
	LAPORAN ONSITE ASSESSMENT INDEKS KAMI	 INDEKS KEAMANAN INFORMASI
Instansi/Perusahaan: PEMERINTAH DAERAH PROVINSI KALIMANTAN SELATAN	Pimpinan Unit Kerja : Dr. H. Muhamad Muslim. S.Pd, M.Kes NIP. 196803111989031003	
Unit Kerja: DINAS KOMUNIKASI DAN INFORMATIKA (DISKOMINFO)	Narasumber Instansi/Perusahaan : 1. M. Noor Ikhwanadi, SH., MM. NIP. 19740721 200903 1 004 2. Yaula Stellamaris, SE., MT NIP. 19750222 199602 2 001 3. Dian Arifin, S.Kom NIP. 19711024 199803 1 010 4. H. Joko Santoso, S.Kom NIP. 19780708 201001 1 015 5. Abdul Hafizh, S.Kom. NIP. 19870520 201503 1 001 6. Febri Riswandi, S.Kom NIP. 19810202 201201 1 001 7. Erix agus Panca S 8. Tajrian Noor Juniardi 9. Winda Andrini Wulandari, S. Kom, M. Kom	
Alamat: Jalan Dharma Praja II Kawasan Perkantoran Pemerintah Provinsi Kalimantan Selatan		
Email: diskominfo@kalselprov.go.id	Asesor : 1. Firman Maulana, S.E. NIP. 19740503 199312 1 001 2. Diah Sulistyowati, S.Kom., M.T. NIP. 19820925 200212 2 001 3. Mochamad Jazuly, S.S.T.TP NIP. 19920625 20141212 1 002 4. Faizal Wahyu Romadhon, S.Tr.TP NIP. 19960216 201712 1 004	
Tel/ Fax : Tlp: 0511-6749844 Fax: 0511-6749844		

A. Ruang Lingkup:

1. Instansi / Unit Kerja:
Layanan Data Center/ Ruang Server dan Sistem Informasi yang dikelola oleh Dinas Komunikasi dan Informatika, Pemerintah Provinsi Kalimantan Selatan.
2. Fungsi Kerja:
Sebagaimana Peraturan Gubernur Kalimantan Selatan Nomor 72 Tahun 2020 tentang Tugas, Fungsi dan Uraian Tugas Dinas Komunikasi dan Informatika, Provinsi Kalimantan Selatan memiliki tugas pokok melaksanakan urusan Pemerintahan yang menjadi kewenangan Daerah dan tugas pembantuan di bidang Komunikasi dan Informatika, Statistik dan Persandian. Dalam menyelenggarakan tugas tersebut, Diskominfo memiliki fungsi sebagai berikut :
 - a. perumusan kebijakan teknis bidang Komunikasi, Informatika, Statistik dan Persandian;
 - b. pelaksanaan kebijakan teknis pengelolaan dan layanan informasi publik;
 - c. pelaksanaan kebijakan teknis pengembangan dan pengelolaan data statistik;
 - d. pelaksanaan kebijakan teknis pengelolaan opini dan kemitraan komunikasi publik;
 - e. pelaksanaan kebijakan teknis pengembangan aplikasi dan tata kelola *E-Government*;
 - f. pelaksanaan kebijakan penyediaan dan pengelolaan infrastruktur TIK;
 - g. pelaksanaan kebijakan teknis pengamanan informasi dan persandian;
 - h. pembinaan, pengawasan dan pengendalian UPTD; dan
 - i. pengelolaan kegiatan kesekretariatan.

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor dan Ruang Server Dinas Komunikasi dan Informatika Pemprov Kalimantan Selatan	Jalan Dharma Praja II Kawasan Perkantoran Pemerintah Provinsi Kalimantan Selatan

B. Nama /Jenis Layanan Publik:

Layanan Infrastruktur Data Center/ Ruang Server dan aplikasi sistem informasi <https://eperformance.kalselprov.go.id> yang dikelola oleh Dinas Komunikasi dan Informatika Provinsi Kalimantan Selatan.

C. Aset TI yang kritis:

1. Aplikasi:
Memiliki 35 aplikasi yang dikelola oleh Diskominfo Pemprov Kalimantan Selatan baik yang hosting di dalam maupun di luar Diskominfo.
2. Server :
 - Server kalselprov.go.id
3. Infrastruktur Jaringan/Network:
 - ISP Samudra, Metro, Icon+ dan Indihome

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

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

Dokumen yang diperiksa:

1. Peraturan Gubernur Provinsi Kalimantan Selatan Nomor 72 Tahun 2020 tentang Tugas, Fungsi dan Uraian Tugas Dinas Komunikasi dan Informatika, Provinsi Kalimantan Selatan;
2. Peraturan Gubernur Provinsi Kalimantan Selatan Nomor 039 Tahun 2018 tentang Sistem Pengelolaan TIK;
3. Renstra Perangkat Daerah 2021-2026 Provinsi Kalimantan Selatan Dinas Komunikasi dan Informatika;
4. Daftar Perencanaan Anggaran Bidang Persandian Tahun 2022;
5. Peraturan Gubernur Provinsi Kalimantan Selatan Nomor 019 Tahun 2019 tentang Pengelolaan Pengaduan Pelayanan Publik melalui Media Komunikasi Elektronik di Provinsi Kalimantan Selatan;
6. Kebijakan Keamanan Informasi Diskominfo Provinsi Kalimantan Selatan Nomor 555/341/sandikami;
7. Kebijakan Manajemen Risiko Keamanan Teknologi Informasi Nomor 555/342/sandikami;
8. Surat Keputusan Gubernur Provinsi Kalimantan Selatan Nomor 188.44/078/KUM/2020 tentang Pembentukan *Computer Security Incident Response Team* Provinsi Kalimantan Selatan;
9. Peraturan Gubernur Provinsi Kalimantan Selatan Nomor 0113 Tahun 2017 tentang Pengembangan dan Penerapan E-Government di Pemerintah Provinsi Kalimantan Selatan;

10. Peraturan Gubernur Provinsi Kalimantan Selatan Nomor 1 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik;
11. Peraturan Gubernur Provinsi Kalimantan Selatan Nomor 70 Tahun 2018 tentang Pedoman Penerapan Sistem *Government Service Bus* di Lingkungan Pemerintah Provinsi Kalimantan Selatan;
12. Keputusan Gubernur Kalimantan Selatan Nomor 188.44/0278/KUM/ 2018 tentang Pembentukan Tim Pengelola Layanan Informasi dan Dokumentasi Provinsi Kalimantan Selatan;
13. Nota Kesepahaman Bersama (MoU) Diskominfo dengan Subdit V Keamanan Khusus Direktorat Intelkam Polda Kalimantan Selatan;
14. Sosialisasi Peraturan Gubernur Kalimantan Selatan Nomor 079 Tahun 2021 Tentang Penyelenggaraan Sertifikat Elektronik Di Lingkungan Pemerintah Daerah;
15. Cascading Pohon Kinerja Dinas Komunikasi dan Informatika, Provinsi Kalimantan Selatan;
16. Dokumen Perjanjian Kinerja Kepala Dinas Komunikasi dan Informatika, Provinsi Kalimantan Selatan;
17. Berita Acara Kegiatan dan Serah Terima Laporan Layanan Honeynet dengan BSSN;
18. Berita Acara tentang Audit Penyelenggaraan Persandian Pemerintah Daerah Provinsi Kalimantan Selatan TA.2020;
19. Laporan Pelaksanaan ITSA Portal Data, CSIRT KalselProv;
20. Keputusan Kepala Dinas Komunikasi dan Informatika, Provinsi Kalimantan Selatan No. 10.4 Tahun 2020 tentang Klasifikasi Informasi Publik yang dikecualikan di lingkungan Pemprov Kalimantan Selatan;
21. SOP Pengelolaan Manajemen Risiko Keamanan Informasi No. 800/415/Sandikami-Diskominfo;
22. SOP Implementasi Aset Baru No. 800/407/Sandikami-Diskominfo;
23. SOP Pengecualian Terhadap Prosedur Keamanan Informasi No. 800/406/Sandikami-Diskominfo;
24. SOP Prosedur Implementasi Security Patch No. 800/408/Sandikami-Diskominfo;
25. SOP Pengelolaan Konfigurasi Perangkat;
26. SOP Perubahan Konfigurasi Perangkat No. 800/405/Sandikami-Diskominfo;
27. SOP Perubahan Proses Bisnis No. 800/402/Sandikami-Diskominfo;
28. SOP Penanganan Insiden Siber (CSIRT) No. 800/404/Sandikami-Diskominfo;
29. SOP Penyusunan Kebijakan Keamanan Informasi No. 800/413/Sandikami-Diskominfo;
30. Tata Tertib Penggunaan Email, Penggunaan Internet dan Intranet, Komputer dan Pengamanan Perangkat Komputer di luar kantor Diskominfo Provinsi Kalimantan Selatan;
31. Laporan serangan pada jaringan server bulan Januari sd Maret TA2022;
32. Laporan Anomali Insiden Siber Diskominfo Prov. Kalsel bulan April sd. Juni TA2022;
33. Laporan Penerapan Skenario pengamanan jaringan komputer pada router tahun 2018 sd 2020;
34. Laporan Analisa Teknis Temuan Website Portal Data, EAbsen dan CSIRT;
35. Hasil Identifikasi Penilaian Risiko aset Hardware, Software dan Informasi;
36. Berita Acara Serah Terima Pemakaian (Penempatan) Barang Inventaris berupa server Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu;
37. Rekapitulasi Identifikasi Alokasi Investasi Total belanja modal pembangunan sistem elektronik E-Performance;
38. Bahan Paparan Pengamanan Informasi Diskominfo Provinsi Kalimantan Selatan;
39. NDA Penerapan Firewall Fortinet dan Firewall Cisco di lingkungan Diskominfo Provinsi Kalimantan Selatan;
40. Laporan Insiden Siber pada Aplikasi Email Resmi Kalimantan Selatan;

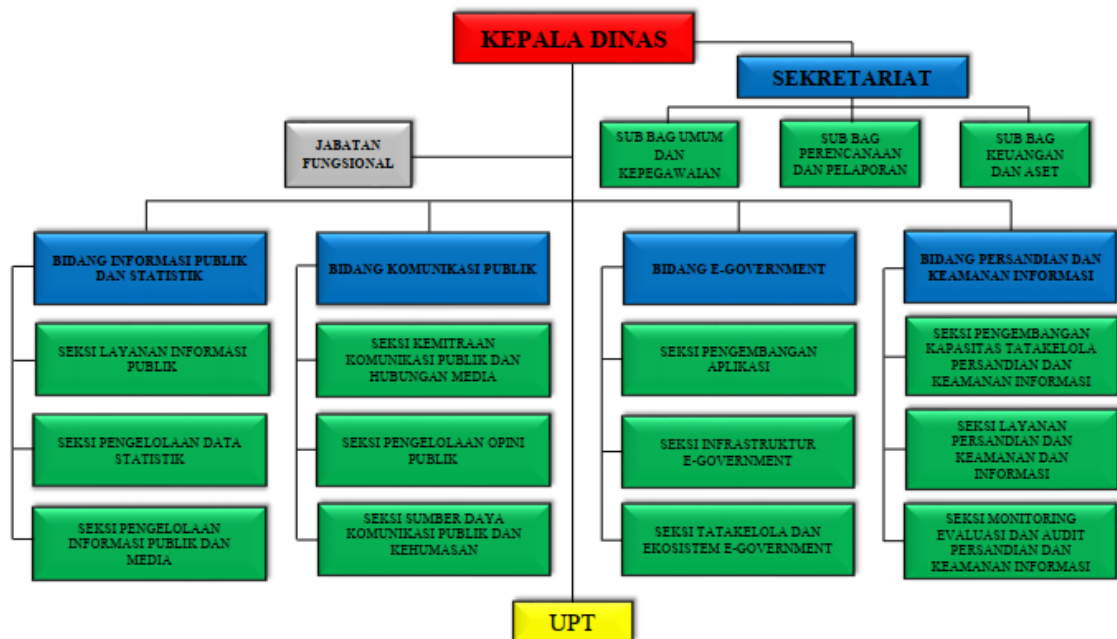
Bukti-bukti (rekaman/arsip) penerapan SMKI:

1. Gambar Topologi Jaringan Server;
2. Tangkapan layar Sistem Login aplikasi Simpeg-Kalsel dan APIK;
3. Tangkapan layer e-dialog kinerja akun pejabat eselon 4;
4. Tangkapan layer *mindmap* regulasi kebijakan keamanan informasi pada Dinas Komunikasi dan Informatika, Provinsi Kalimantan Selatan;
5. Tangkapan Layar konfigurasi jaringan, penggunaan SSL aplikasi *E-performance*.

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

I. KONDISI UMUM:

1. Diskominfo Kalimantan Selatan dibentuk berdasarkan Peraturan Gubernur Provinsi Kalimantan Selatan Nomor 72 Tahun 2020 tentang Susunan Organisasi, Tugas, Fungsi, dan Tatakerja Dinas Komunikasi dan Informatika, Provinsi Kalimantan Selatan, berikut struktur Diskominfo Pemprov Kalimantan Selatan adalah sebagai berikut:



Gambar 1. Struktur Organisasi Diskominfo Pemprov Kalimantan Selatan

2. SDM pengelola terdiri dari: (berdasarkan dokumen Renstra)

No	Status Kepegawaian	Jumlah	Prosentase
1	PNS	39	22,94%
2	TKK/Tenaga Kontrak/Abdi Persada	131	77,06%
Jumlah		170	100%

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

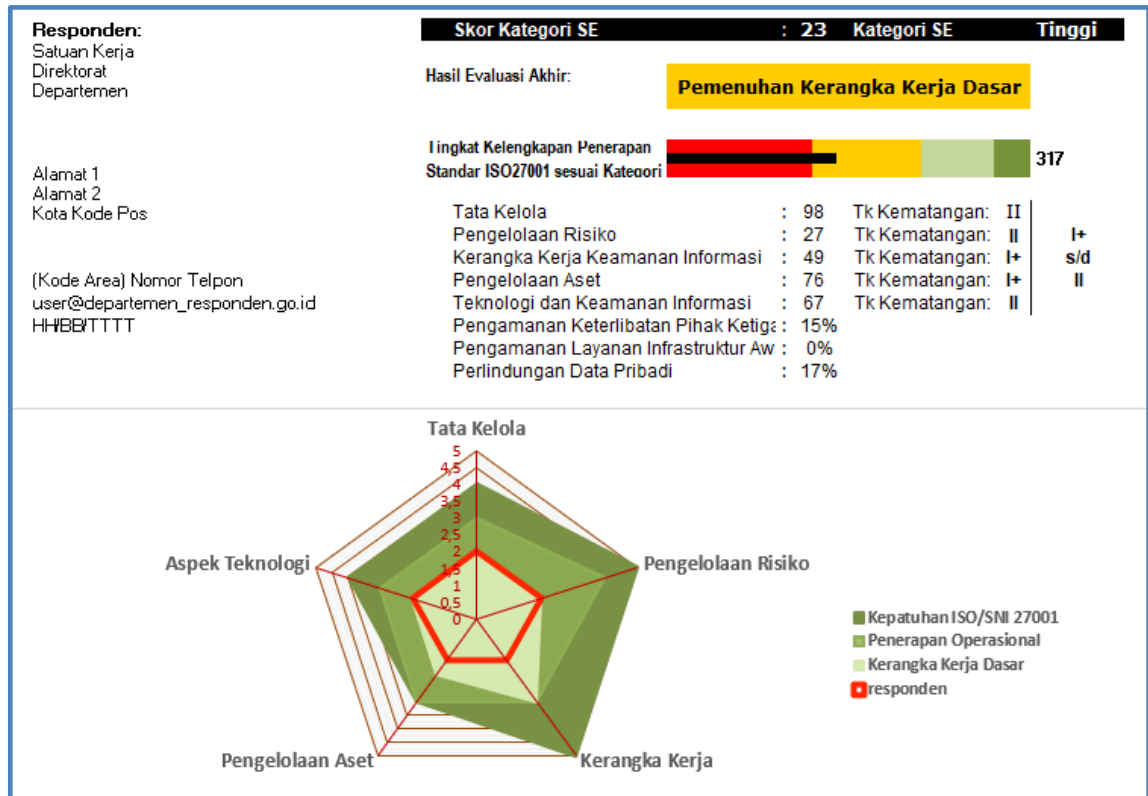
Penilaian Mandiri Indeks KAMI dilakukan di tahun 2022 ini dengan ruang lingkup Diskominfo Pemerintah Provinsi Kalimantan Selatan, Ruang Server dan Sistem Informasi yang dikelola dan dilakukan verifikasi oleh Tim BSSN dengan kategori **Tinggi** dan hasil evaluasi akhir **Pemenuhan Kerangka Kerja Dasar** dengan total nilai **317**.

Pada tahun 2022 ini merupakan periode kali pertama bagi lingkup Diskominfo Pemerintah Provinsi Kalimantan 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.

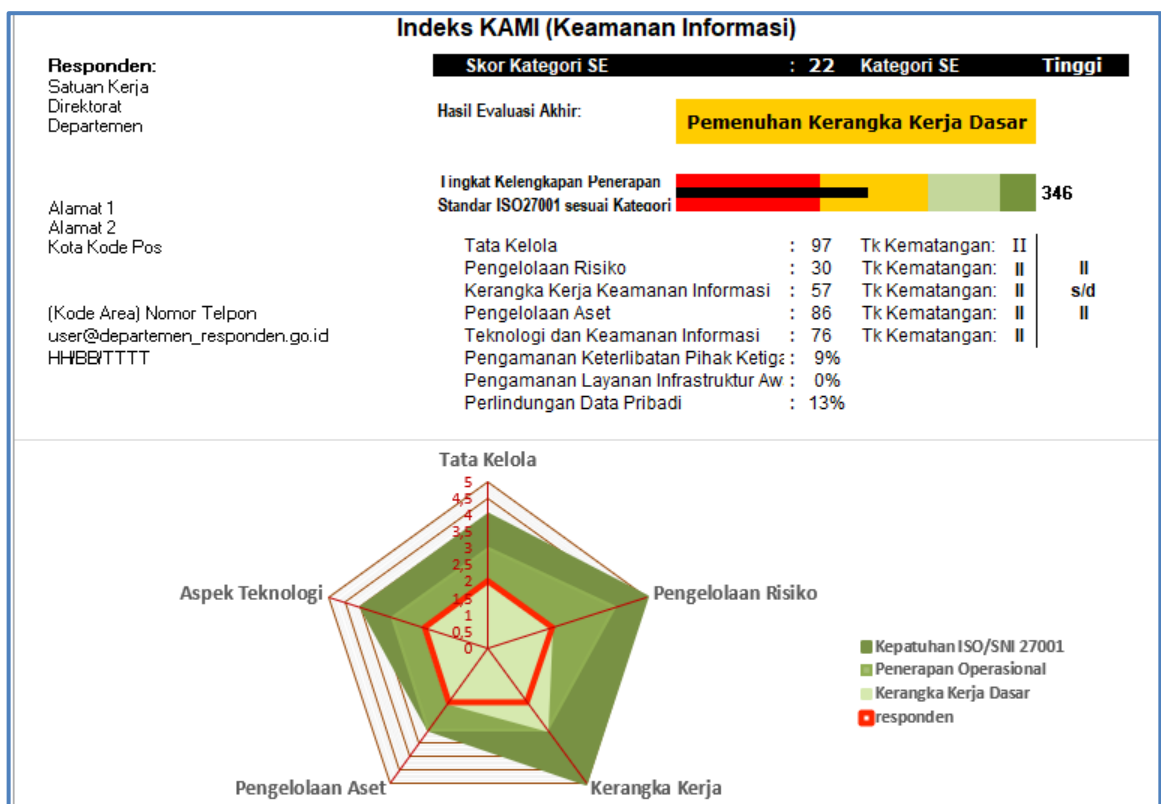
Pada pelaksanaan verifikasi, Tim Asesor berupaya untuk membantu dan mengarahkan lingkup Diskominfo Pemerintah Provinsi Kalimantan Selatan untuk dapat memperbaiki dan meningkatkan implementasi Keamanan Informasi sesuai ruang lingkup Diskominfo melalui penyediaan data dukung/ *evidence* berikut penerapan 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 Kalimantan Selatan secara lebih optimal.

Total Score Sebelum Verifikasi: 317 (ref. file Indeks KAMI v4.2 pra Verifikasi)



Total Score Setelah Verifikasi: 346 (ref. file Indeks KAMI v4.2 pasca Verifikasi)



II. ASPEK TATA KELOLA:

A. Kekuatan/Kematangan

1. Dinas Komunikasi dan Informatika (Diskominfo) Kalimantan Selatan telah memiliki dokumen kebijakan Perencanaan strategis mulai dari RPJMD, Renstra dan DPA yang menjadi dasar dalam pelaksanaan program keamanan informasi serta kebijakan Penerapan Sistem *Government Service Bus*, SPBE dan *masterplan* roadmap TIK.
2. Pelaksanaan tugas dan fungsi keamanan informasi saat ini tercantum dalam Pergub 72 Tahun 2020 tentang SOTK Pemprov Kalimantan Selatan.
3. Telah melakukan program peningkatan kesadaran pemahaman keamanan informasi khususnya pada lingkup jajaran Diskominfo Kalimantan Selatan;
4. Telah memiliki penetapan indikator kinerja yang ditetapkan melalui Indikator Kinerja Utama dan Sasaran Kerja Pegawai yang digunakan sebagai parameter pengelolaan keamanan informasi dan telah dilakukan monitoringnya;
5. Telah mengintegrasikan persyaratan keamanan informasi melalui kesesuaian ketentuan yang sudah tercantum dalam kebijakan keamanan informasi dan yang terkait seperti Penerapan Sistem *Government Service Bus*, SPBE.
6. Telah menjadikan pemasalahan keamanan informasi menjadi konsiderans dan perhatian pimpinan dalam pengambilan kebijakan atau keputusan strategis di Diskominfo Kalimantan Selatan berdasarkan hasil penyampaian laporan kondisi keamanan informasi dan dengan mempertimbangkan sumber daya yang tersedia saat ini.
7. Telah dilakukan penilaian kinerja pengelola keamanan informasi secara hirarki dari level pimpinan sampai dengan pelaksana dengan menggunakan E-dialog kinerja dan pelaporan operasional teknis keamanan informasi lainnya.
8. Telah mendefinisikan dan menyusun prosedur penanggulangan insiden dengan melibatkan pihak penegak hukum yang tertuang dalam dokumen kesepakatan bersama kedua belah pihak (MoU) antar Diskominfo Kalimantan Selatan dengan Direktorat Intelkam Polda Kalimantan Selatan.

B. Kelemahan/Kekurangan

1. Dalam pelaksanaan pembagian peran fungsi pelaksana pengamanan informasi belum dipetakan dalam peta jabatan secara lengkap terhadap penerapan sistem manajemen keamanan informasi secara lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan.
2. Belum adanya alokasi sumber daya yang memadai dalam pengelolaan dan menjamin kepatuhan program penerapan keamanan informasi.
3. Diskominfo Provinsi Kalimantan Selatan belum mendefinisikan persyaratan/standar kompetensi dan keahlian secara menyeluruh baik pada level koordinator maupun pelaksana pengelolaan keamanan informasi dan 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.
4. Telah melakukan identifikasi data pribadi dalam proses kerja dan menerapkan metode keamanannya melalui metode pembatasan akses namun belum adanya penyesuaian standar keamanan terhadap ketentuan peraturan/kebijakan perundangan yang telah ditetapkan.
5. 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.
6. 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 menyelesaikan permasalahan yang ada.
7. 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.

8. 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.
9. Belum adanya hasil identifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi secara komprehensif dari level paling tinggi sampai dengan prosedur yang digunakan untuk dipatuhi serta belum dilakukan proses analisis tingkat kepatuhan terhadap kebijakan yang telah didefinisikan tersebut.

III. ASPEK RISIKO:

a. Kekuatan/Kematangan

1. Diskominfo Pemprov Kalimantan Selatan telah memiliki program kerja, kerangka kerja pengelolaan risiko yang juga telah mencakup definisi, hubungan tingkat klasifikasi aset informasi, tingkat ancaman, dampak kerugian, penetapan ambang batas tingkat risiko keamanan informasi melalui selera risiko dan tertuang dalam kebijakan manajemen risiko Keamanan Teknologi yang telah ditetapkan dan digunakan secara resmi.
2. Telah mendefinisikan kepemilikan dan pengelola, ancaman dan kelemahan serta dampak kerugian termasuk aset utama yang terkait dengan hilangnya/terganggunya fungsi aset utama yang dimiliki Diskominfo Kalimantan Selatan namun belum dilakukan secara menyeluruh terhadap aset TIK yang dimiliki secara keseluruhan.

b. Kelemahan/Kekurangan

1. Belum menetapkan penanggung jawab manajemen risiko dan bentuk eskalasi pelaporan status pengelolaan risiko penerapan keamanan informasi sampai level tingkat pimpinan di Diskominfo Pemprov Kalimantan Selatan.
2. Inisiatif analisa/kajian risiko keamanan informasi masih berupa konseptual dan digunakan sebagai bahan dalam mengidentifikasi langkah mitigasi dalam program pengelolaan keamanan informasi yang akan dilakukan.
3. Telah menyusun rencana langkah mitigasi risiko dan skala prioritas penyelesaiannya namun belum ditetapkan dan digunakan sebagai bahan evaluasi program penilaian risiko (risk register) di Diskominfo Pemprov Kalimantan Selatan.
4. Kebijakan penyelesaian langkah mitigasi risiko dituangkan dalam konsep rekomendasi kontrol namun implementasinya belum dilakukan secara menyeluruh dan belum dilakukan pemantauan secara berkala dalam memastikan konsistensi dan efektivitasnya serta belum dilakukan pengkajian secara berkala.
5. Pengelolaan risiko belum menjadi bagian dari tugas dalam pengelolaan keamanan informasi sehingga perlu ditetapkan dan tidak terpisah dalam suatu kesatuan Sistem Manajemen Keamanan Informasi.
6. Belum menjadikan pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan dalam rangka menjamin kesesuaian, kecukupan dan efektivitas pelaksanaan penilaian risiko secara berkesinambungan.

IV. ASPEK KERANGKA KERJA:

a. Kekuatan/Kematangan

1. Kebijakan keamanan informasi terkait SMKI dan sebagian dari turunannya telah ditetapkan, namun belum mencantumkan pembagian peran dan tanggung jawab pihak-pihak secara spesifik yang akan menjalankan penerapannya serta belum dipublikasikan kebijakan SMKI tersebut menjadi program rutin yang disampaikan pada seluruh karyawan dan pihak terkait lainnya serta belum ditempatkannya kebijakan tersebut dalam suatu media yang dapat diakses oleh pihak-pihak yang membutuhkan.

2. Diskominfo Pemprov Kalimantan Selatan telah mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkan sebagai insiden keamanan informasi dalam suatu prosedur/SOP Penanganan Insiden.
3. Konsekuensi dari pelanggaran kebijakan keamanan informasi telah didefinisikan, dikomunikasikan dan ditegakkan, baik lingkup internal maupun eksternal Pemprov Kalimantan Selatan.
4. Telah memiliki prosedur resmi dalam mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi yang dihadapi dan prosedur operasional untuk pengelolaan implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, sampai dengan memastikan pemasangan dan pelaporannya.
5. Telah dilakukan 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 proses komunikasi kebijakan keamanan melalui publikasi kebijakan maupun prosedur keamanan informasi dan peningkatan *security awareness* namun belum dilakukan secara periodik dan berkelanjutan
6. Penerapan proses untuk mengevaluasi risiko terkait rencana pembelian atau implementasi sistem baru serta menjadi upaya dalam menanggulangi permasalahan yang ada telah dilakukan namun belum dilakukan secara menyeluruh terhadap adanya kebutuhan peningkatan keamanan informasi berdasarkan prioritas maupun jadwal yang ditetapkan.
7. Telah menerapkan proses pengembangan sistem yang aman (*Secure SDLC*) dengan menggunakan framework laravel yang secara langsung telah membantu dalam menangani berbagai masalah seperti *web defacement*, *sql injection*, dan membantu dalam proses sanitasi data serta validasi data dengan baik.
8. Telah menerapkan proses untuk menanggulangi dan penerapan pengamanan baru (*compensating control*) serta jadwal penyelesaiannya.
9. 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.
10. Diskominfo Pemprov Kalimantan Selatan telah melakukan evaluasi kelayakan secara berkala terhadap sebagian kebijakan dan prosedur keamanan informasi yang dimiliki dan menjalankan sebagian evaluasi dan pengujian terhadap tingkat kepatuhan program keamanan informasi.

b. Kelemahan/Kekurangan

1. Belum memiliki mekanisme dalam pengelolaan dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
2. Diskominfo Pemprov Kalimantan Selatan 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.
3. Dalam pengaturan penyelenggaraan TIK pada aspek manajemen keamanan informasi dengan pihak ketiga belum memiliki menerapkan secara menyeluruh aspek kerahasiaan, mekanisme pelaporan insiden, HAKI, tata tertib penggunaan dan pengamanan aset dalam kontrak dengan pihak ketiga yang telah didefinisikan oleh Pemprov Kalimantan Selatan.
4. Belum memiliki strategi penerapan keamanan informasi yang merupakan hasil dari analisis risiko untuk mendukung tugas dan fungsi Diskominfo Pemprov Kalimantan Selatan.
5. Belum memiliki kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning/BCP*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya.
6. 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.

7. Belum memiliki inisiasi melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan dengan hasil penetapan kontrol perbaikan yang akan dilakukan dalam periode waktu sesuai rencana kerja program organisasi.
8. Belum melakukan evaluasi tingkat kepatuhan terhadap pelaksanaan audit internal yang dilakukan secara konsisten dan berkelanjutan sebagai upaya perbaikan dan peningkatan kinerja keamanan informasi yang dilaporkan kepada pimpinan di Diskominfo Pemprov Kalimantan Selatan.

V. ASPEK PENGELOLAAN ASET:

a. Kekuatan/Kematangan

1. Diskominfo Kalimantan Selatan telah memiliki tata tertib penggunaan komputer, email, internet dan intranet.
2. Telah memiliki definisi klasifikasi informasi merujuk pada dokumen kebijakan SMKI, dimana telah dilakukan proses evaluasi dan pengklasifikasian tingkat kepentingan pengamanannya, serta proses perekamannya.
3. Telah menerapkan proses pelaporan insiden keamanan informasi kepada pihak eksternal maupun pihak berwajib yang telah tertuang dalam MoU dengan Polda.
4. Telah tersedia tingkatan akses yang berbeda dari setiap klasifikasi aset informasi, matriks yang dapat merekam alokasi akses tersebut.
5. Belum dilakukan proses merilis aset baru yang merujuk pada kebijakan tentang pengelolaan dan pemutakhiran inventaris aset.
6. Telah memiliki daftar inventaris aset sumber daya yang terpelihara termasuk kepemilikan aset.
7. Telah memiliki kebijakan atau prosedur manajemen perubahan terhadap sistem, proses bisnis dan proses teknologi informasi termasuk pengelolaan, perubahan konfigurasi serta penerapan dari kebijakan manajemen perubahan namun belum dilakukan secara konsisten.
8. Telah memiliki pengaturan kebijakan pengamanan lokasi kerja penting (ruang server) berupa mekanisme pemenuhan dan penyelenggaraannya serta memiliki kebijakan pengendalian hak akses termasuk ketentuan keamanan *data center* (perimeter fisik, akses masuk dua lapis, secara manual dan digital).
9. Telah memiliki prosedur integrasi dan pertukaran data sistem informasi yang diimplementasikan pada lingkup Pemprov Kalimantan Selatan.
10. Telah memiliki mekanisme penggunaan data pribadi sebagai dasar pengaturan penggunaan data pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggungjawab.
11. Telah melakukan pengelolaan identitas elektronik dan proses otentikasi termasuk kebijakan terhadap pelanggarannya.
12. Telah melakukan proses pengecekan latar belakang seluruh SDM yang bekerja pada unit keamanan informasi melalui mekanisme screening baik pegawai ASN, non ASN maupun pihak ketiga (tenaga ahli/konsultan).
13. Telah memiliki ketersediaan pasokan listrik melalui fasilitas UPS dan genset yang dilakukan perawatannya secara berkala serta telah memiliki sistem grounding untuk menangkal petir.

b. Kelemahan/Kekurangan

1. Prosedur kebijakan pengendalian hak akses yang mengatur *user* yang mutasi/keluar baik pegawai tetap maupun tenaga kontrak belum ditetapkan.
2. Prosedur/kebijakan *back-up* dan *restore* serta penanggung jawab telah didefinisikan namun masih berupa konsep.
3. Telah memiliki mekanisme perlindungan terhadap infrastruktur komputasi dari dampak lingkungan atau api, kondisi suhu dan kelembapan serta gangguan pasokan listrik atau dampak petir namun penerapan belum dilakukan secara keseluruhan terhadap ketersediaan dan keamanan layanan TIK di dalamnya.
4. Belum tersedia prosedur rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.

5. Belum terdapat proses pemindahan aset TIK, memeriksa dan merawat perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi untuk menempatkan aset informasi penting yang diterapkan dalam program rutin keamanan informasi..
6. Belum terdapat peraturan secara eksplisit yang bertujuan untuk mengamankan lokasi kerja penting (ruang server/arsip) dari risiko yang membahayakan aset informasi.
7. Belum terdapat proses pengamanan lokasi kerja dari kehadiran pihak ketiga yang bekerja untuk kepentingan organisasi.

VI. ASPEK TEKNOLOGI:

a. Kekuatan/Kematangan

1. Diskominfo Kalimantan Selatan telah menggunakan mekanisme perlindungan aplikasi dengan SSL, penerapan Firewall Fortinet dan Firewall Cisco serta metode pengamanan melalui pembatasan login.
2. Telah melakukan segmentasi jaringan sesuai dengan kepentingannya dan disesuaikan dengan kebutuhan.
3. Telah dilakukan perlindungan terhadap seluruh perangkat desktop dan server. Untuk linux dengan antivirus default dan perangkat OS windows dengan menggunakan windows defender.
4. Telah menerapkan redundansi infrastruktur jaringan dengan Icon+, Metro, BGP.
5. Monitoring jaringan dengan menggunakan router *Operating Sistem*, Fortinet untuk mengontrol dan memantau akses secara terpusat dan menggunakan proxmox sebagai monitoring virtualisasi server.
6. Telah melakukan perekaman terhadap setiap perubahan dalam sistem informasi dalam log untuk mengidentifikasi kejadian/insiden.
7. Telah melakukan Analisa log secara berkala dan mendokumentasikannya dalam laporan hasil monitoring anomali.
8. Pengaturan akses masuk ke sistem pada jaringan dengan menggunakan konfigurasi Filter rule mikrotik Firewall.
9. Mekanisme pemberlakuan pembatasan waktu akses otomatisasi dengan durasi *destroy session time out* telah diterapkan.
10. Telah menggunakan mekanisme sinkronisasi waktu secara akurat dengan *Network Time Protocol*.

b. Kelemahan/Kekurangan

1. Proses analisa kepatuhan belum dilakukan secara rutin terhadap penerapan konfigurasi standar.
2. Implementasi penggunaan fungsi hash masih menggunakan md5.
3. Belum adanya mekanisme proses analisa secara rutin terhadap jejak audit *antivirus/antimalware*.
4. Belum memiliki kebijakan prasyarat pelaksanaan *penetration testing* terhadap setiap aplikasi yang dikembangkan termasuk penerapan dan penjadwalan pengujian tersebut yang didokumentasikan sebagai bagian dari proses pengembangan aplikasi yang perlu dilakukan pemantauannya.
5. Belum melakukan penerapan UAT atau *Security Testing* pada tahap pengembangan dan uji coba.
6. Belum menerapkan lingkungan pengembangan dan uji coba sesuai kriteria keamanan yang diberlakukan pada seluruh siklus hidup sistem yang telah dibangun secara menyeluruh.
7. Belum melibatkan pihak independen untuk mengkaji keandalan keamanan terhadap keseluruhan aplikasi yang dimiliki secara rutin dan terjadwal.

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

1. Kebijakan dengan pihak ketiga yang mencakup persyaratan pengendalian akses, penyediaan layanan pihak ketiga saat ini tercantum dalam kebijakan maupun pedoman sistem manajemen keamanan informasi.
2. Telah melakukan proses pemantauan terhadap pelaksanaan kinerja pihak ketiga untuk layanan yang diberikan dan dilaporkan kepada pimpinan.
3. Telah mendokumentasikan dokumen kertas/elektronik data pribadi yang diolah dan dipertukarkan dengan pihak eksternal.
4. Memiliki program peningkatan pemahaman terkait dengan keamanan informasi dan perlindungan data pribadi menjadi salah satu bahan materi dalam proses *transfer knowledge*.

B. Kelemahan/Kekurangan

1. Belum adanya mekanisme dan proses identifikasi risiko terhadap 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 kajian risiko dan pengelolaan pengamanan layanan infrastruktur awan (*cloud service*).
3. Belum memiliki kebijakan perlindungan data pribadi, kajian risiko masih bersifat secara umum dan perlu dilakukan klasifikasi sesuai dengan tingkat kekritisitas data pribadi yang digunakan dalam sistem elektronik Diskominfo Pemprov Kalimantan Selatan.S

VIII. REKOMENDASI

1. Berdasarkan kebijakan yang tertuang dalam Pergub tentang SOTK, prosedur dan ketentuan penerapan SMKTI yang telah disusun maka perlu dilakukan evaluasi dan penetapan terhadap pendelegasian tugas, wewenang dan tanggung jawab dalam pelaksanaan penerapan SMKTI pada lingkup Diskominfo Pemerintah Provinsi Kalimantan Selatan secara utuh mulai dari tahap perencanaan sampai dengan perbaikan berkelanjutan dalam rangka mewujudkan terselenggaranya keamanan informasi dan mewujudkan implementasi SPBE secara handal dan aman di Diskominfo Pemprov Kalimantan Selatan.
2. Perlu mengevaluasi hasil gap analisis kondisi penerapan keamanan informasi yang selanjutnya dilakukan tinjauan manajemen terhadap regulasi dan kebijakan yang telah dimiliki dan membuat pemetaan turunan kebijakan prioritas keamanan informasi sebagai landasan serta panduan operasional dalam melakukan pemantauan dan perbaikan secara berkelanjutan terhadap penerapan SMKTI di Pemprov Kalimantan Selatan.
3. Perlu menyusun kebijakan pemetaan kebutuhan SDM yang akan mengawaki SMKTI dan dengan memperhatikan kuantitas dan kualifikasi standar/persyaratan kompetensi serta pemenuhan kebutuhannya secara periodik dalam rangka menjaga pengelolaan SMKTI berjalan secara efektif dan efisien dengan tetap memperhatikan aspek dan indikator dalam implementasi SPBE.
4. Agar pelaksanaan SMKTI berjalan sesuai dengan ketentuan dan standar serta keamanan informasi yang telah ditetapkan, Diskominfo Pemerintah Provinsi Kalimantan Selatan perlu menyusun, menetapkan dan mengevaluasi kebijakan sebagai berikut:
 - a. Penetapan identifikasi Data Pribadi berikut klasifikasi dan standar pengamanan yang diterapkan dengan merujuk pada Perkominfo 20 Tahun 2016 tentang Perlindungan Data Pribadi maupun RUU PDP.
 - 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 monitoring dan pengujiannya secara rutin.
 - d. Identifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi secara komprehensif dari level paling tinggi sampai dengan prosedur yang digunakan sebagai dasar dalam evaluasi tingkat kepatuhan dalam penerapannya

5. Agar menerapkan program pengelolaan risiko yang telah disusun dan selanjutnya digunakan sebagai dasar dalam proses penerapan keamanan informasi terhadap keseluruhan aset TIK yang dimiliki dengan tetap memperhatikan aset kritis guna mewujudkan terselenggaranya pengelolaan bisnis proses serta pencapaian tujuan sesuai lingkup tugas dan fungsi Diskominfo Pemprov Kalimantan Selatan secara sistematis dan terstruktur.
6. Perlu menjadikan manajemen risiko sebagai budaya kerja dalam bisnis proses organisasi untuk mengurangi dampak yang merugikan baik individu maupun organisasi secara keseluruhan pada Diskominfo Pemprov Kalimantan Selatan. Penerapannya dapat dilakukan dengan ketentuan antara lain sebagai berikut:
 - a. Menjadikan manajemen risiko menjadi bagian dari tugas dan fungsi di Diskominfo Kalimantan 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 Pemprov Kalimantan 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 rencana mitigasi yang telah disusun.
 - d. Melakukan monitoring terhadap rencana mitigasi yang telah ditetapkan secara periodik atau menyusun *risk treatment plan* sebagai dasar dalam memetakan kelemahan dan mengetahui kekurangan sehingga dapat meminimalisir adanya eksploitasi dari pihak-pihak tertentu (ancaman yang timbul).
7. Agar menggunakan kebijakan SMKI yang telah ditetapkan sebagai panduan dalam implementasi penyelenggaraan keamanan informasi secara menyeluruh dengan melibatkan/mengkomunikasikan kebijakan terkait pada pihak internal maupun eksternal sehingga akan lebih merasakan manfaat dengan keberadaan Diskominfo sebagai *lead* dan penanggung jawab pelaksanaan keamanan informasi di Pemprov Kalimantan Selatan.
8. 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 operasional dan keamanan yang menjadi prasyarat maupun ketentuan yang perlu diperhatikan.
9. Perlu menetapkan tim audit internal TIK dan keamanan yang independen dengan kualifikasi memiliki pemahaman terhadap SNI ISO 19011, 31000, 27001, 270002, 9001, 55001 maupun peraturan BSSN nomor 4 tahun 2021.
10. Perlu melakukan pengujian dan monitoring keamanan jaringan, sistem dan aplikasi yang dimiliki secara rutin dengan menggunakan perangkat (*software/hardware*) dan mengoptimalkan SDM yang telah memiliki kualifikasi dan kompetensi.
11. Agar melakukan pemeliharaan dan monitoring secara rutin terhadap operasional dan lingkungan fisik data center antara lain adalah:
 - a. Melakukan analisis melalui kajian *bisnis impact analysis* penggunaan saluran kabel bawah tanah dengan pertimbangan terhadap kelangsungan operasional data center.
 - b. Menjaga perimeter keamanan fisik mulai dari tahap registrasi sampai dengan akses ke zona pemeliharaan serta perekaman melalui ketentuan maupun prasyarat lalu lintas masuk dan keluar personil baik internal maupun eksternal.
 - c. 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.
 - d. Sistem pendingin ruangan pada Data Center memiliki fungsi dan peran khusus sebagai *thermal management* bagi perangkat IT dan server agar tidak terjadi *overheating* pada perangkat yang berada di dalamnya, maka perlu dipertimbangkan pendingin khusus seperti *Precision Air Conditioning* (PAC) yang akan membantu menstabilkan suhu/temperature dan kelembaban (*relatif humidity*) secara konstan dan akan mempertahankan suhu dan kelembaban yang telah disesuaikan sesuai dengan kebutuhan perangkat komputer di dalam ruangan tersebut.

12. Perlu adanya pelaksanaan dan pengelolaan baik *Business Continuity Plan* dan *Disaster Recovery Plan* (DRP) sebagai upaya dalam menjaga kelangsungan TIK dan menjadi bagian rencana tindakan (*response plan*) dalam mengantisipasi terjadinya bencana. Dalam penyusunannya, dapat menggunakan standar SNI ISO 22301 maupun best practice lainnya. Penyusunan DRP memerlukan beberapa proses seperti pencatatan seluruh aset (layanan TI) yang dimiliki oleh organisasi, pencatatan risiko-risiko negatif yang berpotensi menjadi sebuah bencana bagi organisasi, serta analisis dampak bisnis sebagai pertimbangan keputusan dalam penyusunan dokumen DRP. Selanjutnya DRP akan menjadi panduan yang dipersiapkan Diskominfo Pemprov Kalimantan Selatan dalam menghadapi bencana sehingga proses bisnis/layanan tetap dilanjutkan dan dapat menjaga konsistensi data apabila akibat bencana berdampak pada gangguan maupun kerusakan terhadap layanan teknologi informasi.
13. Perlu melakukan identifikasi dan evaluasi kebijakan maupun prosedur keamanan informasi yang akan menjadi panduan/kontrol operasional TIK di Pemprov Kalimantan Selatan.
14. Perlunya memperhatikan sistem pengamanan yang tidak terbatas pada akses fisik namun juga akses virtual, memperhatikan penggunaan enkripsi dengan level jaringan untuk pengamanan data, penerapan *salt function* yang dapat memperkuat keamanan data, melakukan *patching* dan pembaharuan sistem terbaru untuk melindungi dari kerentanan yang ada.
15. Perlu dibuat *Insident 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.
16. 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 Kalimantan Selatan.
17. Melakukan penerapan *User Acceptance Test* (UAT) dalam proses SDLC untuk memastikan berjalannya fitur dan aplikasi serta menemukan bugs serta permasalahan lain sebelum dilakukan *production*.
18. Melakukan penerapan lingkungan pengembangan dan uji coba yang telah diamankan dengan standar platform teknologi yang ada dan dilakukan secara terpisah dengan tahap *production* yang bertujuan agar sistem yang dalam kategori *production* tidak terganggu pada saat terjadi proses pengembangan.
19. 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, merumuskan 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 Kalimantan Selatan TA2022 ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan informasi Pemerintah Daerah Provinsi Kalimantan Selatan.

Laporan *Onsite Assessment* Indeks KAMI Pemerintah Daerah Provinsi Kalimantan Selatan TA2022 ini disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara
2. Gubernur Pemerintah Daerah Provinsi Kalimantan Selatan
3. Sekretaris Daerah Pemerintah Daerah Provinsi Kalimantan Selatan

Banjarmasin, 28 Juli 2022

Kepala Bidang Persandian dan
Keamanan Informasi,
Diskominfo Kalimantan Selatan

Fungsional Sandiman Madya selaku
Lead Assessor Indeks KAMI:



M. Noor Ikhwanadi, SH., MM.
NIP. 19740721 200903 1 004

Firman Maulana, S.E.
NIP. 19740503 199312 1 001

Mengetahui,
Kepala Dinas Komunikasi dan Informatika
Provinsi Kalimantan Selatan,

Dr. H. Muhamad Muslim. S.Pd, M.Kes
NIP. 196803111989031003