Pd.,MM Kepala Bidang TIK, Persandian dan Statistik 2. Wahida Yusuf, S.IP Sandiman Ahli Muda 3. Taufan Harry Prasetyo SE.M.Ec.Dev, M.Kom Pranata Komputer Ahli Muda 4. Madhur, ST Analis Data dan Informasi 5. Sudarmono, S.IP Sandiman Ahli Pertama	
<b>Alamat:</b>  Jalan H. Abdul Malik Pattana Endeng Rangas Mamuju Sulawesi Barat 91512		
<b>Email:</b>  kominfo@sulbarprov.go.id	<b>Asesor :</b>  1. Dwi Kardono, S.Sos., M.A. Sandiman Madya pada Dir Keamanan Siber dan Sandi Pemerintah Daerah, Deputi III, BSSN 2. Aris Munandar, S.S.T. MP. Analis Tata Kelola Keamanan Siber 3. Ivan Bashofi, S.S.T.TP. Sandiman Pertama 4. Carissa Mega Yulianingrum, S.Tr.TP. Analis Tata Kelola Keamanan Siber	
<b>Tel/ Fax :</b>  -		

A. Ruang Lingkup:

## 1. Instansi / Unit Kerja:

Aplikasi SPBE dan Infrastruktur SPBE atau Sistem Elektronik yang dikelola oleh Dinas Komunikasi dan Informatika, Pemerintah Provinsi Sulawesi Barat.

## 2. Fungsi Kerja:

Sebagaimana Peraturan Gubernur Sulawesi Barat Nomor 45 Tahun 2016 tentang Susunan Organisasi, Tugas, Fungsi, dan Tata kerja Dinas Komunikasi dan Informatika, Provinsi Sulawesi Barat berserta Peraturan Gubernur perubahannya memiliki tugas pokok membantu Gubernur melaksanakan urusan pemerintahan Bidang Komunikasi dan Informatika, urusan pemerintahan Bidang Persandian dan urusan pemerintahan Bidang Statistik.

Dalam menyelenggarakan tugas tersebut, Diskominfo memiliki fungsi sebagai berikut :

- menyusun rencana daerah dibidang Komunikasi, Informatika, Persandian dan Statistik berdasarkan rencana daerah dan nasional;
- perumusan dan pelaksanaan kebijakan daerah dibidang Teknologi Komunikasi Informasi, Persandian dan Statistik;
- pengoordinasian dan pembinaan UPTD; dan
- pelaksanaan fungsi lain yang diberikan oleh Gubernur yang berkaitan dengan tugasnya.

## 3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor dan Ruang Server Dinas Komunikasi dan Informatika Pemprov Sulawesi Barat	Jalan H. Abdul Malik Pattana Endeng Rangas Mamuju Sulawesi Barat 91512

B. Nama /Jenis Layanan Publik:

Sistem Elektronik Sipamandar (<https://sipamandar.sulbarprov.go.id/>) yang dikelola oleh Dinas Komunikasi, Informatika, Statistik, dan Persandian Provinsi Sulawesi Barat.

C. Aset TI yang kritikal:

## 1. Aplikasi:

Memiliki 108 aplikasi yang dikelola oleh Diskominfo Pemprov Sulawesi Barat baik yang hosting di dalam maupun di luar Diskominfo (49 server luar dan 59 server lokal/diskominfo).

## 2. Server :

- Server sulbarprov.go.id

## 3. Infrastruktur Jaringan/Network:

- ISP PT Indonesia Comnets Plus (ICON+)

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		Tdk	-
2	Organisasi, Peran dan Tanggungjawab Keamanan Informasi	Ya		R
3	Panduan Klasifikasi Informasi	Ya		R
4	Kebijakan Manajemen Risiko TIK		Tdk	-
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	Ya		R
2	Pengendalian Rekaman/ Catatan		Tdk	-
3	Audit Internal SMKI		Tdk	-
4	Tindakan Perbaikan & Pencegahan		Tdk	-
5	Pelabelan, Pengamanan, Pertukaran & Disposasi Informasi		Tdk	-
6	Pengelolaan <i>Removable</i> Media & Disposasi Media		Tdk	-
7	Pemantauan ( <i>Monitoring</i> ) Penggunaan Fasilitas TIK		Tdk	-
8	<i>User Access Management</i>		Tdk	Draft
9	<i>Teleworking</i>		Tdk	-
10	Pengendalian instalasi <i>software</i> & HAKI		Tdk	Draft
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 Gubernur Sulawesi Barat Nomor 45 Tahun 2016 tentang Susunan Organisasi, Tugas, Fungsi, dan Tata kerja Dinas Komunikasi dan Informatika, Provinsi Sulawesi Barat;
2. Perubahan Atas Peraturan Gubernur Sulawesi Barat Nomor 45 Tahun 2016 Tentang Kedudukan, Tugas Dan Fungsi, Susunan Organisasi, Dan Tata Kerja Dinas Daerah Provinsi Sulawesi Barat;
3. Peraturan Gubernur Sulawesi Barat Nomor 27 Tahun 2020 tentang Sistem Klasifikasi Keamanan Dan Akses Arsip Dinamis;
4. Rancangan Pergub Penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Provinsi;
5. Rancangan Pergub Penyelenggaraan/Pengelolaan Tanda Tangan Elektronik;
6. Dokumen Inventaris Aplikasi Layanan dan Infrastruktur;
7. Bahan Literasi Keamanan Informasi;
8. Dokumen Teknis Data Aplikasi OPD Pemprov Sulbar.

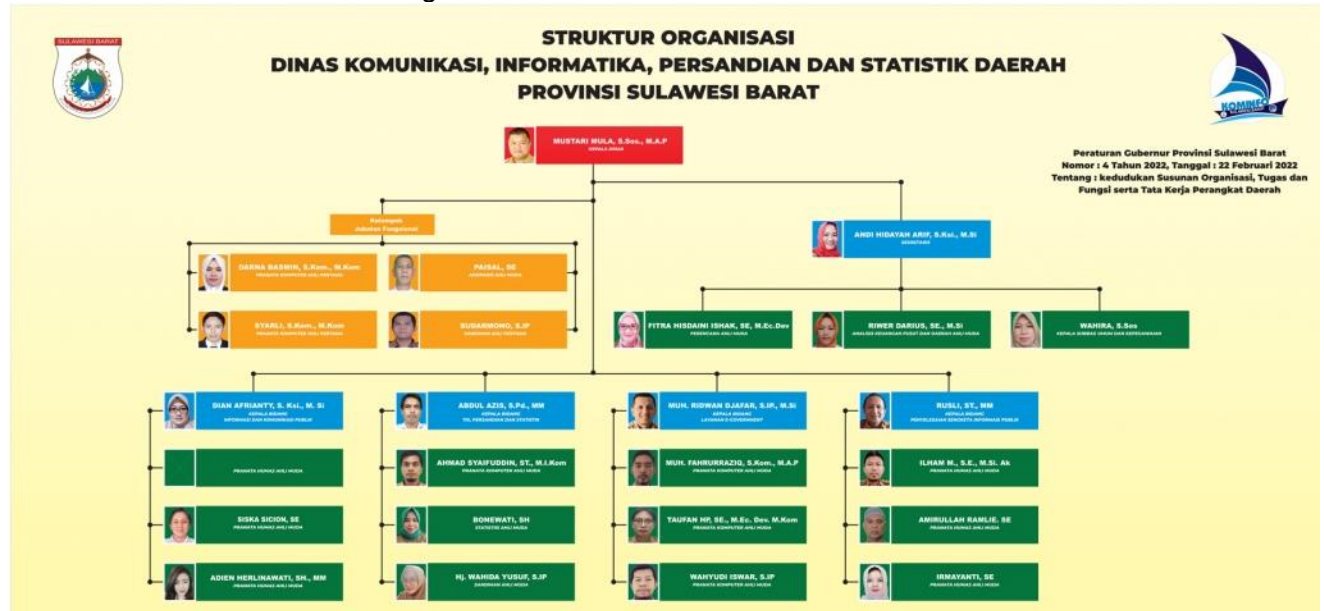
**Bukti-bukti (rekaman/arsip) penerapan SMKI:**

1. Topologi interkoneksi jaringan dan integrasi Server Diskominfo;
2. Sistem monitoring dengan SIEM;
3. Tampilan Sipamandar.

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

### I. KONDISI UMUM:

1. Diskominfo Sulawesi Barat dibentuk berdasarkan Peraturan Gubernur Provinsi Sulawesi Barat Nomor 45 Tahun 2016 tentang Susunan Organisasi, Tugas, Fungsi, dan Tatakerja Dinas Komunikasi dan Informatika, Provinsi Sulawesi Barat, berikut struktur Diskominfo Pemprov Sulawesi Barat adalah sebagai berikut:



Gambar 1. Struktur Organisasi Diskominfo Pemprov Sulawesi Barat

2. SDM pengelola (Sandiman dan Pranata Komputer) terdiri dari:

No	Status Kepegawaian	Jumlah	Prosentase
1.	Pimpinan Struktural	6	
2.	Sandiman dan Teknik Sandi	3	
3.	Pranata Komputer	12	
<b>Jumlah</b>		<b>21</b>	<b>100%</b>

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

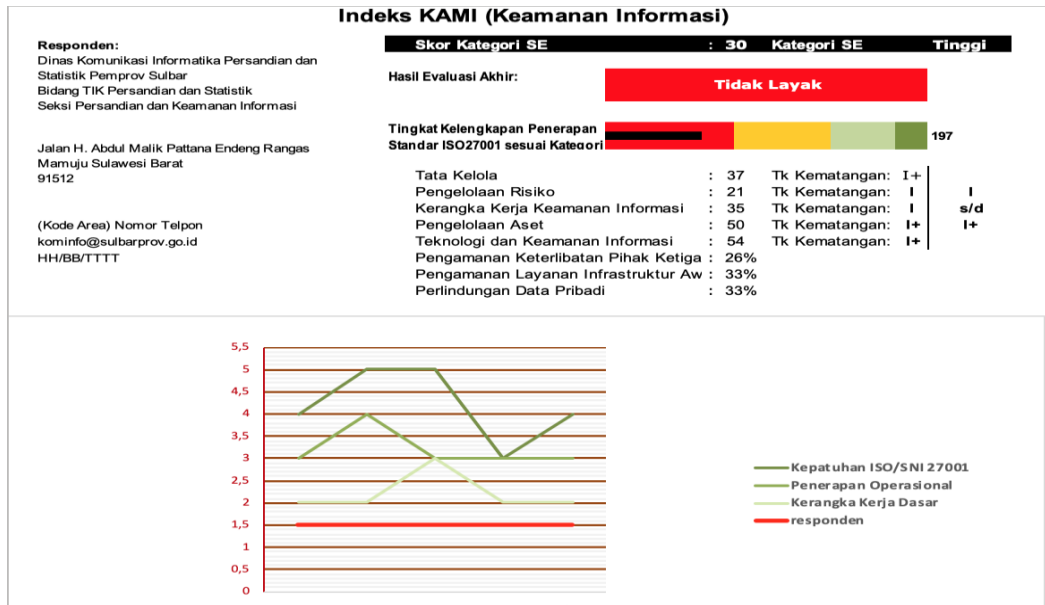
Penilaian Mandiri Indeks KAMI dilakukan pada bulan Juli tahun 2022 dengan ruang lingkup organisasi Diskominfo Pemerintah Provinsi Sulawesi Barat terhadap Aplikasi dan Infrastruktur SPBE atau Sistem Elektronik (SE) yang dikelola. Selanjutnya penilaian mandiri telah dilakukan verifikasi oleh Tim BSSN dan didapat bahwa SE yang ditentukan memiliki kategori SE **Tinggi** dan hasil evaluasi akhir **Tidak Layak** dengan total nilai **187**.

Pada tahun 2022 ini merupakan periode kali pertama bagi lingkup Diskominfo Pemerintah Provinsi Sulawesi Barat dilakukan verifikasi oleh Tim BSSN terhadap penilaian mandiri Indeks KAMI yang telah dilakukan sebelumnya, 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 lingkup Diskominfo Pemerintah Provinsi Sulawesi Barat 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

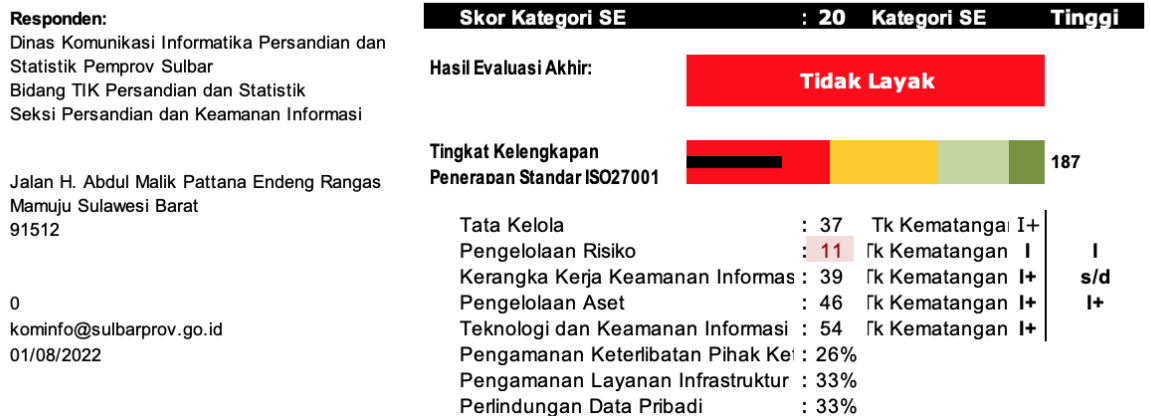
meningkatkan proses penerapan Sistem Manajemen Keamanan Informasi yang secara langsung berdampak pada meningkatnya fungsi Persandian dan Pengamanan Informasi di Diskominfo Provinsi Sulawesi Barat secara lebih optimal.

### Total Score Sebelum Verifikasi: 197 (ref. file Indeks KAMI v4.2 pra Verifikasi)



### Total Score Setelah Verifikasi: 187 (ref. file Indeks KAMI v4.2 pasca Verifikasi)

#### Indeks KAMI (Keamanan Informasi)



**II. ASPEK TATA KELOLA:****A. Kekuatan/Kematangan**

1. Diskominfo Prov Sulbar memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola Persandian dan secara tidak langsung memiliki tugas dalam mengelola keamanan informasi;
2. Pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi;
3. Kondisi dan permasalahan keamanan informasi di Diskominfo Sulbar menjadi pertimbangan atau bagian dari proses pengambilan keputusan strategis; dan
4. Diskominfo Sulbar sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi.

**B. Kelemahan/Kekurangan**

1. Tidak memiliki kebijakan internal terkait Sistem Manajemen Keamanan Informasi (SMKI) atau Kebijakan Manajemen Keamanan Informasi SPBE yang menjelaskan terkait penetapan ruang lingkup, penetapan penanggungjawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, perbaikan berkelanjutan terhadap keamanan informasi dilingkungan Pemprov Sulbar;
2. Tidak memiliki dokumen atau kebijakan pengelolaan langkah kelangsungan layanan TIK merujuk pada *business continuity planning (BCP)* dan *disaster recovery plans (DRP)* termasuk pengalokasian kebutuhan sumber daya dan proses yang diperlukan dalam rangka menjamin kelangsungan bisnis ketika terjadi kondisi darurat;
3. Target dan sasaran pengelolaan keamanan informasi terhadap area yang relevan belum didefinisikan dan diformulasikan langkah perbaikannya secara rutin serta laporan hasil evaluasi terhadap target dan sasaran tersebut belum dilaporkan statusnya kepada pimpinan organisasi;
4. Belum adanya hasil identifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang digunakan dan dipatuhi serta belum dilakukan proses analisis tingkat kepatuhan terhadap kebijakan tersebut; dan
5. Diskominfo belum menetapkan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).
6. Ketersediaan SDM Keamanan Informasi yang dinilai masih kurang dari segi kuantitas dan kemampuan terhadap keamanan informasi.

**III. ASPEK RISIKO:****a. Kekuatan/Kematangan**

1. Diskominfo Prov Sulbar sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
2. Diskominfo secara metode sederhana 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).

**b. Kelemahan/Kekurangan**

1. Diskominfo tidak memiliki dokumen manajemen risiko atau daftar risiko (risk register) terkait pengelolaan IT atau keamanan informasi yang menjelaskan substansi paling sedikit memuat :
  - a. inventarisir aset (perangkat keras IT & perangkat lunak);
  - b. inventarisir layanan berbasis aplikasi SPBE;
  - c. Identifikasi ancaman;
  - d. Identifikasi kerentanan;
  - e. Penentuan risiko yang menjadi prioritas;
  - f. Analisa dampak jika terjadi risiko;
  - g. Analisa kontrol keamanan yang bisa diterapkan; dan
  - h. Rekomendasi kontrol keamanan.



2. Diskominfo belum menentukan langkah mitigasi risiko yang disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK.
3. Tidak adanya profil risiko berikut bentuk mitigasinya serta belum secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru.

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

##### **a. Kekuatan/Kematangan**

1. Sebagian kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada sebagian kecil staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya.
2. Tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan sebagian kebijakan keamanan informasi (dan perubahannya) kepada sebagian pihak terkait.

##### **b. Kelemahan/Kekurangan**

1. Kebijakan keamanan informasi terkait SMKI dan turunannya serta penetapan peran dan tanggung jawab implementasinya belum ditetapkan dan belum terdapat strategi untuk mempublikasikan kebijakan keamanan informasi secara terprogram dan rutin baik pada pihak internal maupun eksternal.
2. Belum memiliki proses identifikasi kondisi yang membahayakan keamanan informasi dan menetakannya sebagai insiden keamanan informasi dalam suatu prosedur/SOP Penanganan Insiden.
3. Diskominfo belum memiliki kebijakan dan prosedur keamanan informasi yang dibutuhkan berdasar hasil kajian risiko keamanan informasi maupun sasaran/obyektif tertentu yang telah ditetapkan oleh pimpinan di mana kajian tersebut menghasilkan mitigasi yang dituangkan dalam kebijakan dan prosedur secara keseluruhan terhadap aset yang dimiliki.
4. Dalam pengaturan penyelenggaraan TIK pada aspek manajemen pihak ketiga belum memiliki kebijakan pencantuman aspek kerahasiaan, mekanisme pelaporan insiden, HAKI, tata tertib penggunaan dan pengamanan aset, saat ini masih dalam konsep kebijakan keamanan informasi dengan pihak ketiga.
5. Konsekuensi dari pelanggaran kebijakan keamanan informasi masih belum didefinisikan, dikomunikasikan dan ditegakkan, baik di internal maupun eksternal Pemprov Sulawesi Barat.
6. Belum memiliki prosedur resmi dalam mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi yang dihadapi.
7. Belum melakukan evaluasi tingkat kepatuhan terhadap pelaksanaan audit internal yang dilakukan secara konsisten dan berkelanjutan.
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 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.
10. Belum memiliki kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning/BCP*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya.
11. Belum memiliki perencanaan pemulihan bencana terhadap layanan TIK (*Disaster Recovery Plan/DRP*) yang terdapat komposisi, peran, wewenang dan tanggung jawab tim serta belum dilakukan uji coba dan evaluasi sebagai tahap langkah perbaikan atau pembenahan yang diperlukan.

12. Belum melakukan evaluasi kelayakan secara berkala terhadap seluruh kebijakan dan prosedur keamanan informasi yang dimiliki.
13. 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.
14. Belum melakukan pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada secara periodik.

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

##### **a. Kekuatan/Kematangan**

1. Tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara.
2. Tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku.
3. Tersedia persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi.
4. Tersedia prosedur back-up dan uji coba pengembalian data (restore) secara berkala.
5. Terlaksana proses pengecekan latar belakang SDM.

##### **b. Kelemahan/Kekurangan**

1. Belum memiliki kebijakan dan SOP terkait penggunaan computer, internet dan intranet, yang digunakan sebagai panduan pelaksanaan keamanan informasi bagi pegawai.
2. Belum memiliki kebijakan dan implementasi mekanisme pengamanan dan penggunaan aset organisasi terkait HAKI seperti penggunaan lisensi resmi untuk aplikasi yang digunakan dan belum memiliki formulir daftar instalasi *software*.
3. Belum memiliki tata tertib penggunaan komputer, email, internet dan intranet.
4. Belum memiliki Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan.
5. Belum memiliki mekanisme penggunaan data pribadi sebagai dasar pengaturan penggunaan data pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggungjawab.
6. Belum memiliki kebijakan proses otentikasi dan sanksi pelanggaran.
7. Belum memiliki tata cara pemusnahan barang TIK namun yang merujuk pada klasifikasi aset yang dimiliki organisasi.
8. Belum tersedia prosedur rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
9. Kebijakan pengendalian pihak ketiga telah tercantum pengaturan pemenuhan standar keamanan dan penerapan manajemen insiden namun masih berupa konsep prosedur yang belum ditetapkan.
10. Telah memiliki prosedur perlindungan terhadap infrastruktur komputasi dari dampak lingkungan maupun gangguan pasokan listrik dan adanya ancaman terhadap bencana kebakaran namun penerapan dan evaluasi belum dilakukan secara berkala dalam menjaga ketersediaan dan keamanan layanan TIK di dalamnya.

#### **VI. ASPEK TEKNOLOGI:**

##### **a. Kekuatan/Kematangan**

1. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan.
2. Jaringan komunikasi telah disegmentasi sesuai dengan kepentingannya.
3. Jaringan, sistem dan aplikasi yang digunakan secara berkala telah dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi.
4. Keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada.
5. Setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log.



6. Sistem operasi untuk sebagian perangkat desktop dan server dimutakhirkan dengan versi terkini.
7. Sebagian desktop dan setiap server dilindungi dari penyerangan virus (malware).

b. Kelemahan/Kekurangan

1. Belum memiliki standar konfigurasi sistem, jaringan dan aplikasi serta proses analisa kepatuhan penerapan konfigurasi sesuai standar yang ada.
2. Belum secara rutin menganalisa kepatuhan penerapan konfigurasi sesuai standar yang ada.
3. Diskominfo belum menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada.
4. Diskominfo belum mempunyai atau mengacu standar dalam menggunakan enkripsi.
5. Tidak ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis.
6. Tidak adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan.
7. Diskominfo 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. Diskominfo memiliki kesadaran terkait kebijakan keamanan informasi bagi pihak ketiga dengan cukup memadai, mencakup persyaratan pengendalian akses, dan manajemen risiko penyediaan layanan pihak ketiga.
2. Diskominfo sudah menerapkan langkah pengamanan data pribadi ataupun data kedinasan yang disimpan/diolah/dipertukarkan melalui layanan cloud.

### **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 internal pengamanan layanan infrastruktur awan (*cloud service*).
3. Belum memiliki turunan kebijakan perlindungan data pribadi, kajian risiko masih bersifat secara umum dan perlu dilakukan klasifikasi sesuai dengan tingkat kekritisitas data pribadi.

## **VIII. REKOMENDASI**

### **A. TATA KELOLA :**

1. Keberadaan Diskominfo sebagai *lead* dan penanggung jawab pelaksanaan keamanan informasi di Pemprov Sulawesi Barat perlu diperkuat dengan tersedianya fungsi tata kelola keamanan informasi, fungsi Layanan atau penerapan keamanan informasi serta fungsi evaluasi dan monitoring keamanan informasi.
2. Ketiga fungsi sebagaimana dimaksud pada point 1 tentunya perlu dituangkan dalam bentuk struktur organisasi yang secara khusus dibawah Bidang Persandian. Selanjutnya terkait tugas dari setiap fungsi tersebut paling sedikit dapat meliputi :
  - a. Tata Kelola Keamanan Informasi
    - Menyusun kebijakan Keamanan informasi;
    - Edukasi dan Literasi Keamanan Informasi;
    - Peningkatan Kompetensi SDM Keamanan Informasi.
  - b. Layanan Keamanan Informasi
    - Perlindungan informasi melalui pengamanan sinyal dan kontra penginderaan;
    - Penerapan dan Pengelolaan Sertifikat elektronik;
    - Penanganan Insiden Siber/Mengkoordinir Tim CSIRT;
    - Peningkatan Keamanan Aplikasi dan Infrastruktur SPBE (Sistem Elektronik).

- c. Evaluasi dan Monitoring Keamanan Informasi
  - Audit Keamanan SPBE;
  - Penilaian atau Identifikasi Kerentanan terhadap Aplikasi dan Infrastruktur SPBE atau SE;
  - Evaluasi Pelaksanaan Persandian Kabupaten dan Kota;
  - Penilaian Risiko Keamanan Informasi;
  - Evaluasi Kebijakan Keamanan Informasi.
3. Peningkatan pemenuhan Sumber Daya Manusia (SDM) Keamanan Informasi atau SDM yang memiliki *background* pendidikan di bidang TIK melalui skema *open recruitment* atau mutasi atau melalui dukungan magang dari beberapa SMU/SMK.
4. Peningkatan pemenuhan SDM sebagaimana dimaksud pada point 3 harus didukung juga dengan program peningkatan kemampuan pengetahuan (*knowledge*) atau keahlian (*skill*) terkait keamanan informasi atau siber.
5. Menyusun kebijakan Sistem Manajemen Keamanan Informasi (SMKI) atau Manajemen Keamanan Informasi SPBE dalam bentuk Peraturan Gubernur, yang selanjutnya digunakan sebagai panduan dalam implementasi keamanan informasi untuk setiap dinas atau OPD secara menyeluruh.
6. Kebijakan Sistem Manajemen Keamanan Informasi (SMKI) atau Kebijakan Manajemen Keamanan Informasi SPBE harus menjelaskan substansi paling sedikit meliputi penetapan ruang lingkup, penetapan penanggungjawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, perbaikan berkelanjutan terhadap keamanan informasi dilingkungan Pemprov Sulbar.
7. Penyusunan kebijakan sebagaimana dimaksud pada point 5 perlu melibatkan/mengkomunikasikan dengan pihak internal (OPD) maupun eksternal (BSSN dan Kemenkominfo/BRIN) sehingga kebijakan akan lebih komprehensif.
8. Selanjutnya agar pelaksanaan SMKI berjalan dengan baik sesuai Pergub yang akan atau telah ditetapkan, Diskominfo Pemerintah Provinsi Sulawesi Barat perlu menyusun juga kebijakan teknis sebagai berikut:
  - a. Standar operasional prosedur keamanan perangkat komputer dilingkungan Provinsi Sulbar;
  - b. Standar operasional prosedur cloud;
  - c. Standar operasional prosedur server;
  - d. Standar operasional prosedur penerapan keamanan aplikasi SPBE;
  - e. Standar operasional prosedur insiden keamanan informasi atau siber;
  - f. Standar operasional prosedur penerapan keamanan jaringan; dan
  - g. Kebijakan teknis lainnya yang diperlukan dalam penerapan SMKI untuk setiap OPD.

## **B. MANAJEMEN RISIKO DAN PENGELOLAAN ASET :**

1. Menyusun dokumen manajemen risiko atau daftar risiko (*risk register*) terkait pengelolaan IT atau keamanan informasi yang menjelaskan substansi paling sedikit memuat :
  - a. inventarisir aset (perangkat keras IT & perangkat lunak);
  - b. inventarisir layanan berbasis aplikasi SPBE;
  - c. Identifikasi ancaman;
  - d. Identifikasi kerentanan;
  - e. Penentuan risiko yang menjadi prioritas;
  - f. Analisa dampak jika terjadi risiko;
  - g. Analisa kontrol keamanan yang bisa diterapkan; dan
  - h. Rekomendasi kontrol keamanan.
2. Ketentuan lebih lanjut terkait kebijakan/panduan pengelolaan risiko dapat merujuk pada Permenpan 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 (tiga) tahapan dalam proses manajemen risiko, yaitu *risk assessment*, *risk mitigation*, dan *risk evaluation*.
3. Perlu menjadikan manajemen risiko sebagai budaya kerja dalam bisnis proses organisasi dengan tujuan untuk mengurangi dampak yang merugikan dari adanya suatu kejadian. Manajemen risiko akan membantu mengawal pencapaian tujuan Diskominfo Sulawesi Barat tanpa harus menanggung kerugian yang tidak diinginkan baik secara personil maupun organisasi. Penerapannya dilakukan dengan ketentuan sebagai berikut:

- a. Menjadikan manajemen risiko menjadi bagian dari tugas dan fungsi di Diskominfo Sulawesi Barat.
  - b. Identifikasi risiko dilakukan berdasarkan kritikalitas aset untuk setiap kategori aset yaitu Perangkat Keras, Perangkat Lunak, Sistem Aplikasi, Jaringan Komunikasi, Personil (pegawai tetap dan non tetap serta pihak ketiga yang terlibat), Informasi, dan Sarana Pendukung yang digunakan dalam penyelenggaraan layanan-layanan TI oleh Diskominfo Pemprov Sulawesi Barat.
  - c. Perlunya penambahan identifikasi risiko-risiko lainnya yang perlu diidentifikasi dari aset utama/penting berikut kontrol yang ada saat ini, rencana kontrol tambahan dan penetapan status penyelesaian dengan mengacu pada *risk treatment plan* yang telah dibuat.
  - d. Perlu tambahan definisi pemilik dan pengelola aset, misal terjadi kerusakan atau kehilangan aset, maka perlu penanggung jawab dan penerapan kebijakan manajemen risiko yang akan diimplementasikan.
4. Melakukan identifikasi keseluruhan aset yang dimiliki baik aset informasi maupun aset lainnya berdasarkan kategori yang berkaitan dengan pengelolaan sistem elektronik dan memperhatikan aspek keamanannya mulai dari perencanaan sampai dengan pengembangannya dengan merujuk pada ketentuan dan standar yang telah ditetapkan.

### C. PENERAPAN KEAMANAN TEKNOLOGI DAN KEBIJAKAN PIHAK KETIGA

1. Perlu melakukan pengujian dan monitoring keamanan jaringan, sistem dan aplikasi yang dimiliki dengan menggunakan perangkat (*software/hardware*) dan mengoptimalkan SDM yang telah memiliki kualifikasi.
2. Agar melakukan pemeliharaan dan monitoring secara rutin terhadap operasional dan lingkungan fisik data center seperti:
  - a. Menjaga perimeter keamanan fisik mulai dari saat registrasi sampai dengan melakukan akses ke zona pemeliharaan serta perekaman terhadap lalu lintas masuk dan keluar personil eksternal.
  - b. Perlunya upaya dari antisipasi kebakaran dengan langkah berupa gladi/simulasi penanggulangan kebakaran yang dapat dilakukan secara berkala terhadap APAR yang dimiliki, dapat juga dengan menerapkan *thermatic sistem* dimana terdapat fungsi pendeteksi kebakaran dan sensor asap.
3. Penerapan Sertifikat Elektronik terhadap seluruh Sistem Elektronik atau Aplikasi SPBE yang dimiliki.
4. Perlunya memperhatikan sistem pengamanan yang tidak terbatas pada akses fisik namun juga akses virtual dengan salah satunya adalah melakukan peninjauan bagi pengguna eksternal yang mengakses ke data center, penggunaan enkripsi dengan level jaringan untuk pengamanan data, manajemen sertifikat SSL/TLS yang telah terpasang pada endpoint, melakukan *patching* dan pembaharuan sistem terbaru untuk melindungi dari kerentanan yang ada.
5. Memiliki kebijakan internal dan meningkatkan prosedur terkait pengamanan layanan infrastruktur awan (*cloud service*).
6. Perlu dibuat Incident Response Plan antara lain dengan menentukan prioritas aset, menyusun mekanisme laporan penyerangan *virus/malware* yang berhasil ditindaklanjuti dan diselesaikan yang juga didokumentasikan dalam playbook insiden serta tahapan penyelesaiannya sebagai upaya dalam proses pembelajaran dan peningkatan kapabilitas tim penanganan insiden.
7. Perlu mengoptimalkan fungsi CSIRT dengan melakukan *vulnerability assessment* dan *penetration testing* secara rutin baik dilakukan oleh internal maupun oleh pihak eksternal sebagai upaya untuk mendeteksi kelemahan sistem di Pemprov Sulawesi Barat.
8. Proses pembangunan dan pengembangan aplikasi SPBE harus memperhatikan standar keamanan serta pedoman *secure system development life cycle* (S-SDLC) untuk memastikan persyaratan kontrol keamanan terpenuhi dan meminimalisir risiko keamanan yang akan terjadi dikemudian hari. Salah satu tujuan dari S-SDLC adalah memastikan pengkodean pemrograman aplikasi yang dibuat dan dikembangkan tidak memiliki kerawanan (contohnya *SQL Injection* atau kemungkinan yang akan menjadi bug lainnya);
9. Memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan;

10. Menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instansi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga.
11. Perlu melakukan peningkatan pengelolaan pengamanan keterlibatan pihak ketiga penyedia layanan melalui proses penyusunan kebijakan yang ditetapkan dan dievaluasi secara berkala mulai dari proses identifikasi risiko sampai dengan kelangsungan layanan dengan pihak ketiga, meningkatkan prosedur pengamanan layanan cloud yang dikelola melalui penerapan kebijakan secara tertulis dan kajian risiko serta melakukan evaluasi terhadap implementasinya baik terhadap standar keamanan teknis dan pemenuhan sertifikasi layanan berbasis ISO 27001, menerapkan kebijakan terkait dengan perlindungan data pribadi dan mendorong kesadaran tentang pentingnya perlindungan data pribadi baik internal maupun pengguna layanan (publik) dengan merujuk pada peraturan perundang-undangan yang telah ada.

**IX. PENUTUP**

Demikian Laporan *Onsite Assessment* Indeks KAMI Pemerintah Daerah Provinsi Sulawesi Barat TA 2022 ini disusun, sebagai bahan pengambilan keputusan Pimpinan dalam pelaksanaan pengamanan informasi Pemerintah Daerah Provinsi Sulawesi Barat.

Laporan *Onsite Assessment* Indeks KAMI Pemerintah Daerah Provinsi Sulawesi Barat TA 2022 ini disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Pemerintah Daerah Provinsi Sulawesi Barat;
3. Kepala Dinas Komunikasi, Informatika, Persandian dan Statistik Provinsi Sulawesi Barat;
4. Direktur Keamanan Siber dan Sandi Pemerintah Daerah, Deputi III, BSSN.



Kepala Bidang TIK, Persandian dan Statistik

Abdul Aziz, S.Pd., MM  
NIP. 19760509 199501 1 001

**Mamuju, 3 Agustus 2022**

Fungsional Sandiman Madya selaku  
Lead Asesor Indeks KAMI

Dwi Kardono, S.Sos., M.A.  
NIP. 19710218 199110 1 001