
	LAPORAN ONSITE ASSESSMENT INDEKS KAMI	 INDEKS KEAMANAN INFORMASI
Instansi/Perusahaan: Pemerintah Daerah Provinsi Bengkulu	Pimpinan Unit Kerja : Moh. Redhwan Arif, S.Sos.,M.PH. NIP. 19690523 199001 1 001	
Unit Kerja: Dinas Komunikasi Informatika Dan Statistik Provinsi Bengkulu	Narasumber Instansi/Perusahaan : 1. Tanti Nasilva, S.Sos NIP. 19701115 199203 2 004	
Alamat: JL. Basuki Rahmat no. 06 Sawah Lebar Baru, Ratu Agung, Kota Bengkulu. 38222	2. Isweldi, S.Sos NIP. 19750511 200502 1 003 3. Mukhlis S, S.Sos NIP. 19650909 198503 1 003 4. M. Iqbal, S.T., M.E NIP. 19790827 200212 1 002 5. Hijrah Saputra, S.Kom.,M.E. NIP. 19811114 201101 1 003 6. Febriyanda Ardita Putra, S.Kom NIP. 19920214 201902 1 002 7. Ferdi Septianda, S.T NIP. 19920910 202012 1 002 8. Adio Gustiansyah, S.T NIP. 19850803 201902 1 002 9. Hendy Dwiyanasyah, S.Kom. NIP. 19860730 200502 1 001	
Email: diskominfotik@bengkuluprov.go.id	Asesor : 1. Nurchaerani, S.E. NIP. 19650708 198710 2 003	
Tel/ Fax : (0736) 7325176	2. Melita Irmasari, S.ST, M.M. NIP. 19861010 200604 2 007 3. Ni Putu Ayu Lhaksmi W.,S.Tr.TP. NIP. 19960622 201812 2 001 4. Siti Rahmawati, S.Kom. NIP. -	

A. Ruang Lingkup:

1. Instansi / Unit Kerja:

Layanan Data Center/ Ruang Server dan Sistem Informasi yang dikelola oleh Dinas Komunikas, Informatika dan Statistik Provinsi Bengkulu.

2. Fungsi Kerja:

Sebagaimana Peraturan Gubernur Bengkulu Nomor 58 Tahun 2018 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik Provinsi Bengkulu memiliki tugas pokok membantu Gubernur dalam melaksanakan urusan pemerintahan dan tugas pembantuan bidang komunikasi dan informatika, bidang statistik dan bidang persandian yang menjadi kewenangan provinsi.

Dalam menyelenggarakan tugas tersebut, Dinas Kominfo dan Statistik memiliki fungsi sebagai berikut :

- a. perumusan kebijakan di bidang informasi dan komunikasi publik, penyelenggaraan E-Government, hubungan media, layanan informatika, teknologi informasi dan komunikasi, statistik dan persandian persandian yang menjadi kewenangan daerah dan tugas pembantuan kepada daerah provinsi;
- b. pelaksanaan kebijakan di bidang informasi dan komunikasi publik, penyelenggaraan E-Government, hubungan media, layanan informatika, teknologi informasi dan komunikasi, statistik dan persandian persandian yang menjadi kewenangan daerah dan tugas pembantuan kepada daerah provinsi;
- c. pelaksanaan evaluasi dan pelaporan bidang informasi dan komunikasi publik, penyelenggaraan E-Government, hubungan media, layanan informatika, teknologi informasi dan komunikasi, statistik dan persandian persandian yang menjadi kewenangan daerah dan tugas pembantuan kepada daerah provinsi;
- d. pelaksanaan administrasi Dinas; dan
- e. pelaksanaan fungsi lain yang diberikan oleh Gubernur di bidang komunikasi dan informatika, statistik dan persandian.

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor dan Ruang Server Dinas Komunikasi, Informatika dan Statistik Provinsi Bengkulu	JL. Basuki Rahmat no. 06 Sawah Lebar Baru, Ratu Agung, Kota Bengkulu

B. Nama /Jenis Layanan Publik:

Layanan infrastruktur data center/ruang server dan aplikasi sistem informasi yang dikelola oleh Dinas Kominfo dan Statistik Provinsi Bengkulu.

C. Aset TI yang kritical:

1. Informasi:

- Data Pribadi pegawai (identitas pribadi dan keluarga pegawai)
- Data Status pegawai
- Riwayat pegawai

2. Aplikasi:

- E-Kinerja
- E-Cuti
- E-Statistik
- Website

3. Server :
 - Server bengkuluprov.go.id
4. Infrastruktur Jaringan/Network:
 - Telkom dan 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)
	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		Tdk	-
	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 & Disposasi Informasi		Tdk	-
6	Pengelolaan <i>Removable</i> Media & Disposasi Media		Tdk	-
7	Pemantauan (<i>Monitoring</i>) Penggunaan Fasilitas TIK		Tdk	-

8	User Access Management		Tdk	-
9	Teleworking		Tdk	-
10	Pengendalian instalasi software & HAKI		Tdk	-
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 Bengkulu Nomor 58 Tahun 2018 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik, Provinsi Bengkulu;
2. Peraturan Gubernur Bengkulu Nomor 35 Tahun 2016 Tentang Penerapan Electronic Government Pada Pemerintah Provinsi Bengkulu;
3. Peraturan Gubernur Bengkulu Nomor 15 Tahun 2018 Tentang Pengelolaan Webiste Di Lingkungan Pemerintah Provinsi Bengkulu;
4. Peraturan Gubernur Bengkulu Nomor 17 Tahun 2018 Tentang Master Plan E-Government Di Lingkungan Pemerintah Provinsi Bengkulu;
5. Keputusan Kepala Dinas Komunikasi Informatika dan Statistik Provinsi Bengkulu Nomor 31 Tahun 2018 Tentang Penunjukan Tenaga Pengelola Teknis Pada Dinas Komunikasi Informatika dan Statistik Provinsi Bengkulu;
6. Rencana Strategis Dinas Kominfo dan Statistik Provinsi Bengkulu 2016-2021;
7. Nota Kesepahaman Antara Pemerintah Provinsi Bengkulu dengan PT. Telekomunikasi Indonesia, Tbk Tentang Implementasi Smart Province Provinsi Bengkulu;
8. Daftar inventaris barang;
9. Dokumen Analisis Risiko SPBE;
10. Peraturan Gubernur Bengkulu Nomor 36 Tahun 2020 tentang Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Provinsi Bengkulu.

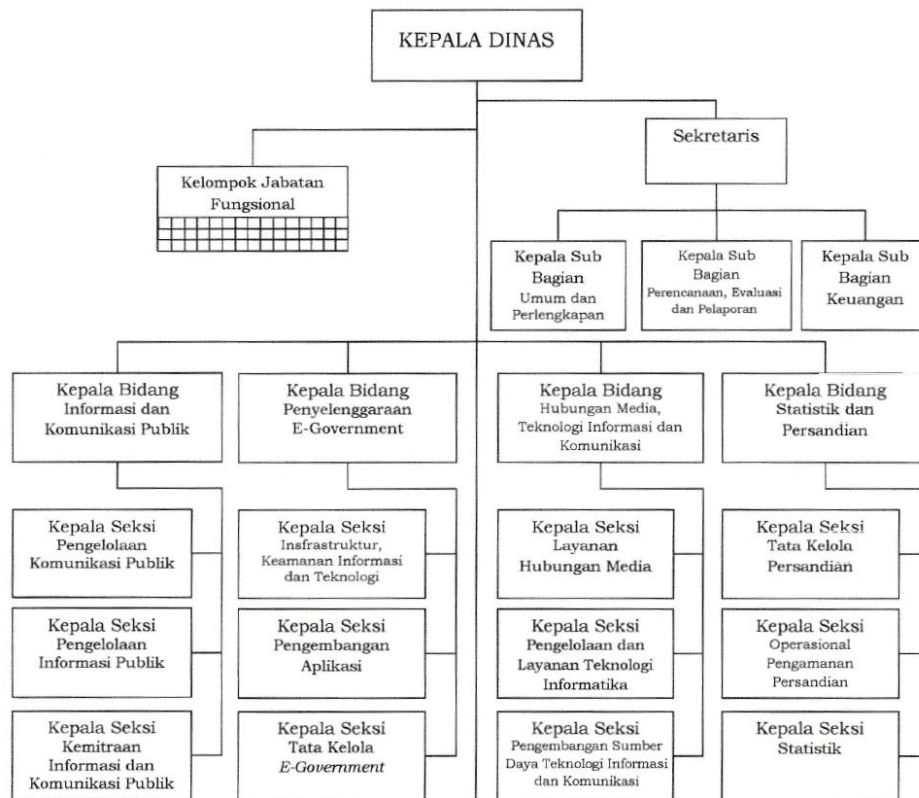
Bukti-bukti (rekaman/arsip) penerapan SMKI:

1. Simulasi aplikasi e-kinerja;
2. Source code aplikasi e-kinerja;
3. Gambar topologi jaringan.

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

I. KONDISI UMUM:

1. Peraturan Gubernur Bengkulu Nomor 58 Tahun 2018 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik Provinsi Bengkulu, berikut struktur Diskominfo Pemprov Bengkulu adalah sebagai berikut:



Gambar 1. Struktur Organisasi Diskominfo Prov Bengkulu

2. SDM pengelola terdiri dari:
 - 1 orang Jabatan Struktural
 - 5 orang Jabatan Fungsional Tertentu (di bidang Keamanan Informasi)
 - 14 orang Fungsional Umum
 - 2 orang Non PNS
3. Berdasarkan verifikasi terhadap hasil *Self Assessment* isian file Indeks KAMI diperoleh hasil sebagai berikut:

Total Score Sebelum Verifikasi: 564 (ref. file Indeks KAMI v4.2pra Verifikasi)

Indeks KAMI (Keamanan Informasi)

Responden:
Pemerintah Provinsi Bengkulu
Dinas Komunikasi, Informatika dan Statistik
Provinsi Bengkulu

Skor Kategori SE : 27 Kategori SE Tinggi

Hasil Evaluasi Akhir:

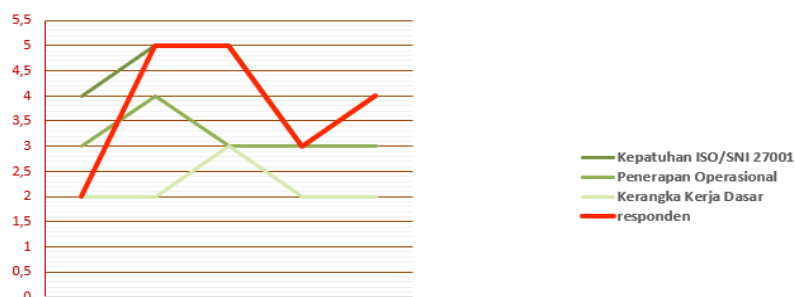
Cukup Baik

Jln. Basuki Rahmat No. 5, Sawah Lebar Baru

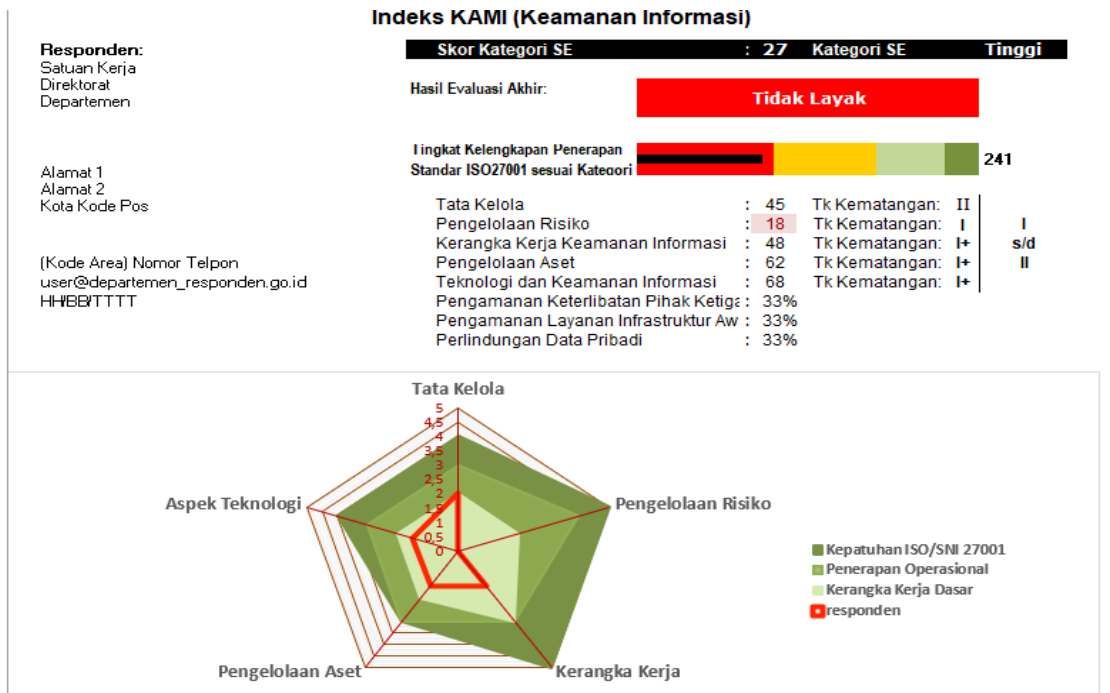
Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai Kategori 564

Tata Kelola	: 45	Tk Kematangan: II	
Pengelolaan Risiko	: 72	Tk Kematangan: V	II
Kerangka Kerja Keamanan Informasi	: 159	Tk Kematangan: V	s/d
Pengelolaan Aset	: 168	Tk Kematangan: III	V
Teknologi dan Keamanan Informasi	: 120	Tk Kematangan: IV	
Pengamanan Keterlibatan Pihak Ketiga	: 96%		
Pengamanan Layanan Infrastruktur Awan	: 100%		
Perlindungan Data Pribadi	: 100%		

0736 7325176
diskominfo@bengkuluprov.go.id
07/07/2022



Total Score Setelah Verifikasi: 241 (ref. file Indeks KAMI v4.2 pasca Verifikasi)



II. ASPEK TATA KELOLA:

A. Kekuatan/Kematangan

1. Dinas Kominfo dan Statistik Provinsi Bengkulu telah memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggung jawab dalam pengelolaan keamanan informasi yang tercantum dalam Peraturan Gubernur Bengkulu Nomor 58 Tahun 2018 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik Provinsi Bengkulu.
2. Pejabat/petugas pelaksana pengamanan informasi memiliki wewenang yang sesuai dalam mengelola dan menjamin kepatuhan program keamanan informasi.
3. Alokasi sumber daya baik anggaran, peralatan dan sumber daya manusia untuk pengelolaan keamanan informasi cukup didukung pimpinan.

B. Kelemahan/Kekurangan

1. Dinas Kominfo dan Statistik Provinsi Bengkulu belum menetapkan kebijakan yang secara resmi dan bertanggung jawab terhadap pelaksanaan program 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. 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.
4. Telah mendefinisikan persyaratan/ standar kompetensi pelaksana pengelola keamanan informasi yang dituangkan dalam anjab, namun masih terlalu umum.
5. Belum semua pelaksana pengamanan informasi yang terlibat, memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku khususnya terkait aspek kontrol teknis dan operasional keamanan informasi.
6. Telah menerapkan program sosialisasi keamanan informasi yaitu sosialisasi persandian dan penggunaan sertifikat elektronik namun belum menerapkan program untuk

- peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi dengan merencanakan secara berkala minimal setiap tahun.
7. Belum melakukan identifikasi data pribadi yang digunakan dalam proses kerja secara menyeluruh dan belum menerapkan pengamanan secara menyeluruh sesuai dengan peraturan perundangan yang berlaku.
 8. 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 menyeluruh.
 9. Tanggung jawab pengelolaan keamanan informasi yang didelegasikan kepada fungsi pengelola keamanan informasi sudah mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, namun belum dilakukan identifikasi persyaratan/kebutuhan pengamanan dalam hal tersebut (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting dan penyelesaian masalah yang ada).
 10. Belum ada konsiderans kebijakan keamanan informasi yang menjadi dasar regulasi dan dituangkan dalam daftar kebijakan yang harus dievaluasi tingkat kepatuhannya.
 11. Belum memiliki dokumen *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP).
 12. Pelaporan kepada pimpinan terkait pengelolaan keamanan informasi dan kepatuhannya belum dilakukan secara menyeluruh.
 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. Belum mendefinisikan kebijakan terkait pelaporan dan penanganan insiden keamanan informasi termasuk yang menyangkut pelanggaran hukum (pidana dan perdata).

III. ASPEK RISIKO:

a. Kekuatan/Kematangan

1. Telah melakukan penilaian risiko SPBE sesuai dengan pedoman pada peraturan Menpan.

b. Kelemahan/Kekurangan

1. Dinas Kominfo dan Statistik Provinsi Bengkulu belum memiliki program kerja berupa kebijakan/pedoman/panduan terkait pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
2. Belum memiliki kerangka kerja pengelolaan risiko, menetapkan penanggung jawab manajemen risiko, ambang batas tingkat risiko yang dapat diterima untuk seluruh aset yang dikelola diskominfo.
3. Secara umum telah melakukan identifikasi ancaman dan kelemahan, dan penetapan dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset namun hanya sebatas pada server dan e-kinerja. Belum menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi utama yang telah dimiliki.
4. Belum menyusun langkah mitigasi risiko dan 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.

IV. ASPEK KERANGKA KERJA:**a. Kekuatan/Kematangan**

1. Telah mencantumkan aspek keamanan informasi dalam kontrak dengan pihak ketiga berupa menjaga kerahasiaan dan HAKI merujuk pada dokumen kontrak dengan pihak ketiga, namun belum terdapat klausul keamanan informasi lainnya seperti perlunya menambahkan mekanisme pelaporan insiden, tata tertib penggunaan dan pengamanan aset.
2. Telah menjadikan aspek keamanan informasi menjadi bagian dari manajemen proyek, hal tersebut diketahui dari adanya inisiasi *hardening* yang bekerjasama dengan BSSN untuk menindaklanjuti temuan dari hasil IT *Security Assessment* (ITSA).
3. Telah memiliki strategi penerapan keamanan informasi yang direalisasikan mengacu pelaksanaan IT *Security Assessment* (ITSA).

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 menetapkan 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. 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 aset yang dimiliki.
6. Konsekuensi dari pelanggaran kebijakan keamanan informasi masih belum didefinisikan, dikomunikasikan dan ditegakkan baik di internal maupun eksternal.
7. Belum memiliki prosedur resmi dalam mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi yang dihadapi.
8. Telah menerapkan implementasi *security patch*, namun belum memiliki kebijakan dan prosedur operasional secara resmi untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, hingga memastikan pemasangan dan melaporkannya.
9. Belum memiliki prosedur untuk mengevaluasi risiko terkait rencana pembelian atau implementasi sistem baru serta menjadi upaya dalam menanggulangi permasalahan yang ada.
10. Belum adanya penerapan proses pengembangan sistem yang aman (*Secure SDLC*) dengan menggunakan prinsip atau metode sesuai standar platform teknologi, pelaksanaannya masih secara sporadis dan belum ditetapkan dalam kebijakan/prosedur yang perlu dilakukan secara berkesinambungan dan konsisten.
11. Belum adanya prosedur/mekanisme penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, termasuk proses untuk menanggulangi dan penerapan pengamanan baru (*compensating control*) serta jadwal penyelesaiannya.

12. Belum memiliki kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning/BCP*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya.
13. Belum memiliki perencanaan pemulihan bencana terhadap layanan TIK (*Disaster Recovery Plan/DRP*) yang terdapat komposisi, peran, wewenang dan tanggung jawab tim serta belum dilakukan uji coba dan evaluasi sebagai tahap langkah perbaikan atau pembenahan yang diperlukan.
14. Belum melakukan evaluasi kelayakan secara berkala terhadap seluruh kebijakan dan prosedur keamanan informasi yang dimiliki.
15. Belum memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada serta belum melakukan evaluasi tingkat kepatuhan secara konsisten dan berkelanjutan maupun kaji ulang dan penyampaian kepada pimpinan terkait dengan langkah peningkatan kinerja keamanan informasi.
16. Belum ada proses yang dilakukan untuk merevisi kebijakan dan prosedur yang berlaku, termasuk analisa untuk menilai aspek finansial ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya.
17. Belum melakukan pengujian dan evaluasi tingkat/status kepatuhan program keamanan informasi yang ada secara periodik.

V. ASPEK PENGELOLAAN ASET:

a. Kekuatan/Kematangan

1. Telah memiliki peraturan terkait pengamanan lokasi kerja penting (ruang server) berupa mekanisme pemenuhan dan penyelenggaraannya.
2. Telah memiliki kebijakan pengendalian hak akses termasuk ketentuan keamanan *data center/ruang server* (perimeter fisik, akses masuk, pengamanan CCTV).

b. Kelemahan/Kekurangan

1. Dinas Kominfo dan Statistik telah memiliki daftar inventaris aset *hardware* dan *software*, 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 resmi terkait pengendalian hak akses yang mengatur *user* yang mutasi/keluar baik pegawai tetap maupun tenaga kontrak.
5. Belum memiliki dan menerapkan peraturan terkait pengamanan lokasi kerja penting (ruang server) berupa tata tertib himbauan masuk bagi pengguna/pengunjung layanan data center (ruang server).
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 resmi manajemen perubahan terhadap sistem, proses bisnis dan proses teknologi informasi termasuk pengelolaan, perubahan konfigurasi.
8. Belum memiliki prosedur resmi terkait mekanisme rilis aset baru dan proses pemutakhiran inventaris aset.
9. Belum memiliki kebijakan dan SOP terkait penggunaan komputer, email dan internet, yang digunakan sebagai panduan pelaksanaan keamanan informasi bagi pegawai.
10. 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*.

11. Belum memiliki mekanisme penggunaan data pribadi sebagai dasar pengaturan penggunaan data pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggungjawab.
12. Belum memiliki kebijakan proses otentikasi dan sanksi pelanggaran.
13. Belum memiliki kebijakan terkait dengan pertukaran data dengan pihak eksternal.
14. Belum memiliki tata cara pemusnahan barang TIK namun yang merujuk pada klasifikasi aset yang dimiliki organisasi.
15. Belum memiliki prosedur resmi dalam proses *backup* data/informasi maupun *restore* data.
16. Belum tersedia prosedur rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
17. Telah menerapkan perlindungan terhadap infrastruktur komputasi dari dampak lingkungan maupun gangguan pasokan listrik namun penerapan dan evaluasi belum dilakukan secara berkala dalam menjaga ketersediaan dan kelayakannya.
18. 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 dan mekanisme kirim terima informasi melalui email dinas.
19. 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).
20. Konstruksi ruang penyimpanan perangkat pengolah informasi penting (ruang server) belum memenuhi kaidah yang berlaku.

VI. ASPEK TEKNOLOGI:

a. Kekuatan/Kematangan

1. Telah menerapkan penggunaan SSL, firewall dan router untuk pengamanan sistem dan jaringan serta telah dipastikan konfigurasi pada firewall sudah disesuaikan dengan ketentuan pengamanan.
2. Telah menerapkan antivirus pada server sedangkan pada perangkat end user (dekstop) dipastikan menggunakan antivirus bawaan sistem operasi (windows defender).
3. Telah menggunakan mekanisme sinkronisasi waktu secara akurat dengan *Network Time Protocol*.
4. Telah menerapkan pengamanan berlapis pada sistem yaitu pada aplikasi e-kinerja, menggunakan SSL, captcha serta pengaturan panjang dan kompleksitas karakter password.

b. Kelemahan/Kekurangan

1. Belum memiliki standar resmi konfigurasi sistem, jaringan dan aplikasi serta proses analisa kepatuhan penerapan konfigurasi sesuai standar yang ada.
2. Belum memiliki kebijakan resmi terkait pengendalian/pengelolaan konfigurasi.
3. Belum melakukan monitoring infrastruktur jaringan, sistem dan aplikasi.
4. Belum adanya proses perekaman dalam log untuk setiap perubahan dalam sistem informasi.
5. Belum diberlakukan penerapan penggantian *password* secara otomatis pada sistem/aplikasi.
6. Telah dilakukan kegiatan *vulnerability assessment* namun belum dilakukan secara mandiri dan berkala untuk keseluruhan sistem dan aplikasi yang dikelola diskominfo.
7. Belum memiliki konsep penyediaan redundan terhadap keseluruhan infrastruktur jaringan, sistem dan aplikasi yang dimiliki, masih sebatas *back up database* dan aplikasi.
8. Analisa log belum dilakukan, masih bersifat insidental dan belum ada penjadwalan yang dilakukan secara periodik.
9. Belum memiliki standar dalam penggunaan enkripsi namun telah menerapkan enkripsi walaupun belum pada keseluruhan aset yang dikelola, hanya enkripsi pada database dan penggunaan aplikasi selection.

10. Belum adanya prosedur pengelolaan kunci enkripsi.
11. Belum adanya mekanisme proses analisa secara rutin terhadap jejak audit *antivirus/antimalware*.
12. Belum dilakukan mekanisme laporan adanya penyerangan *virus/malware* yang gagal/sukses ditindaklanjuti dan diselesaikan yang juga didokumentasikan.

VII. ASPEK SUPLEMEN:

A. Kekuatan/Kematangan

-

B. Kelemahan/Kekurangan

1. Belum melakukan manajemen risiko dan pengelolaan keamanan pihak ketiga.
2. Belum memastikan terhadap pengelolaan sub-kontraktor/ alih daya pada pihak ketiga, penanganan aset, pengelolaan insiden dan rencana keberlangsungan layanan pihak ketiga.
3. Belum melakukan pengelolaan layanan dan keamanan pihak ketiga.
4. Belum ada implementasi *cloud service* dan belum memiliki kebijakan pengamanan layanan infrastruktur awan (*cloud service*).
5. Belum menyusun kebijakan terkait pengelolaan perlindungan data pribadi yang dikelola berserta turunan kebijakan perlindungan data pribadi, kajian risiko masih bersifat secara umum dan perlu dilakukan klasifikasi sesuai dengan tingkat kekritisannya data pribadi.

VIII. REKOMENDASI

1. Agar menyusun dokumen kebijakan Sistem Manajemen Keamanan Informasi (SMKI) kemudian disahkan, disosialisasikan dan dipublikan (internal dan eksternal) serta selanjutnya disusun turunan dari kebijakan tersebut dapat berupa SOP/Pedoman/Juknis/Juklah.
2. Memperbaharui Roadmap atau Master Plan E-Government Dinas Kominfo dan Statistik Provinsi Bengkulu.
3. Melakukan identifikasi keseluruhan aset yang dimiliki (aset informasi, perangkat keras, perangkat lunak, regulasi atau kebijakan kebijakan serta sumber daya manusia).
4. Menyusun dokumen Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP) serta melakukan pengujian secara berkala (1 tahun sekali).
5. Perlu menyusun standar kompetensi dan keahlian pengelola keamanan informasi dengan merujuk pada Peta Okupasi Nasional Keamanan Siber (PONKS) yang diterbitkan oleh BSSN.
6. Merencanakan dan mengalokasikan kegiatan sosialisasi terkait keamanan informasi bagi pihak internal maupun stakeholder Dinas Kominfo dan Statistik Provinsi Bengkulu dan mengadakan program peningkatan kompetensi secara berkala bagi pejabat/pelaksana pengelola keamanan informasi.
7. Diharapkan 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 Dinas Kominfo dan Statistik Provinsi Bengkulu 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 Dinas Komunikasi dan Informatika Provinsi Bengkulu.
 - b. Menyusun kebijakan/pedoman terkait kerangka kerja 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 khususnya pada lingkup Dinas Kominfo dan Statistik Provinsi Bengkulu.

- c. 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 Dinas Kominfo dan Statistik Provinsi Bengkulu.
 - d. Perlunya penambahan identifikasi risiko-risiko lainnya dari aset utama/penting berikut kontrol yang ada saat ini, rencana kontrol tambahan dan penetapan status penyelesaian dengan mengacu pada *risk treatment plan*.
8. Menyusun dokumen *risk register* untuk seluruh aset yang dikelola Dinas Kominfo dan Statistik Provinsi Bengkulu.
 9. Perlu adanya penetapan identifikasi Data Pribadi berikut klasifikasi dan metode pengamanan yang diterapkan dengan merujuk pada Perkominfo 20 Tahun 2016 tentang Perlindungan Data Pribadi.
 10. Perlu menyusun dokumen BCP dan DRP.
 11. Menyusun, mengelola dan mengevaluasi Daftar Induk Dokumen (DID) yang terkait keamanan informasi.
 12. Perlu melakukan pengujian dan monitoring keamanan jaringan, sistem dan aplikasi yang dimiliki dengan menggunakan perangkat (*software/hardware*) dan mengoptimalkan SDM yang telah memiliki kualifikasi.
 13. Menerapkan pengaturan perlindungan terhadap perangkat pengolah informasi penting (server) sesuai dengan kaidah dan memastikan kelayakan perangkat pendukung lainnya.
 14. Perlu dibuat turunan kebijakan dari regulasi keamanan informasi berupa standar/prosedur antara lain ;
 - a. Standar terkait konfigurasi aset jaringan, sistem dan aplikasi
 - b. Standar penerapan enkripsi pada aset jaringan, sistem dan aplikasi
 - c. SOP Pelaksanaan *Back up* dan *Restore* data
 - d. SOP Pelaporan dan Penanganan insiden keamanan informasi
 - e. SOP Manajemen Hak Akses
 - f. SOP Manajemen Perubahan
 - g. SOP Teleworking
 - h. SOP Security Patching
 - i. SOP Penghancuran Data/Aset (spesifik Data/Aset TI)
 15. Menerapkan pengaturan perlindungan terhadap perangkat pengolah informasi penting (server) sesuai dengan kaidah dan memastikan kelayakan perangkat pendukung lainnya.
 16. Memastikan secara berkala penerapan *update* sistem operasi dan antivirus pada server dan seluruh dekstop karyawan.

Penutup

Demikian Laporan Penilaian Indeks Keamanan Informasi Pemerintah Daerah Provinsi Bengkulu T.A. 2022 ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam Pelaksanaan Keamanan Informasi Pemerintah Daerah Provinsi Bengkulu. Agar Pemerintah Daerah Provinsi Bengkulu melaksanakan tindak lanjut atas hasil observasi dan rekomendasi yang disampaikan pada Laporan Evaluasi Pelaksanaan Persandian untuk Pengamanan Informasi Pemerintah Daerah Provinsi Bengkulu T.A. 2022 ini dan melaporkan tindak lanjutnya kepada BSSN.

Laporan Penilaian Indeks Keamanan Informasi Pemerintah Daerah Provinsi Bengkulu T.A. 2022 ini disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi Bengkulu;
3. Sekretaris Daerah Provinsi Bengkulu; dan
4. Kepala Dinas Komunikasi, Informatika dan Statistik Provinsi Bengkulu.

Bengkulu, 14 Juli 2022

Sub Koordinator
Tata Kelola Persandian

Sandiman Madya pada Direktorat Keamanan
Siber dan Sandi Pemerintah Daerah

Isweldi, S.Sos
NIP. 19750511 200502 1 003

Nurchaerani, S.E.
NIP. 19650708 198710 2 003

Mengetahui,

Kepala Bidang Statistik dan Persandian
Dinas Komunikasi, Informatika dan Statistik
Provinsi Bengkulu

Tanti Nasilva, S.Sos.
NIP. 19701115 199203 2 004