



LAPORAN ONSITE ASSESSMENT INDEKS KAMI



INDEKS
KEAMANAN
INFORMASI

Instansi/Perusahaan: PEMERINTAH DAERAH PROVINSI SULAWESI SELATAN	Pimpinan Unit Kerja : Amson Padolo, S.Sos. NIP. 19701113 199203 1 004
Unit Kerja: DINAS KOMUNIKASI INFORMATIKA, STATISTIK DAN PERSANDIAN (DISKOMINFO-SP)	Narasumber Instansi/Perusahaan : 1. Riswan, S.Sos., M.M. NIP. 19670121 199003 1 004 2. Irvan, S.STP.,M.Adm.,SDA NIP. 19800528 199810 1 001 3. Hasanuddin, S.Kom. NIP. 19761127 200901 1 003 4. Suriany, S.H. NIP. 19661231 199803 2 022 5. Muhammad Danial Rapi, S.Kom NIP. 19711024 200112 1 001 6. Mohammad Rizki Soetrisno,S.T.,M.T NIP. 19770117 200312 1 009 7. Andi Paisal, S.Sos NIP. 19810122 201408 1 001 8. Ahmad Tasyrif Arief,S.T, M.T NIP. 19840811 201101 1 005 9. Andi Achmad Paulangi,S.Sos., M.M NIP. 19810308 200801 1 008 10. Putrawal Daha, S.Kom
Email: persandian.dkisp@sulselprov.go.id	Asesor : 1. Lukman Nul Hakim, S.E., M.M. NIP. 19701116 199110 1 001 2. Diah Sulistyowati, S.Kom., M.T. NIP. 19820925 200212 2 001 3. Mochamad Jazuly, S.S.T.TP NIP. 19920625 201412121002 4. Ni Putu Ayu Lhaksmi W., S.Tr.TP NIP. 19960622 201812 2 001
Tel/ Fax : (0411) 442855	

A. Ruang Lingkup:**1. Instansi / Unit Kerja:**

Layanan Data Center/ Ruang Server dan Sistem Informasi yang dikelola oleh Dinas Komunikasi dan Informatika, Diskominfo SP Pemerintah Provinsi Sulawesi Selatan.

2. Fungsi Kerja:

Sebagaimana Peraturan Gubernur Sulawesi Selatan Nomor 18 Tahun 2019 tentang Kedudukan, Susunan Organisasi, Tugas, Fungsi dan Tata Kerja Dinas Komunikasi, Informatika, Statistik, dan Persandian Provinsi Sulawesi Selatan memiliki tugas pokok membantu Gubernur dalam menyelenggarakan urusan pemerintahan bidang Komunikasi, Informatika, Statistik, dan Persandian yang menjadi kewenangan Daerah dan tugas pembantuan yang ditugaskan kepada Pemerintah Daerah.

Dalam menyelenggarakan tugas tersebut, SP Sulawesi Selatan memiliki fungsi sebagai berikut :

- a. perumusan kebijakan Urusan Pemerintahan Bidang Komunikasi, Informatika, Statistik, dan Persandian;
- b. pelaksanaan kebijakan Urusan Pemerintahan Bidang Komunikasi, Informatika, Statistik, dan Persandian;
- c. pelaksanaan evaluasi dan pelaporan Urusan Pemerintahan Bidang Komunikasi, Informatika, Statistik, dan Persandian;
- d. pelaksanaan administrasi Dinas; dan
- e. pelaksanaan fungsi lain yang diberikan oleh Gubernur terkait tugas dan fungsinya.

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor dan Ruang Server Dinas Komunikasi dan Informatika Pemprov Sulawesi Selatan	Jl. Urip Sumoharjo No.269, Makassar Sulawesi Selatan.

B. Nama /Jenis Layanan Publik:

Layanan Infrastruktur Data Center/ Ruang Server dan aplikasi sistem informasi yang dikelola oleh Dinas Komunikasi, Informatika, Statistik, dan Persandian Provinsi Sulawesi Selatan.

C. Aset TI yang kritikal:**1. Informasi:**

- Data Pribadi : 1. Akte Kelahiran, 2. Karpeg, 3. BPJS, 4. TASPEN, 5. KARIS, 6. NPWP, 7. KTP, 8. No. Rekening Gaji
- Data Status : 1. SK CPNS, 2. SKP PNS
- Data Riwayat : 1. SK Golongan awal sampai akhir, 2. SK Jabatan awal sampai akhir, 3. Ijazah Pendidikan awal sampai akhir, 4. Sertifikat Diklat Struktural, 5. Sertifikat Kursus, 6. SKP 2 Tahun Terakhir, 7. Penghargaan Satyalancana Karya Satya, 8. Bukti Penetapan Angka Kredit (PAK), 9. Cuti Tahunan, Cuti Sakit, Cuti Melahirkan, CTLN
- Data Keluarga : 1. KTP Orang Tua, 2. Akta Nikah Suami/Istri, 3. Akta Lahir Anak, 4. BPJS Anak
- Data Lainnya : 1. KGB 2 Tahun Terakhir, 2. LHKPN 2 Tahun Terakhir, 3. LHKASN 2 Tahun Terakhir, 4. Keanggotaan Organisasi, 5. Penguasaan Bahasa, 6. SPT tahunan 2020
- Data Riwayat Lainnya : 1. Berita Sumpah PNS, 2. Tugas belajar, 3. Ijin belajar, 4. SK pemberhentian Sementara, 5. SK pengangkatan Kembali

2. Aplikasi:
 Kurang lebih memiliki 95 aplikasi, yang dikelola oleh Diskominfo-SP maupun aplikasi permohonan *subdomain* dan *hosting* dari lingkup perangkat daerah terkait. Aplikasi tersebut antara lain sebagai berikut:
- **epinisi.sulselprov.go.id** (penetapan kategori dilakukan pada SE berikut)
 - ekinerja.sulselprov.go.id
 - bkd.sulselprov.go.id
 - sigas.persandian.sulselprov.go.id
 - smartoffice.sulselprov.go.id
3. Server :
- Server sulselprov.go.id
4. Infrastruktur Jaringan/Network:
- ISP Indosat (utama) dan Telkomsel (backup)

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)
Kebijakan, Sasaran, Rencana, Standar				
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	Ya		-
Prosedur/ Pedoman:				
1	Pengendalian Dokumen		Tdk	-

2	Pengendalian Rekaman/ Catatan		Tdk	-
3	Audit Internal SMKI		Tdk	-
4	Tindakan Perbaikan & Pencegahan		Tdk	-
5	Pelabelan, Pengamanan, Pertukaran & Disposal Informasi		Tdk	-
6	Pengelolaan <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	Ya		R
11	Pengelolaan Perubahan (<i>Change Management</i>) TIK		Tdk	-
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi		Tdk	-

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

1. Peraturan Gubernur Sulawesi Selatan Nomor 18 Tahun 2019 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Dinas Komunikasi, Informatika, Statistik, dan Persandian Provinsi Sulawesi Selatan;
2. Peraturan Gubernur Sulawesi Selatan Nomor 29 Tahun 2019 Penggunaan Sertifikat Elektronik dengan Rahmat Tuhan Yang Maha Esa;
3. Peraturan Gubernur Sulawesi Selatan Nomor 21 Tahun 2020 tentang Sistem Klasifikasi Keamanan dan Akses Arsip Dinamis;
4. Peraturan Gubernur Sulawesi Selatan Nomor 26 Tahun 2020 tentang perubahan atas Peraturan Gubernur Sulawesi Selatan Nomor 131 Tahun 2017 tentang Penyelenggaraan Teknologi Informasi dan Komunikasi Lingkup Pemerintah Daerah Provinsi Sulawesi Selatan;
5. Kertas Kerja Penilaian dan Penanganan Risiko Dinas Kominfo-SP Prov.Sulsel dalam Lingkup Penyelenggaraan Keamanan Informasi;
6. Laporan Pelaksanaan Rapat Koordinasi Kegiatan Persandian dengan Kabupaten/Kota Tahun 2021;
7. Identifikasi Sumber daya Diskominfo berupa aset kritis, sumber daya manusia dan aplikasi;
8. Hasil pelaksanaan *IT Security Assessment* dari BSSN pada tiga aplikasi;
9. Hasil pelaksanaan *vulnerability assessment* pada kab/kota di Sulawesi Selatan.
10. Sertifikasi Peningkatan Kompetensi Personil Bidang Persandian.

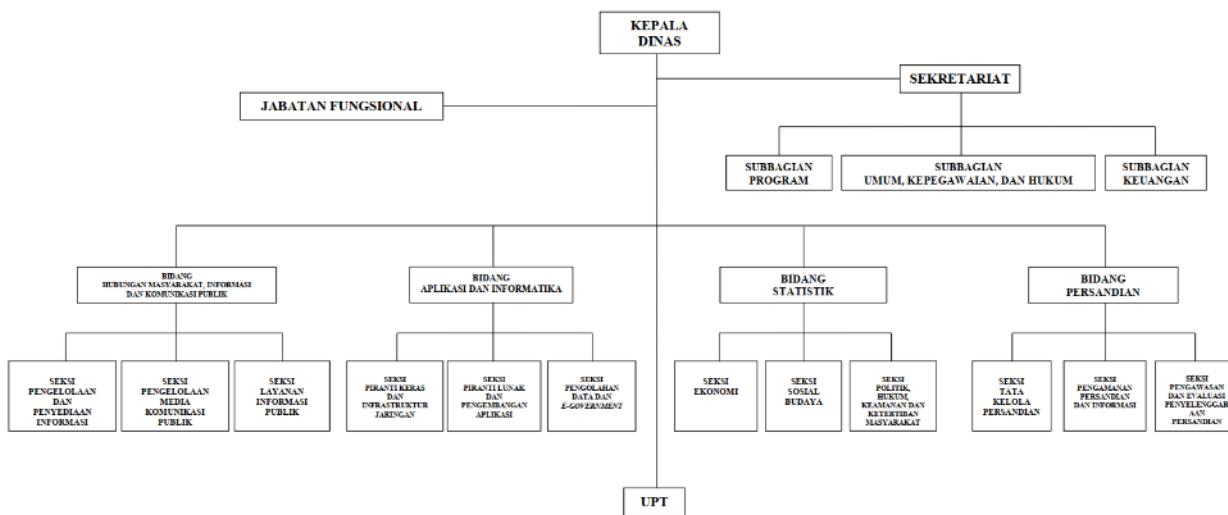
Bukti-bukti (rekaman/arsip) penerapan SMKI:

1. Tangkapan layar target kinerja individu pada ekinerja.sulselprov.go.id;
2. Tangkapan layar aplikasi e-pinisi terkait informasi data pribadi yang diupload ke dalam sistem;
3. Tangkapan layar Dashboard Penilaian Mandiri Indeks KAMI Tahun 2022;
4. Tangkapan gambar topologi jaringan.

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

I. KONDISI UMUM:

1. Diskominfo-SP Diskominfo-SP Sulawesi Selatan dibentuk berdasarkan Peraturan Gubernur Nomor 18 Tahun 2019 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Dinas Komunikasi, Informatika, Statistik, dan Persandian Provinsi Sulawesi Selatan, berikut struktur Diskominfo-SP Pemprov Sulawesi Selatan adalah sebagai berikut:



Gambar 1. Struktur Organisasi Diskominfo-SP Pemprov Sulsel

2. SDM pengelola terdiri dari: (disesuaikan kebutuhan)

No	Unit Kerja/ Bidang	ASN	TA	TKK	Jumlah
1	Sekretariat	22	-	16	38
2	Bidang Humas. Informasi dan Komunikasi Publik	28	3	20	51
3	Bidang Aptika	13	12	2	27
4	Bidang Statistik	11	-	4	15
5	Bidang Persandian	15	-	4	19
Total		89	15	46	150

Keterangan : - ASN (Aparatur Sipil Negara)

- TA (Tenaga Ahli)

- TKK (Tenaga Kerja Kontrak)

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

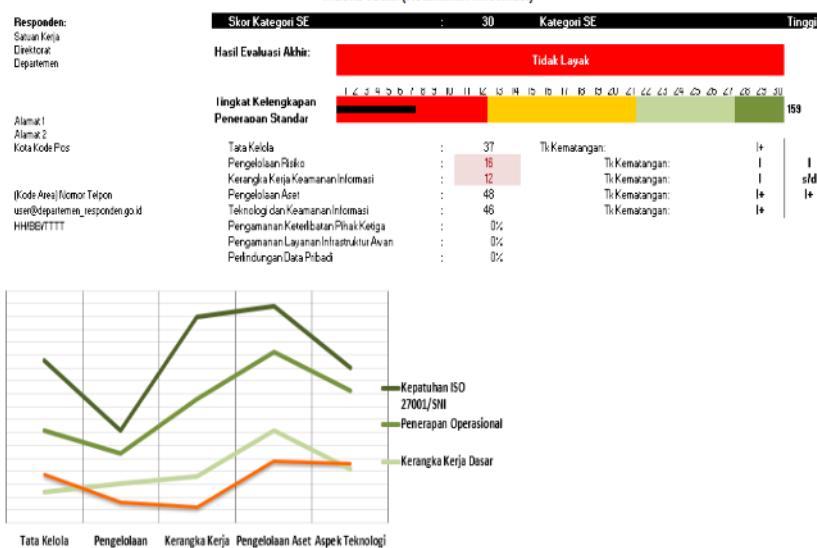
Penilaian Mandiri Indeks KAMI dilakukan di tahun 2022 ini dengan ruang lingkup Diskominfo-SP Pemerintah Provinsi Sulawesi Selatan, Ruang Server dan Sistem Informasi yang dikelola dan dilakukan verifikasi oleh Tim BSSN dengan kategori **Tinggi** dan hasil evaluasi akhir **Tidak Layak** dengan total nilai **158**.

Pada tahun 2022 ini merupakan periode kali pertama bagi lingkup Diskominfo-SP Pemerintah Provinsi Sulawesi Selatan dilakukan verifikasi oleh Tim BSSN dalam penilaian mandiri Indeks KAMI, sehingga sesuai mekanisme kebijakan yang ada untuk pelaksanaan kegiatan verifikasi adalah dengan melakukan pengecekan keseluruhan kelengkapan kebijakan dan/atau prosedur dan penerapan dokumen kebijakan dan/atau prosedur pada area Kategori, Tata Kelola, Pengelolaan Risiko, Aset, Teknologi dan Keamanan Informasi serta Suplemen. Pada pelaksanaan verifikasi, Tim Asesor berupaya untuk membantu dan mengarahkan lingkup Diskominfo SP Pemerintah Provinsi Sulawesi Selatan 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-SP Sulawesi Selatan secara lebih optimal.

Total Score Sebelum Verifikasi: 159 (ref. file Indeks KAMI v4.1pra Verifikasi)

Indeks KAMI (Keamanan Informasi)



Total Score Setelah Verifikasi: 158 (ref. file Indeks KAMI v4.2 pasca Verifikasi)

Indeks KAMI (Keamanan Informasi)

Responden:

Dinas Komunikasi, Informatika, Statistik dan Persandian
Jl. Urip Sumoharjo No.269, Makassar

(0411) 442855
persandian.dkisp@sulselprov.go.id
28/01/2022

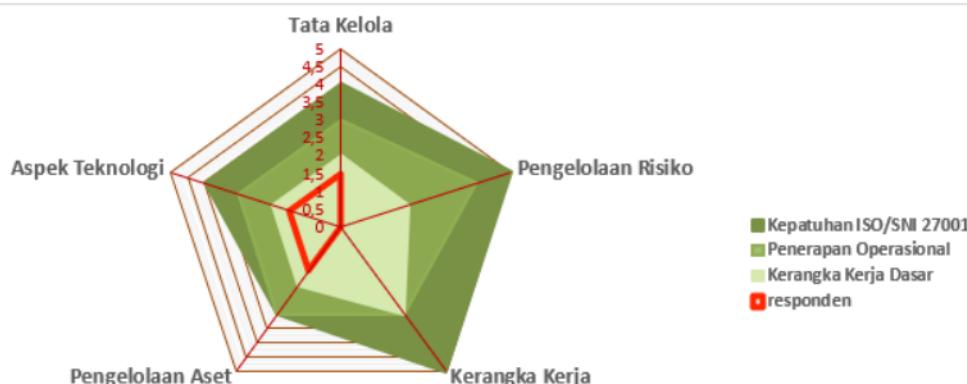
Skor Kategori SE

: 24

Kategori SE**Tinggi****Hasil Evaluasi Akhir:****Tidak Layak****Lingkup Kelengkapan Penerapan Standar ISO27001 sesuai Kategori**

158

Tata Kelola	: 27	Tk Kematangan:	I+
Pengelolaan Risiko	: 19	Tk Kematangan:	I
Kerangka Kerja Keamanan Informasi	: 24	Tk Kematangan:	s/d
Pengelolaan Aset	: 45	Tk Kematangan:	I+
Teknologi dan Keamanan Informasi	: 43	Tk Kematangan:	I+
Pengamanan Keterlibatan Pihak Ketiga	: 6%	Tk Kematangan:	I+
Pengamanan Layanan Infrastruktur Awan	: 0%		
Perlindungan Data Pribadi	: 19%		



II. ASPEK TATA KELOLA:

A. Kekuatan/Kematangan

1. Dinas Komunikasi dan Informatika Diskominfo-SP Sulawesi Selatan telah menetapkan kebijakan secara resmi dan bertanggung jawab terhadap pelaksanaan program keamanan informasi baik yang tertuang dalam program jangka menengah maupun jangka pendek melalui dokumen Rencana Strategis (Renstra) Tahun 2018-2023, Dokumen Pelaksanaan Anggaran (DPA) dan Peraturan Gubernur Nomor 26 Tahun 2020 tentang Penyelenggaraan TIK lingkup Pemprov Sulawesi Selatan.
2. Telah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya yang diimplementasikan dalam sistem elektronik ekinerja.sulselprov.go.id.
3. Telah mendefinisikan metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi dalam dokumen perencanaan kinerja yang mencakup mekanisme, waktu pengukuran, pelaksananya, dan harus diukur dan dievaluasi pemantauannya secara berkala tiap tahun.

B. Kelemahan/Kekurangan

1. Telah memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggung jawab dalam pengelolaan keamanan informasi yang tercantum dalam SOTK namun belum dilakukan secara menyeluruh terhadap aspek keamanan informasi mulai dari proses perencanaan sampai dengan pemantauan pelaksanaannya secara berkelanjutan termasuk belum adanya pelaksanaan tugas dan wewenang serta alokasi sumber daya dalam menjamin kepatuhan keamanan informasi.
2. Telah mengintegrasikan persyaratan keamanan informasi dalam proses kerja yang ada mulai dari kebijakan dan prosedur keamanan informasi namun belum dilakukan secara menyeluruh terhadap ruang lingkup kebijakan Sistem Manajemen Keamanan Informasi (SMKI).
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. Diskominfo-SP Sulawesi Selatan belum mendefinisikan persyaratan/standar kompetensi dan keahlian khususnya terkait pelaksana pengelolaan keamanan informasi.
6. Semua pelaksana pengamanan informasi yang terlibat belum memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku khususnya terkait aspek kontrol teknis dan operasional keamanan informasi
7. 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. Belum melakukan identifikasi data pribadi yang digunakan dalam proses kerja dan belum menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku.
9. Pelaksanaan koordinasi antara fungsi pengelola keamanan informasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) belum terlaksana secara memadai.
10. 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 penyelesaian masalah yang ada).

11. Belum ada konsiderans kebijakan keamanan informasi yang menjadi dasar regulasi dan dituangkan dalam daftar kebijakan yang harus dievaluasi tingkat kepatuhannya.
12. Tanggung jawab terhadap pengelolaan langkah kelangsungan layanan TIK merujuk pada *business continuity planning (BCP)* dan *disaster recovery plans (DRP)* belum dituangkan dalam sebuah dokumen perencanaan kinerja termasuk pengalokasian kebutuhan sumber daya dan proses yang diperlukan dalam rangka menjamin kelangsungan bisnis ketika terjadi kondisi darurat.
13. 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.
14. Belum adanya identifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi dan pelaksanaan serta analisis tingkat kepatuhannya.
15. Diskominfo-SP Sulawesi Selatan belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

III. ASPEK RISIKO:

a. Kekuatan/Kematangan

1. Telah memiliki Kertas Kerja Penilaian dan Penanganan Risiko yang digunakan sebagai dasar dalam melakukan pemantauan, evaluasi terhadap penyelesaian langkah mitigasi risiko berdasar pemetaan aset utama yang dimiliki.
2. Telah menetapkan dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset yang tercantum dalam kertas kerja penilaian dan penanganan risiko dan analisis aplikasi yang dimiliki Diskominfo-SP Sulawesi Selatan namun belum dilakukan secara menyeluruh terhadap keseluruhan aset.

b. Kelemahan/Kekurangan

1. Diskominfo-SP Sulawesi Selatan belum memiliki program kerja berupa kebijakan/pedoman/panduan 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. Belum memiliki kerangka kerja pengelolaan risiko, menetapkan penanggung jawab manajemen risiko, ambang batas tingkat risiko yang dapat diterima.
3. Telah memiliki identifikasi ancaman dan kelemahan yang terkait dengan aset informasi, terutama aset utama namun 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 utama yang telah dimiliki.
4. Telah menyusun langkah mitigasi risiko namun penanggulangan risiko belum dilakukan sampai dengan level kriteria penerimaan risiko/ *Risk Acceptance Criteria (RAC)*.
5. Belum menerapkan langkah prioritas dan target serta penanggung jawab penyelesaian risiko serta metode memastikan efektivitasnya terhadap kebijakan manajemen risiko yang dimiliki.
6. Kebijakan penyelesaian langkah mitigasi risiko dalam kertas kerja identifikasi risiko telah ditetapkan namun implementasinya belum dilakukan pemantauannya secara berkala dalam memastikan konsistensi dan efektivitasnya serta perlu dilakukan penyempurnaan dan *review* secara berkala.
7. Pengelolaan risiko belum menjadi bagian dari tugas dalam pengelolaan keamanan informasi sehingga perlu ditetapkan dan tidak terpisah dalam suatu kesatuan Sistem Manajemen Keamanan Informasi.
8. Diskominfo-SP Sulawesi Selatan belum mendefinisikan kepemilikan dan pihak pengelola (kustodian) aset informasi, inventaris aset eksisting tercantum dalam buku inventaris

- sumber daya yang dimiliki dengan tingkat kepemilikan asset dilakukan pada tiap bidang, namun berdasarkan inventaris tersebut, belum terdapat pengelompokan asset utama/penting yang akan menjadi modal dasar dalam melindungi keamanan informasi di dalamnya dan belum terdapat penanggung jawab yang akan melakukan pengelolaan terhadap asset saat terjadi kerusakan atau kehilangan.
9. Belum menjadikan pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan.

IV. ASPEK KERANGKA KERJA:

a. Kekuatan/Kematangan

1. Diskominfo-SP Sulawesi Selatan telah memiliki beberapa kebijakan pengelolaan TIK dimana di dalamnya terdapat aspek-aspek keamanan informasi dan dalam SOTK juga telah mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang dalam pengelola keamanan informasi yang tertuang dalam penjabaran tugas dan fungsi khususnya pada bidang Persandian.
2. Telah mencantumkan aspek keamanan informasi dalam kontrak dengan pihak ketiga berupa menjaga kerahasiaan pada Pergub tentang Penyelenggaraan TIK dan dengan merujuk pada dokumen kontrak dengan pihak ketiga, kriteria HAKI telah dicantumkan sebagai prasyarat.
3. Pemprov Sulawesi Selatan telah menjadikan aspek keamanan informasi menjadi bagian dari manajemen proyek, mekanisme tersebut ter gambarkan dalam proses *hardening* secara mandiri yang dilakukan sesuai dengan hasil pelaporan ITSA yang telah dilakukan oleh BSSN.
4. Telah memiliki strategi penerapan keamanan informasi namun belum disinkronisasikan dengan hasil analisa risiko organisasi, kondisi saat ini masih mengacu pada laporan ITSA yang dilakukan sebelumnya.
5. 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 pada dokumen Renstra dan DPA.

b. Kelemahan/Kekurangan

1. Belum ada kebijakan keamanan informasi terkait SMKI dan belum terdapat strategi berkelanjutan dalam 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 menetapkannya sebagai insiden keamanan informasi dalam suatu prosedur/SOP Penanganan Insiden.
3. Belum memiliki mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
4. 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)
5. Pemprov Sulawesi Selatan belum memiliki kebijakan dan prosedur keamanan informasi yang dibutuhkan berdasar hasil kajian risiko keamanan informasi maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan di mana kajian tersebut menghasilkan mitigasi tertentu yang dituangkan dalam kebijakan dan prosedur secara menyeluruh terhadap asset yang dimiliki.
6. Dalam pengaturan penyelenggaraan TIK pada aspek manajemen 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.
7. Konsekuensi dari pelanggaran kebijakan keamanan informasi masih belum didefinisikan, dikomunikasikan dan ditegakkan, baik di internal maupun eksternal Pemprov Sulawesi Selatan, saat ini ketentuan tersebut telah tercantum dalam dokumen konsep SMKI.
 8. Belum memiliki prosedur resmi dalam mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi yang dihadapi.
 9. 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.
 10. Belum menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian atau implementasi sistem baru serta menjadi upaya dalam menanggulangi permasalahan yang ada.
 11. 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.
 12. 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.
 13. Belum memiliki kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning/BCP*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya.
 14. 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.
 15. Belum melakukan evaluasi kelayakan secara berkala terhadap seluruh kebijakan dan prosedur keamanan informasi yang dimiliki.
 16. 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.
 17. 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.
 18. Belum melakukan pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada secara periodik.

V. ASPEK PENGELOLAAN ASET:

a. Kekuatan/Kematangan

1. Diskominfo-SP Sulawesi Selatan telah memiliki definisi klasifikasi informasi merujuk pada Peraturan Gubernur 26/2020 dan melakukan proses evaluasi aset dengan merujuk pada tugas sebagaimana yang telah tercantum dalam SOTK.
2. Telah memiliki peraturan terkait pengamanan lokasi kerja penting (ruang server) berupa mekanisme pemenuhan dan penyelenggaranya.
3. Telah memiliki kebijakan pengendalian hak akses termasuk ketentuan keamanan *data center* (perimeter fisik, akses masuk, pengamanan CCTV) dan pengaturan kualifikasi perangkat lunak.
4. Telah memiliki kebijakan klasifikasi keamanan dan akses arsip dinamis sampai dengan waktu penyimpanan dan metode pemusnahannya.

5. Telah memiliki kebijakan dan implementasi mekanisme pengamanan dan penggunaan aset organisasi dengan serangkaian ketentuan dari manajemen tingkat layanan sampai dengan datanya.

b. Kelemahan/Kekurangan

1. Diskominfo-SP Sulawesi Selatan telah memiliki daftar inventaris aset sumber daya namun belum terdapat penanganan secara komprehensif dan menyeluruh terhadap aset yang dimiliki.
2. Belum memiliki mekanisme proses penyidikan/investigasi penyelesaian insiden keamanan informasi.
3. Belum memiliki proses pelaporan insiden keamanan informasi dimana di dalamnya telah memiliki ketentuan yang perlu diperhatikan dalam proses pelanggaran hukum yaitu adanya keterlibatan pihak penegak hukum.
4. Belum memiliki prosedur kebijakan pengendalian hak akses yang mengatur *user* yang mutasi/keluar baik pegawai tetap maupun tenaga kontrak.
5. Belum memiliki peraturan pengamanan lokasi kerja penting (ruang server) berupa tata tertib himbauan masuk bagi pengguna/pengunjung layanan data center.
6. Belum memiliki kebijakan tingkatan akses yang berbeda dari setiap klasifikasi aset informasi, berikut *user access metrik* yang dapat merekam alokasi akses tersebut.
7. Belum memiliki kebijakan atau prosedur manajemen perubahan terhadap sistem, proses bisnis dan proses teknologi informasi termasuk pengelolaan, perubahan konfigurasi serta penerapan dari kebijakan manajemen perubahan belum dilakukan secara konsisten.
8. Belum memiliki proses merilis aset baru yang merujuk pada kebijakan tentang pengelolaan BMD dan proses pemutakhiran inventaris aset.
9. Pendefinisian tanggung jawab pengamanan informasi telah dilakukan pada pegawai ASN namun belum diberlakukan pada pegawai non ASN.
10. Belum memiliki kebijakan dan SOP terkait penggunaan komputer, email dan internet, yang digunakan sebagai panduan pelaksanaan keamanan informasi bagi pegawai.
11. 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*.
12. Belum memiliki mekanisme penggunaan data pribadi sebagai dasar pengaturan penggunaan data pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggungjawab.
13. Belum memiliki kebijakan proses otentikasi dan sanksi pelanggaran.
14. Belum memiliki kebijakan terkait dengan pertukaran data dengan pihak eksternal.
15. Belum memiliki proses pengecekan latar belakang seluruh SDM yang bekerja pada unit keamanan informasi melalui mekanisme *screening* baik pegawai non ASN maupun pihak ketiga (tenaga ahli/konsultan).
16. Belum memiliki tata cara pemusnahan barang TIK namun yang merujuk pada klasifikasi aset yang dimiliki organisasi.
17. Belum memiliki sumber daya dan prosedur dalam proses *backup* data/informasi.
18. Belum tersedia prosedur rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
19. Telah memiliki kebijakan pengendalian pihak ketiga namun belum terdapat ketentuan untuk memastikan kepatuhan terhadap kebijakan dan kontrak terkait dengan HAKI dan penggunaan perangkat keras/lunak.
20. Telah dilakukan penerapan keamanan fasilitas fisik termasuk pengelolaan alokasi kuncinya namun terbatas hanya pada *data center*, untuk ruang lingkup lainnya di Diskominfo belum diberlakukan.
21. Telah memiliki prosedur perlindungan terhadap infrastruktur komputasi dari dampak lingkungan maupun gangguan pasokan listrik namun penerapan dan evaluasi belum dilakukan secara berkala dalam menjaga ketersediaan dan keamanan layanan TIK di dalamnya.
22. Belum memiliki peraturan *mobile computing* dan *teleworking*, kebijakan peminjaman/pemindahan aset TIK berikut formulirnya, proses perawatan peralatan

komputasi dan mekanisme terkait dengan implementasi kebijakan pengendalian vendor seperti berita acara, *form* masuk keluar barang dan mekanisme kirim terima informasi melalui email dinas.

23. Belum memiliki kebijakan atau prosedur *backup server* dan mekanisme akses ruang secara berkala serta belum memiliki kebijakan keamanan fisik dan lingkungan (perimeter fisik, akses masuk, pengamanan CCTV).

VI. ASPEK TEKNOLOGI:

a. Kekuatan/Kematangan

1. Diskominfo Sulawesi Selatan telah menggunakan mekanisme perlindungan dengan antivirus, firewall (*embedded* pada router) dan SSL serta pengamanan dengan *password* dan telah melakukan segmentasi jaringan sesuai dengan kepentingannya.
2. Proses keamanan sistem pada seluruh asset jaringan, sistem dan aplikasi telah mengikuti perkembangan teknologi, eksisting saat ini menggunakan penerapan firewall pada rourer/mikrotik.
3. Telah dilakukan perlindungan terhadap seluruh perangkat desktop dan server. Untuk linux dengan *firewall* dan windows dengan windows defender yang dipelihara lisensinya secara rutin.
4. Telah menggunakan mekanisme sinkronisasi waktu secara akurat dengan *Network Time Protocol*.
5. Telah menerapkan pengelolaan sistem dengan bentuk pengamanan berlapis yaitu pada aplikasi yang dimiliki dengan menggunakan *captcha* termasuk aplikasi <https://epinisi.sulselprov.go.id>.

b. Kelemahan/Kekurangan

1. Belum memiliki standar konfigurasi sistem, jaringan dan aplikasi serta proses analisa kepatuhan penerapan konfigurasi sesuai standar yang ada.
2. Belum memiliki kebijakan pengendalian/pengelolaan konfigurasi.
3. Belum melakukan monitoring infrastruktur jaringan, sistem dan aplikasi.
4. Belum adanya proses perekaman dalam setiap perubahan dalam sistem informasi.
5. Belum diberlakukan penerapan penggantian *password* secara otomatis dan dibuat kebijakan penggunaan kompleksitas *password*.
6. Belum adanya pemberlakuan pembatasan waktu akses otomatisasi dengan durasi *destroy session time out*.
7. Telah dilakukan kegiatan *vulnerability assessment* namun belum dilakukan secara berkala baik pada penjadwalannya maupun keseluruhan sistem dan aplikasi yang telah dimiliki.
8. Belum memiliki konsep penyediaan redundant terhadap keseluruhan infrastruktur jaringan, sistem dan aplikasi yang dimiliki, masih sebatas *back up database* dan aplikasi.
9. Analisa log belum dilakukan, masih bersifat insidental dan belum ada penjadwalan yang dilakukan secara periodik.
10. Belum adanya implementasi penggunaan enkripsi sesuai kebijakan yang telah ditetapkan termasuk penerapan pengamanan pengelolaan kunci enkripsi yang digunakan.
11. Belum menerapkan mekanisme pendekripsi dan pencegahan penggunaan akses jaringan dengan menggunakan IDS/IPS.
12. Belum adanya pemutakhiran versi terkini perangkat server pada sistem operasi linux yaitu dengan Ubuntu versi 21/22.
13. Belum adanya mekanisme proses analisa secara rutin terhadap jejak audit *antivirus/antimalware*.
14. Belum dilakukan mekanisme laporan adanya penyerangan *virus/malware* yang gagal/sukses ditindaklanjuti dan diselesaikan yang juga didokumentasikan.
15. Belum memiliki kebijakan prasyarat pelaksanaan *penetration testing* terhadap setiap aplikasi yang dikembangkan namun belum dilakukan penerapan dan penjadwalan pengujian tersebut yang didokumentasikan sebagai bagian dari proses pengembangan aplikasi yang perlu dilakukan pemantauannya.

16. Belum menerapkan lingkungan pengembangan dan uji coba sesuai kriteria keamanan yang diberlakukan pada seluruh siklus hidup sistem yang telah dibangun.
17. Telah melibatkan pihak independen (BSSN) untuk mengkaji keandalan keamanan informasi baik pada sistem manajemen keamanan informasi maupun aplikasi yang dimiliki namun belum dilakukan secara rutin dan terjadwal (untuk kegiatan *penetration testing* belum secara rutin)

VII. ASPEK SUPLEMEN:

A. Kekuatan/Kematangan

1. Kebijakan dengan pihak ketiga saat ini tercantum dalam Pergub Penyelenggaraan TIK, dan belum terdapat turunannya yang digunakan sebagai dasar implementasinya pelaksanaan pengamanan informasi.
2. Data pribadi menjadi salah satu identifikasi asset data dalam pemetaan risiko sebagaimana yang ditetapkan.

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 turunan kebijakan perlindungan data pribadi, kajian risiko masih bersifat secara umum dan perlu dilakukan klasifikasi sesuai dengan tingkat kekritisan data pribadi

VIII. REKOMENDASI

1. Merujuk pada Pergub tentang SOTK dan Penyelenggaraan TIK, perlu ditetapkan secara spesifik pendelegasian tugas, wewenang dan tanggung jawab dalam pelaksanaan penerapan SMKI pada lingkup Diskominfo-SP Pemerintah Provinsi Sulawesi Selatan mulai dari perencanaan sampai dengan evaluasi serta pengujian kepatuhannya secara berkelanjutan (audit internal).
2. Perlu menyusun kebijakan pemetaan kebutuhan SDM yang akan mengawaki SMKI dan dengan memperhatikan kualifikasi kompetensi serta pemenuhan kebutuhannya secara periodik dalam rangka menjaga pengelolaan SMKI berjalan secara efektif dan efisien dengan tetap memperhatikan aspek dalam implementasi SPBE.
3. Agar pelaksanaan SMKI berjalan sesuai dengan ketentuan dan standar serta keamanan informasi yang telah ditetapkan, Diskominfo-SP Pemerintah Provinsi Sulawesi Selatan perlu menyusun dan mengevaluasi kebijakan sebagai berikut:
 - a. Penetapan identifikasi Data Pribadi berikut klasifikasi dan metode pengamanan yang diterapkan dengan merujuk pada Perkominfo 20 Tahun 2016 tentang Perlindungan Data Pribadi.
 - b. Pola koordinasi secara efektif baik internal maupun eksternal.
 - c. Kebijakan BCP dan DRP dalam menjaga keberlangsungan bisnis proses dan keamanan serta perlindungan aset organisasi secara terencana dan dilakukan monitoringnya secara rutin.
4. Agar menyusun kebijakan/panduan pengelolaan risiko yang 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 tahapan dalam proses manajemen risiko, yaitu risk assessment, risk mitigation, dan risk evaluation dan selanjutnya digunakan sebagai proses penerapan manajemen risiko di Pemprov Sulawesi Selatan khususnya pada lingkup Diskominfo secara sistematis dan terstruktur.
5. 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-SP Sulawesi Selatan 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-SP Sulawesi Selatan.
- 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-SP Pemprov Sulawesi Selatan.
- 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.
6. Agar menyusun kebijakan SMKI yang akan digunakan sebagai panduan dalam implementasi keamanan informasi secara menyeluruh dengan melibatkan/mengkomunikasikan kebijakan terkait pada pihak internal maupun eksternal sehingga akan lebih merasakan manfaat dengan keberadaan Diskominfo-SP sebagai *lead* dan penanggung jawab pelaksanaan keamanan informasi di Pemprov Sulawesi Selatan.
7. 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.
8. Perlu melakukan pengujian dan monitoring keamanan jaringan, sistem dan aplikasi yang dimiliki dengan menggunakan perangkat (*software/hardware*) dan mengoptimalkan SDM yang telah memiliki kualifikasi.
9. Agar melakukan monitoring secara rutin terhadap lingkungan fisik data center seperti:
 - a. Menjaga perimeter keamanan fisik mulai dari saat registrasi sampai dengan melakukan akses ke zona pemeliharaan.
 - b. Kelembapan suhu/udara untuk menjaga kestabilan dan suhu harus relatif merata di setiap sudut ruangan, dapat dilakukan pemasangan termometer dan hidrometer pada beberapa lokasi data center serta pengecekan secara berkala.
 - c. Kestabilan sumber daya listrik dari adanya pemadaman listrik, selain telah memiliki back up yang telah disediakan baik UPS dan genset, perlu mempertimbangkan efektifitas UPS yang bergantung pada kekuatan baterai (perlunya perawatan secara rutin terhadap baterai-baterai yang telah terpasang). Kemudian juga perlu menjaga kapasitas UPS supaya tidak kelebihan beban sehingga dapat memberikan daya dalam waktu yang cukup sebelum sumber daya cadangan beroperasi. Untuk genset, harus dipastikan ketersediaan bahan bakar dalam jumlah yang cukup dan dapat beroperasi dalam jangka waktu beberapa hari dan perlunya melakukan uji coba menghidupkan selama beberapa saat minimal sepekan sekali untuk memastikan kinerja genset tersebut dan perlu melakukan *load test* yang dilakukan minimal setahun sekali.
 - d. Perlunya upaya dari antisipasi kebakaran dengan langkah berupa gladi/simulasi penanggulangan kebakaran yang dapat dilakukan secara berkala terhadap APAR yang dimiliki, dengan juga memastikan *smoke detector* dan alarm data center berfungsi sebagai pendekripsi adanya asap/api yang muncul.
10. Perlu dibuat turunan kebijakan dari regulasi keamanan informasi berupa standar/prosedur penerapan kriptografi yang digunakan untuk melindungi informasi rahasia atau sensitif, penerapan prosedur *Secure SDLC* yang bertujuan untuk memberikan kepastian keamanan terhadap kontrol yang ada misal enkripsi dalam transfer informasi, standar penerapan kriptografi yang digunakan, pembuatan kunci untuk password dan lainnya.

11. 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.
12. Dengan merujuk pada standar TIA-942, maka topologi standar data center yang dipersyaratkan setidaknya memiliki 4 komponen utama yang perlu diperhatikan, yaitu jalur akses (pintu utama), ruang telekomunikasi, ruangan utama dan beberapa ruangan distribusi atau ruangan operasional. Dengan memperhatikan keempat komponen utama tersebut, maka diharapkan pengelolaan data center menjadi lebih murah, mudah untuk digunakan, dipelihara dan diperluas. Filosofi dasar pembuatan data center terkait erat dengan 5 prinsip dimana desain data center harus sederhana (simplicity), desain data center memiliki ukuran yang relatif (scalability), desainnya harus bersifat modular (modularity) dan fleksibel (flexibility) dan mampu menunjang kebutuhan penggunaan jangka panjang sehingga diperlukan ruang kerja yang nyaman dan aman (sanity).
13. 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 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 perundangan yang telah ada.

Penutup

Demikian Laporan Penilaian Indeks Keamanan Informasi pada Dinas Komunikasi Informatika Statistik dan Persandian Provinsi Sulawesi Selatan ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam Pelaksanaan Pengamanan Keamanan Informasi Pemerintah Daerah Provinsi Sulawesi Selatan. Agar Pemerintah Daerah Provinsi Sulawesi Selatan melaksanakan tindak lanjut atas hasil observasi dan rekomendasi yang disampaikan pada Laporan Penilaian Indeks Keamanan Informasi ini dan melaporkan tindak lanjutnya kepada BSSN.

Laporan Penilaian Indeks Keamanan Informasi ini disusun rangkap 2 (dua) untuk disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara; dan
2. Gubernur Provinsi Sulawesi Selatan.

Kepala Bidang Persandian



Riswan, S.Sos.,M.M.
NIP. 19670121 199003 1 004

Makassar, 16 Juni 2022

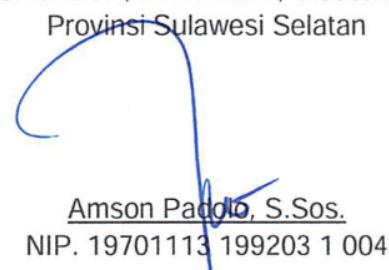
Koordinator Tata Kelola Kamsibersan Pemda
selaku Lead Asesor



Lukman Nul Hakim, S.E.,M.M.
NIP. 19701116 199110 1 002

Mengetahui,

Kepala Dinas Komunikasi, Informatika, Statistik dan Persandian
Provinsi Sulawesi Selatan



Amson Pacilio, S.Sos.
NIP. 19701113 199203 1 004