

	<b>LAPORAN ONSITE ASSESSMENT INDEKS KAMI</b>	 INDEKS KEAMANAN INFORMASI
<b>Instansi/Perusahaan:</b>  PEMERINTAH DAERAH PROVINSI KALIMANTAN TIMUR	<b>Pimpinan Unit Kerja :</b>  H. Muhammad Faisal, S.Sos., M.Si. NIP. 19680805 199402 1 001	
<b>Unit Kerja:</b>  DINAS KOMUNIKASI DAN INFORMATIKA (DISKOMINFO)	<b>Narasumber Instansi/Perusahaan :</b>  1. Drs Dianto, M.Si. NIP. 19660413 199703 1 004 2. Dra. Hj. Normalina, M.Si. NIP. 19651223 198603 2 009 3. Agus Eko Santoso, S.Sos, MM NIP. 19820831 200604 1 006 4. Bambang Kukiloargo Suryo, S.Kom., MMSI NIP. 19760123 200502 1 003 5. Fahmy Asa, S.IP, M.Eng NIP. 19780609 200803 1 002 6. Eva Yusefa, ST, MM NIP. 19830929 200903 2 003 7. Edo Santradijaya, ST NIP. 19840719 200803 1 002 8. Fery, S.Kom., M.Si NIP. 19810227 201001 1 017 9. Riko Aji Prabowo, S.Sn NIP. 19791111 201101 1 001	
<b>Alamat:</b>  Jl. Basuki Rahmat No.41, Sungai Pinang Luar, Kec. Samarinda Kota, Kota Samarinda, Kalimantan Timur 75121		
<b>Email:</b>  diskominfo@kaltimprov.go.id	<b>Asesor :</b>  1. Firman Maulana, S.E. NIP. 19740503 199312 1 001 2. Jehan Bilhaq, S.ST., M.AP NIP. 19871227 200801 1 002 3. Diah Sulistyowati, S.Kom., M.T. NIP. 19820925 200212 2 001 4. Aris Munandar, S.S.T. MP. NIP. 19900917 200912 1 001	
<b>Tel/ Fax :</b>  (0541) 731963		

**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 Timur.

**2. Fungsi Kerja:**

Sebagaimana Peraturan Gubernur Kalimantan Timur Nomor 41 Tahun 2020 tentang Susunan Organisasi, Tugas, Fungsi, dan Tatakerja Dinas Komunikasi dan Informatika, Provinsi Kalimantan Timur 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 :

- perumusan kebijakan teknis bidang Komunikasi dan Informatika, bidang Persandian dan bidang Statistik sesuai dengan rencana strategis yang ditetapkan pemerintah daerah;
- perencanaan, pembinaan dan pengendalian kebijakan teknis bidang Komunikasi dan Informatika, bidang Persandian dan bidang Statistik;
- pelaksanaan kebijakan teknis bidang Informasi Komunikasi Publik dan Kehumasan;
- pelaksanaan kebijakan teknis bidang Teknologi Informasi Komunikasi dan Persandian;
- pelaksanaan kebijakan teknis bidang Aplikasi Informatika;
- pelaksanaan kebijakan teknis bidang Statistik;
- pelaksanaan evaluasi dan pelaporan bidang Informasi Komunikasi Publik dan Kehumasan, Teknologi Informasi Komunikasi dan Persandian, Aplikasi Informatika dan Statistik;
- pelaksanaan administrasi Dinas Kominfo sesuai dengan lingkup tugasnya; 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 Kalimantan Timur	Jl. Basuki Rahmat No.41, Sungai Pinang Luar, Kec. Samarinda Kota, Kota Samarinda, Kalimantan Timur 75121

**B. Nama /Jenis Layanan Publik:**

Layanan Infrastruktur Data Center/ Ruang Server dan aplikasi sistem informasi (<https://webmail.kaltimprov.go.id/>) yang dikelola oleh Dinas Komunikasi, Informatika, Statistik, dan Persandian Provinsi Kalimantan Timur.

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

Memiliki 131 aplikasi yang dikelola oleh Diskominfo Pemprov Kalimantan Timur baik yang hosting di dalam maupun di luar Diskominfo.

**2. Server :**

- Server kaltimprov.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	Ya		Draft
2	Organisasi, Peran dan Tanggungjawab Keamanan Informasi	Ya		R
3	Panduan Klasifikasi Informasi	Ya		Draft
4	Kebijakan Manajemen Risiko TIK	Ya		Draft
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		
2	Pengendalian Rekaman/ Catatan	Ya	-	Draft
3	Audit Internal SMKI		Tdk	-
4	Tindakan Perbaikan & Pencegahan		Tdk	-
5	Pelabelan, Pengamanan, Pertukaran & Disposal Informasi	Ya	-	Draft
6	Pengelolaan <i>Removable Media</i> & Disposal Media		Tdk	-
7	Pemantauan ( <i>Monitoring</i> ) Penggunaan Fasilitas TIK		Tdk	-
8	User Access Management	Ya	-	Draft
9	Teleworking		Tdk	-
10	Pengendalian instalasi software & HAKI	Ya	-	Draft
11	Pengelolaan Perubahan ( <i>Change Management</i> ) TIK		Tdk	-
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi	Ya	-	Draft

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

**Dokumen yang diperiksa:**

1. Peraturan Gubernur Provinsi Kalimantan Timur nomor 2 tahun 2019 tentang RPJMD 2019-2023
2. Peraturan Gubernur Provinsi Kalimantan Timur nomor 41 tahun 2020 tentang Susunan Organisasi, Tugas, Fungsi, dan Tatakerja Dinas Komunikasi dan Informatika, Provinsi Kalimantan Timur;
3. Rancangan Perubahan Rencana Strategis Diskominfo Provinsi Kalimantan Timur Tahun 2019-2023;
4. Surat Keputusan Tim CSIRT Kalimantan Timur;
5. Rancangan Pergub Penyelenggaraan SPBE di lingkungan Daerah;
6. Draft Penyelenggaraan Persandian untuk Pengamanan Informasi di lingkungan Provinsi Kalimantan Timur;
7. Draft penyelenggaraan dan pemanfaatan sistem elektronik di pemerintah provinsi Kalimantan Timur;
8. Laporan Pendahuluan dan Akhir hasil Asesmen Keamanan Informasi dalam rangka Penyusunan Dokumen dan kelengkapan SMKI;

9. Kumpulan Daftar SOP SMKI dan Operasional Diskominfo;
10. Indikator Kinerja Individu Kepala Diskominfo tahun 2021 dan 2022;
11. Dokumen Pelaksanaan Anggaran Tahun 2018, 2019 dan 2020;
12. Dokumen Inventaris Barang dari SIMDA tahun 2018 sd. 2019;
13. Laporan Realisasi Anggaran Tahun 2019 dan 2020;
14. Bahan Literasi Keamanan Informasi "Pengenalan Internet Sehat".
15. Laporan Interoperabilitas Sistem Informasi No 10 Tahun 2014;
16. Keputusan Kepala Diskominfo Provinsi Kalimantan Timur No. 489/064/Diskominfo/2019 tentang Pembentukan Tim untuk Perancangan Raperda tentang Penyelenggaraab Pemerintah Berbasis Teknologi Informasi dan Komunikasi.

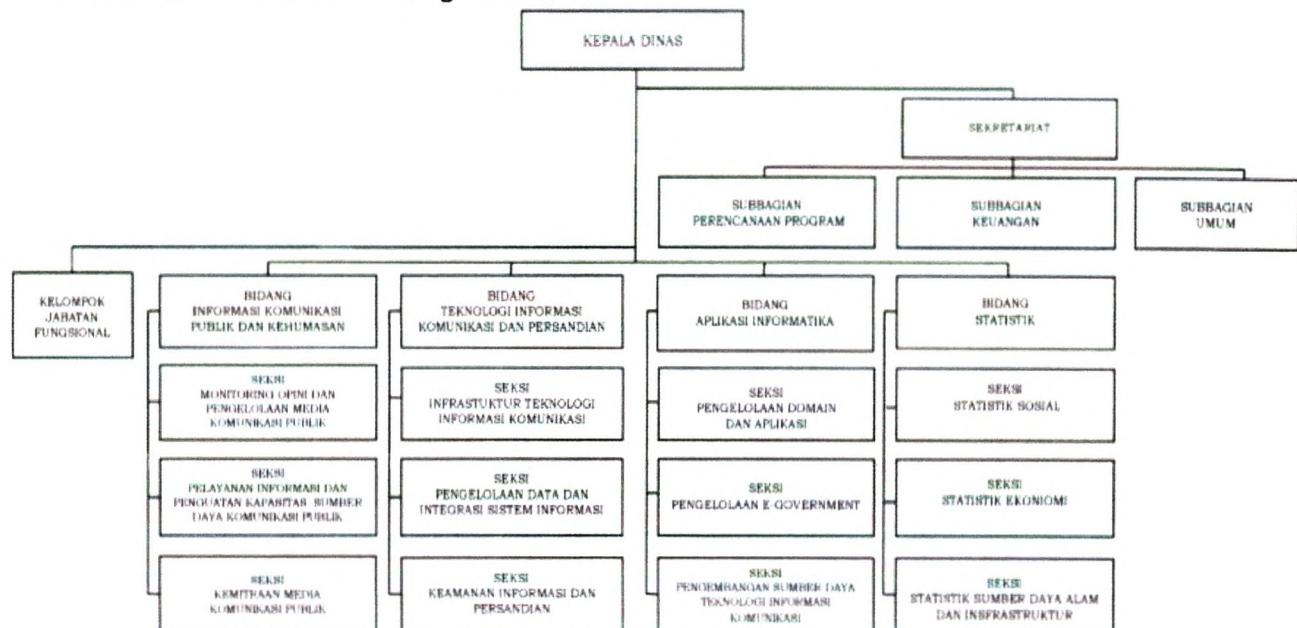
**Bukti-bukti (rekaman/arsip) penerapan SMKI:**

1. Tangkapan layer hasil filtering email dengan mikrotik;
2. Topologi interkoneksi jaringan dan integrasi Server Diskominfo;
3. Hasil tangkapan Web Application Firewall;
4. Sistem monitoring dengan open source Wazuh;
5. Hasil tangkapan scanning dengan BitNinja console.

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

**I. KONDISI UMUM:**

1. Diskominfo Kalimantan Timur dibentuk berdasarkan Peraturan Gubernur Provinsi Kalimantan Timur Nomor 41 Tahun 2020 tentang Susunan Organisasi, Tugas, Fungsi, dan Tatakerja Dinas Komunikasi dan Informatika, Provinsi Kalimantan Timur, berikut struktur Diskominfo Pemprov Kalimantan Timur adalah sebagai berikut:



Gambar 1. Struktur Organisasi Diskominfo Pemprov Kalimantan Timur

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

No	Status Kepegawaian	Jumlah	Prosentase
1	PNS	51	49%
2	CPNS	0	0%
3	Tenaga Ahli Daya	62	51%
<b>Jumlah</b>		<b>113</b>	<b>100%</b>

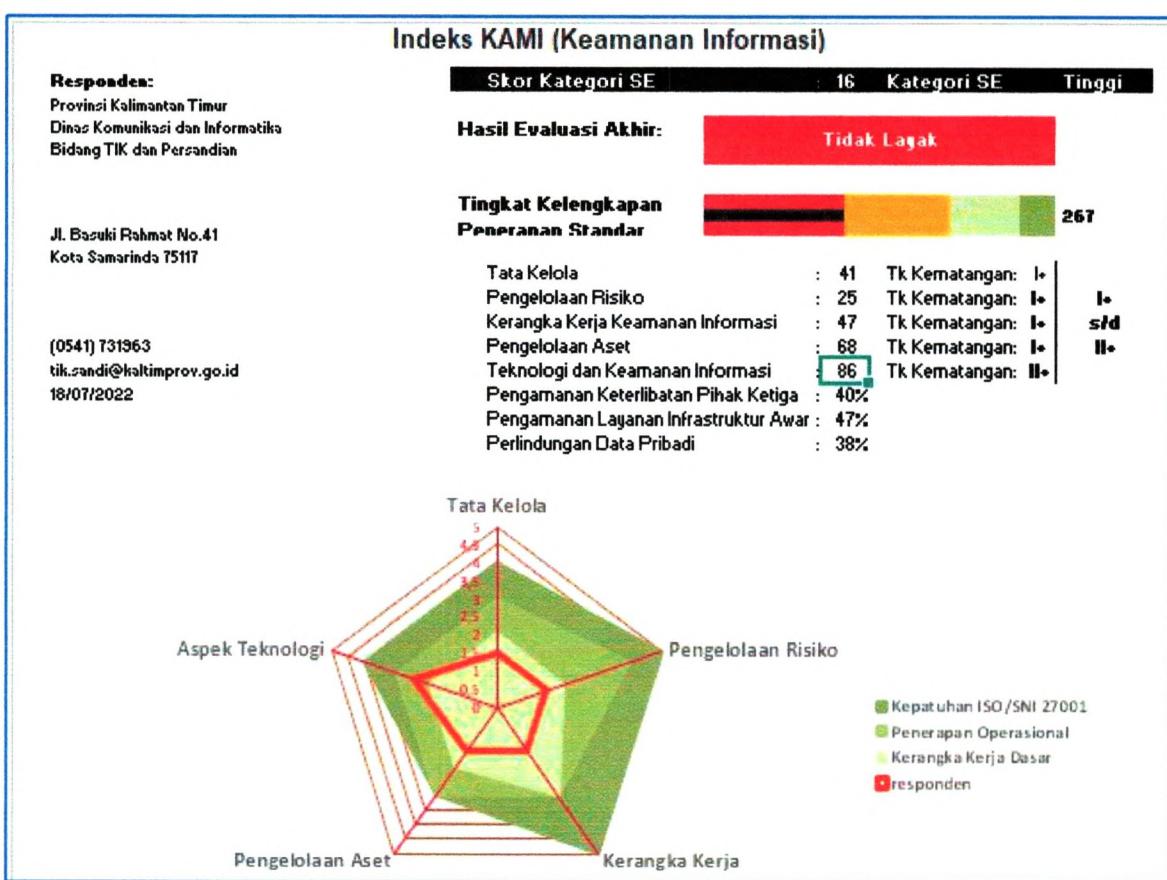
3. Berdasarkan verifikasi terhadap hasil *Self Assessment* isian file Indeks KAMI diperoleh hasil sebagai berikut:

Penilaian Mandiri Indeks KAMI dilakukan di tahun 2022 ini dengan ruang lingkup Diskominfo Pemerintah Provinsi Kalimantan Timur, 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 **250**.

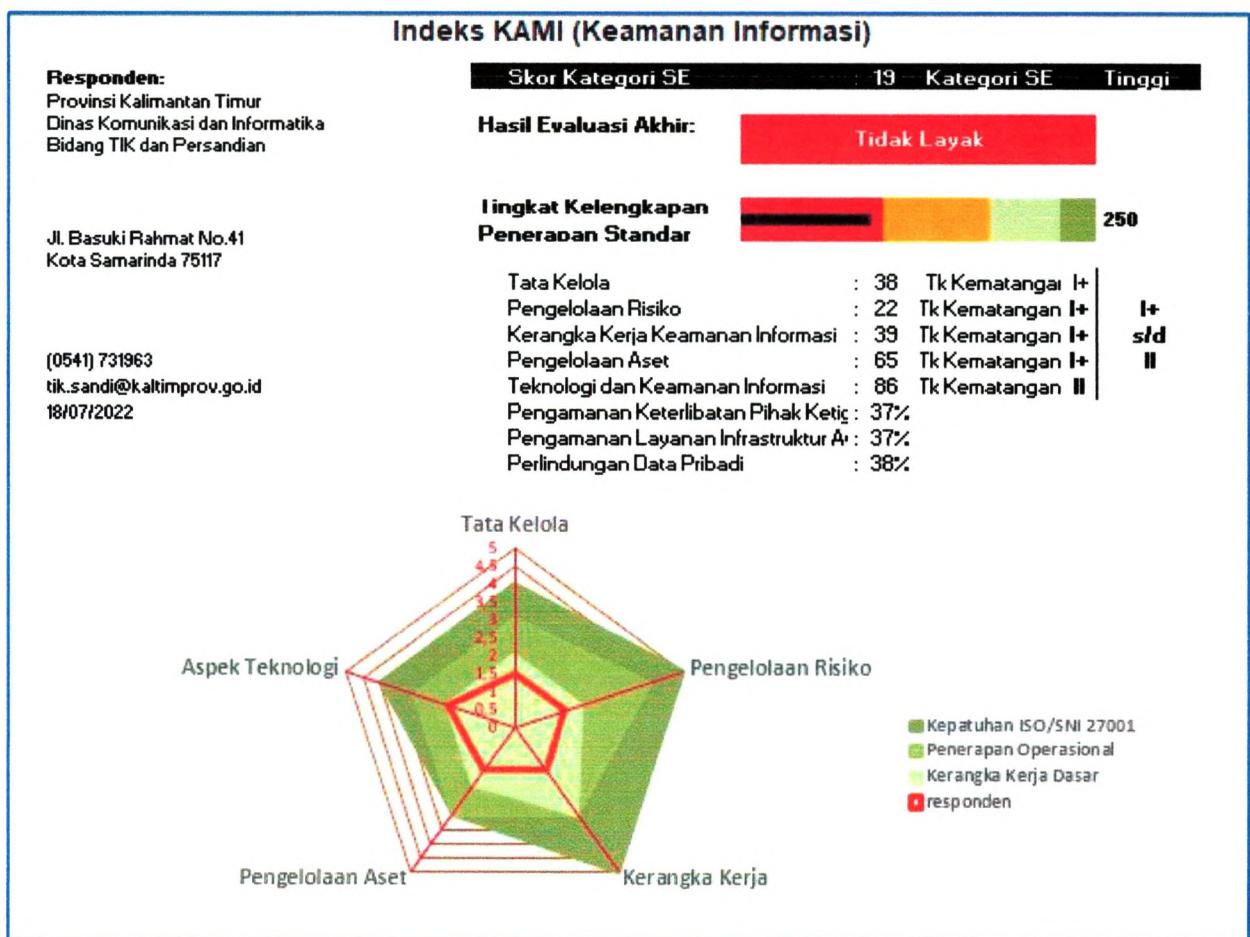
Pada tahun 2022 ini merupakan periode kali pertama bagi lingkup Diskominfo Pemerintah Provinsi Kalimantan Timur dilakukan verifikasi oleh Tim BSSN dalam penilaian mandiri Indeks KAMI, sehingga sesuai mekanisme kebijakan yang ada untuk pelaksanaan kegiatan verifikasi adalah dengan melakukan pengecekan 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 Timur 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 Kalimantan Timur secara lebih optimal.

#### Total Score Sebelum Verifikasi: 267 (ref. file Indeks KAMI v4.2 pra Verifikasi)



**Total Score Setelah Verifikasi: 250 (ref. file Indeks KAMI v4.2 pasca Verifikasi)**



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

### A. Kekuatan/Kematangan

1. Dinas Komunikasi dan Informatika (Diskominfo) Kalimantan Timur telah memiliki dokumen Perencanaan strategis mulai dari RPJMD, Renstra dan DPA yang menjadi dasar dalam pelaksanaan program keamanan informasi.
2. Pelaksanaan tugas dan fungsi keamanan informasi saat ini tercantum dalam Pergub 41 Tahun 2020 tentang SOTK Pemprov Kalimantan Timur.
3. 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 namun belum menjadi strategi dalam perbaikan sasaran keamanan informasi.

### B. Kelemahan/Kekurangan

1. Belum memiliki panduan secara utuh dan komprehensif yang digunakan dalam penerapan keamanan informasi berikut penjabaran tugas dan tanggung jawab dalam pengelolaan keamanan informasi yang dilakukan secara menyeluruh terhadap keseluruhan aspek keamanan informasi mulai dari proses perencanaan, pemantauan pelaksanaannya secara berkelanjutan dan proses dalam menjamin kepatuhan keamanan informasi di lingkup Pemprov Kalimantan Timur.
2. Peran fungsi pelaksana pengamanan informasi belum dipetakan dalam peta jabatan secara lengkap terkait pengelolaan program keamanan informasi secara lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan.
3. Diskominfo Kalimantan Timur 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 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).
  5. Telah melakukan identifikasi data pribadi dalam proses kerja dan menerapkan metode keamanannya melalui pembatasan akses namun belum adanya penyesuaian standar keamanan terhadap ketentuan peraturan/kebijakan perundungan yang telah ditetapkan.
  6. 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.
  7. 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).
  8. 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.
  9. 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.
  10. 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.
  11. Diskominfo Kalimantan Timur belum menetapkan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

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

#### a. Kekuatan/Kematangan

1. Telah memiliki dokumen hasil evaluasi penilaian kondisi penerapan keamanan infomasi yang dituangkan sebagai kerangka kerja dokumen pengelolaan risiko keamanan informasi Pemprov Kalimantan Timur yang digunakan sebagai salah satu dasar dalam melakukan pemetaan kebutuhan pembenahan tata kelola SMKI dan sebagai upaya dalam menangani risiko yang mengganggu tercapainya visi, misi dan sasaran strategis Pemprov Kalimantan Timur.
2. Merujuk pada dokumen tersebut, telah tercantum tingkat ancaman, kemungkinan dan dampak yang digunakan sebagai dasar dalam proses penilaian risiko dengan mengacu pada framework Risk IT dan COBIT Dari ISACA. Berdasarkan proses tersebut telah dilakukan Analisa/kajian risiko dan penetapan langkah mitigasi sebagai antisipasi adanya gangguan/insiden yang merugikan reputasi maupun sumber daya yang dimiliki Pemprov Kalimantan Timur.

#### b. Kelemahan/Kekurangan

1. Diskominfo Kalimantan Timur belum memiliki program kerja berupa kebijakan/pedoman/panduan pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan dan dilakukan monitoringnya secara periodik sesuai dengan kebutuhan waktu penyelesaian tingkat penanganan risiko yang telah ditetapkan..
2. Belum menetapkan penanggung jawab manajemen risiko dan penentuan ambang batas tingkat risiko yang dapat diterima oleh Pemprov Kalimantan Timur.

3. Telah menetapkan dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi asset yang tercantum dalam kajian analisis oleh pihak ketiga yang dimiliki Diskominfo Kalimantan Timur namun belum dilakukan secara menyeluruh terhadap keseluruhan asset yang dimiliki .
4. Telah memiliki identifikasi ancaman dan kelemahan yang terkait dengan asset informasi, terutama asset utama namun belum menetapkan dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi asset utama termasuk belum menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap asset informasi utama yang telah dimiliki termasuk asset utama organisasi.
5. Telah menyusun rencana langkah mitigasi risiko namun penanggulangan risiko belum dilakukan sampai dengan level kriteria penerimaan risiko/ *Risk Acceptance Criteria* (RAC).
6. Belum menerapkan langkah prioritas dan target serta penanggung jawab penyelesaian risiko serta metode memastikan efektivitasnya terhadap kebijakan manajemen risiko yang dimiliki.
7. 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 perlu dilakukan penyempurnaan dan *review* secara berkala.
8. Pengelolaan risiko belum menjadi bagian dari tugas dalam pengelolaan keamanan informasi sehingga perlu ditetapkan dan tidak terpisah dalam suatu kesatuan Sistem Manajemen Keamanan Informasi.
9. Diskominfo Kalimantan Timur belum mendefinisikan kepemilikan dan pihak pengelola (kustodian) asset informasi, inventaris asset 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 dasar dalam melindungi keamanan informasi
10. Belum adanya penetapan profil risiko yang dilakukan pengujinya secara berkala dalam rangka melakukan penyesuaian terhadap penerapan bentuk pengamanan yang baru.
11. Belum menjadikan pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan.

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

##### a. Kekuatan/Kematangan

1. 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
2. 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.
3. 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.
4. Telah memiliki strategi penerapan keamanan informasi yang dituangkan dalam keselarasan perencanaan program mulai dari dokumen Renstra, penyusunan DPA dan program keamanan informasi yang mendukung tugas dan fungsi Diskominfo Pemprov Kalimantan Timur.
5. Telah memiliki inisiasi pelaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan asset informasi, kebijakan dan prosedur keamanan yang ada dengan hasil penetapan kontrol perbaikan yang akan dilakukan dalam periode waktu yang telah ditetapkan dan tertuang dalam rencana kerja program organisasi.
6. Telah mempunyai rencana dan program peningkatan keamanan informasi untuk jangka pendek maupun menengah yang telah diupayakan pencapaian realisasinya sesuai dengan durasi pencapaian target yang telah ditetapkan pada dokumen Renstra dan DPA.

##### 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 mekanisme dalam pengelolaan dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
3. Belum memiliki proses identifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi dalam suatu prosedur/SOP Penanganan Insiden.
4. Pemprov Kalimantan Timur belum memiliki kebijakan dan prosedur keamanan informasi yang dibutuhkan berdasarkan 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.
5. 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.
6. Konsekuensi dari pelanggaran kebijakan keamanan informasi masih belum didefinisikan, dikomunikasikan dan ditegakkan, baik di internal maupun eksternal Pemprov Kalimantan Timur.
7. Belum memiliki prosedur resmi dalam mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi yang dihadapi.
8. Belum melakukan evaluasi tingkat kepatuhan terhadap pelaksanaan audit internal yang dilakukan secara konsisten dan berkelanjutan.
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 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.
11. Belum memiliki kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning/BCP*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya.
12. 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 pemberian yang diperlukan.
13. Belum melakukan evaluasi kelayakan secara berkala terhadap seluruh kebijakan dan prosedur keamanan informasi yang dimiliki.
14. 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.
15. Belum melakukan pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada secara periodik.

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

##### a. Kekuatan/Kematangan

1. Diskominfo Kalimantan Timur telah memiliki daftar inventaris aset sumber daya secara lengkap, akurat dan terpelihara yang telah dituangkan dalam daftar inventaris SIMDA maupun daftar identifikasi data dan informasi berupa aplikasi Perangkat daerah dan website.
2. Telah melakukan proses penyidikan/investigasi dan pelaporan insiden sampai dengan tahap penyelesaiannya dengan melalui mekanisme pelaporan SiGeLATIK (Sistem Informasi Gangguan Layanan TIK) melalui penggunaan media web dan *mobile application*.

3. Telah memiliki prosedur permohonan email dan manajemen serta akses jaringan yang telah ditetapkan.
4. Telah memiliki pengaturan kebijakan pengamanan lokasi kerja penting (ruang server) berupa mekanisme pemenuhan dan penyelenggaraan serta memiliki kebijakan pengendalian hak akses termasuk ketentuan keamanan *data center* (perimeter fisik, akses masuk dua lapis pengamanan secara digital) dan pengaturan operasional perangkat keras dan perangkat lunak dengan menggunakan *sangford acloud*.
5. Telah memiliki prosedur *back-up* dan *restore* terhadap server secara berkala melalui prosedur yang telah ditetapkan dan dikomunikasikan pada seluruh perangkat daerah.
6. Telah memiliki prosedur integrasi dan pertukaran data sistem informasi yang diimplementasikan pada lingkup Pemprov Kalimantan Timur.
7. Telah memiliki mekanisme pengecekan kondisi suhu dan kelembapan ruang server dengan penerapan PAC untuk menjaga kestabilan temperature pada operasional data center yang membutuhkan pendinginan secara terus menerus.
8. 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. Diskominfo Kalimantan Timur belum memiliki definisi klasifikasi informasi merujuk dan belum melakukan proses evaluasi aset serta proses evaluasi dan klasifikasi tingkat kepentingan pengamanannanya, serta proses perekamannya saat ini masih berupa konsep prosedur kebijakan yang akan ditetapkan.
2. Prosedur kebijakan pengendalian hak akses yang mengatur *user* yang mutasi/keluar baik pegawai tetap maupun tenaga kontrak belum ditetapkan.
3. Belum memiliki kebijakan tingkatan akses yang berbeda dari setiap klasifikasi aset informasi, berikut *user access metrik* yang dapat merekam alokasi akses tersebut.
4. 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.
5. Belum memiliki proses merilis aset baru yang merujuk pada kebijakan tentang pengelolaan dan pemutakhiran inventaris aset.
6. Belum memiliki kebijakan dan SOP terkait penggunaan computer, internet dan intranet, yang digunakan sebagai panduan pelaksanaan keamanan informasi bagi pegawai.
7. 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*.
8. Belum memiliki mekanisme penggunaan data pribadi sebagai dasar pengaturan penggunaan data pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggungjawab.
9. Belum memiliki kebijakan proses otentifikasi dan sanksi pelanggaran.
10. 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).
11. Belum memiliki tata cara pemusnahan barang TIK namun yang merujuk pada klasifikasi aset yang dimiliki organisasi.
12. Belum tersedia prosedur rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
13. Kebijakan pengendalian pihak ketiga telah tercantum pengaturan pemenuhan standar keamanan dan penerapan manajemen insiden namun masih berupa konsep prosedur yang belum ditetapkan.
14. 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. Diskominfo Kalimantan Timur 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 mikrotik.
3. Telah dilakukan perlindungan terhadap seluruh perangkat desktop dan server. Untuk linux dengan antivirus default dan perangkat OS windows dengan menggunakan windows defender.
4. Monitoring telah menggunakan open source Wazuh sebagai analisis data log dan untuk mendeteksi adanya malware.
5. Telah dilakukan penerapan pemberlakuan pembatasan waktu akses otomatisasi dengan durasi *destroy session time out*.
6. Telah menggunakan mekanisme sinkronisasi waktu secara akurat dengan *Network Time Protocol*.
7. Telah menerapkan pengelolaan sistem dengan bentuk pengamanan filtering email yang terintegrasi dengan Zimbra.
8. Telah melibatkan pihak independen (BSSN maupun pihak ketiga/sektor privat) untuk mengkaji keandalan keamanan informasi baik pada sistem manajemen keamanan informasi maupun aplikasi yang dimiliki namun belum dilakukan secara rutin dan terjadwal.

b. Kelemahan/Kekurangan

1. Belum memiliki standar konfigurasi sistem, jaringan dan aplikasi serta proses analisa kepatuhan penerapan konfigurasi sesuai standar yang ada.
2. Belum dibuat kebijakan penggunaan kompleksitas *password* (ketentuan panjang password masih belum sesuai standar yaitu minimal masih 6 karakter)
3. Belum memiliki konsep penyediaan redundant terhadap keseluruhan infrastruktur jaringan, sistem dan aplikasi yang dimiliki, masih sebatas *back up database* dan aplikasi.
4. Belum adanya implementasi penggunaan enkripsi sesuai kebijakan yang telah ditetapkan termasuk penerapan pengamanan pengelolaan kunci enkripsi yang digunakan.
5. Belum adanya mekanisme proses analisa secara rutin terhadap jejak audit *antivirus/antimalware*.
6. 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.
7. Belum menerapkan lingkungan pengembangan dan uji coba sesuai kriteria keamanan yang diberlakukan pada seluruh siklus hidup sistem yang telah dibangun secara menyeluruh.

**VII. ASPEK SUPLEMEN:**

A. Kekuatan/Kematangan

1. Kebijakan dengan pihak ketiga saat ini tercantum dalam rancangan kebijakan prosedur yang merupakan bagian dari kontrol penerapan keamanan informasi.
2. Telah melakukan proses pemantauan secara rutin (tiap bulan) terhadap pelaksanaan kinerja pihak ketiga untuk layanan yang diberikan maupun adanya gangguan terhadap operasional layanan dan terlaporkan kepada pimpinan.
3. Telah menerapkan proses penghentian penggunaan cloud sebagai antisipasi pengamanan data dengan melakukan *back up*.

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 maka perlu ditetapkan kebijakan tata kelola keamanan informasi yang terintegrasi dengan konsep keamanan lainnya baik penyelenggaran persandian untuk pengamanan informasi maupun SPBE dimana berdasarkan dokumen tersebut selanjutnya menjadi dasar penetapan pendelegasian tugas, wewenang dan tanggung jawab dalam pelaksanaan penerapan SMKI pada lingkup Diskominfo Pemerintah Provinsi Kalimantan Timur mulai dari perencanaan sampai dengan evaluasi serta pengujian kepatuhannya secara berkelanjutan (audit internal).
2. Perlu mengevaluasi hasil gap analisis kondisi keamanan informasi yang telah disusun untuk dilakukan tinjauan manajemen terhadap regulasi dan kebijakan yang telah dimiliki dan membuat pemetaan terhadap turunan kebijakan prioritas keamanan informasi yang digunakan sebagai prosedur operasional dan dasar melakukan pemantauan dan perbaikan secara berkelanjutan dalam penerapan SMKI di Pemprov Kalimantan Timur.
3. 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.
4. Agar pelaksanaan SMKI berjalan sesuai dengan ketentuan dan standar serta keamanan informasi yang telah ditetapkan, Diskominfo Pemerintah Provinsi Kalimantan Timur 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 dan Peraturan BSSN Nomor 4 Tahun 2021 tentang Manajemen Keamanan Informasi SPBE dan Standar Teknis Prosedur Keamanan SPBE.
  - b. Pola koordinasi secara efektif baik internal maupun eksternal Diskominfo.
  - c. Kebijakan BCP dan DRP dalam menjaga keberlangsungan bisnis proses dan keamanan serta perlindungan aset organisasi secara terencana dan dilakukan monitoringnya secara rutin.
5. 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 (tiga) tahapan dalam proses manajemen risiko, yaitu *risk assessment*, *risk mitigation*, dan *risk evaluation*.dan selanjutnya digunakan sebagai bagian dari proses penerapan manajemen risiko di Pemprov Kalimantan Timur khususnya pada lingkup Diskominfo secara sistematis dan terstruktur.
6. 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 Kalimantan Timur 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 Kalimantan Timur.
  - 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 Timur.
  - 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.

7. 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 sebagai *lead* dan penanggung jawab pelaksanaan keamanan informasi di Pemprov Kalimantan Timur.
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 yang telah ditetapkan.
9. Perlu melakukan pengujian dan monitoring keamanan jaringan, sistem dan aplikasi yang dimiliki dengan menggunakan perangkat (*software/hardware*) dan mengoptimalkan SDM yang telah memiliki kualifikasi.
10. 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 pendekripsi kebakaran dan sensor asap.
11. Perlu penetapan kebijakan maupun prosedur yang telah diidentifikasi sebagai kontrol dalam meningkatkan keamanan informasi yang akan menjadi panduan keamanan pada seluruh aspek dan operasional TIK di Pemprov Kalimantan Timur.
12. 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.
13. 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.
14. Perlu mengoptimalkan fungsi CSIRT dengan melakukan *vulnerability assessment* dan *penetration testing* secara rutin baik dilakukan oleh internal maupun oleh pihak eksternal sebagai upaya untuk mendekripsi kelemahan sistem di Pemprov Kalimantan Timur.
15. 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 Kalimantan Timur TA2022 ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan informasi Pemerintah Daerah Provinsi Kalimantan Timur.

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

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

Samarinda, 21 Juli 2022

Kepala Bidang TIK dan Persandian,  
Diskominfo Provinsi Kalimantan Timur

Drs Dianto, M.Si.  
NIP. 19660413 199703 1 004

Fungsional Sandiman Madya selaku  
Lead Asesor Indeks KAMI

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