



LAPORAN ONSITE ASSESSMENT INDEKS KAMI



INDEKS
KEAMANAN
INFORMASI

Instansi/Perusahaan: Pemerintah Kabupaten Belitung	Narasumber Instansi/Perusahaan: 1. Mohammad Iqbal, ST. 2. Laila Asfiyani, SIP, M.Si. 3. Mohd.Isnaini, S.Sos. 4. Ichsan Zainul Hakim, ST 5. Ikhwanudin, S.Si
Unit Kerja: Dinas Komunikasi dan Informatika Pemerintah Kabupaten Belitung	
Alamat: JL. Anwar Dalam Kompleks Marakas, Kel. Lesung Batang, Kec. Tanjungpandan, Kab. Belitung, Prov. Kepulauan Bangka Belitung, 33412	Tel: (0719) 24942
Email: kominfo@belitung.go.id	Pimpinan Unit Kerja: Dinas Komunikasi dan Informatika Kabupaten Belitung

A. Ruang Lingkup:

Pengelolaan Data Center dan Aplikasi Sistem informasi Kabupaten Belitung

1. Instansi / Unit Kerja:

Dinas Komunikasi dan Informatika Kabupaten Belitung.

2. Tugas dan Fungsi Kerja:

Sebagaimana Peraturan Bupati Nomor 51 Tahun 2016 Tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta Tata Kerja Dinas Komunikasi dan Informatika, Kabupaten Belitung mempunyai tugas membantu Bupati melaksanakan urusan pemerintahan di bidang komunikasi dan informatika, urusan pemerintahan bidang persandian dan urusan pemerintahan bidang statistik yang menjadi kewenangan daerah dan tugas pembantuan yang ditugaskan kepada daerah Kabupaten Belitung. Dalam melaksanakan tugas, Dinas Komunikasi dan Informatika menyelenggarakan fungsi:

- perumusan kebijakan di bidang pengelolaan opini dan aspirasi publik di lingkup pemerintah daerah, pengelolaan informasi untuk mendukung kebijakan nasional dan pemerintah daerah, penyediaan konten lintas sektoral dan pengelolaan media komunikasi publik, pelayanan informasi publik, layanan kehumasan, penguatan kapasitas sumber daya komunikasi publik dan penyediaan akses informasi, layanan nama domain dan sub domain, layanan infrastuktur dasar data center, disaster recovery center dan Teknologi Informasi dan Komunikasi Pemerintah Daerah, layanan keamanan informasi e-government, layanan sistem komunikasi intra pemerintah daerah, layanan manajemen data dan informasi e-government, layanan akses internet dan intranet, layanan pengembangan dan pengelolaan aplikasi generik dan spesifik dan suplemen yang terintegrasi, integrasi layanan publik dan kepemerintahan, penyelenggaraan ekosistem Teknologi Informasi dan Komunikasi Smart City, penyelenggaraan *government chief information officer* (GCIO), pengembangan sumber daya Teknologi Informasi dan Komunikasi pemerintah daerah dan masyarakat lingkup daerah, persandian dan statistik;
- pelaksanaan kebijakan di bidang pengelolaan opini dan aspirasi publik di lingkup pemerintah daerah, pengelolaan informasi untuk mendukung kebijakan nasional

- dan pemerintah daerah, penyediaan konten lintas sektoral dan pengelolaan media komunikasi publik, pelayanan informasi publik, layanan kehumasan, penguatan kapasitas sumber daya komunikasi publik dan penyediaan akses informasi, layanan nama domain dan sub domain, layanan infrastuktur dasar data center, disaster recovery center dan Teknologi Informasi dan Komunikasi, layanan keamanan informasi e-government, layanan sistem komunikasi intra pemerintah daerah, layanan manajemen data dan informasi e-government, layanan akses internet dan intranet, layanan pengembangan dan pengelolaan aplikasi generik dan spesifik dan suplemen yang terintegrasi, integrasi layanan publik dan kepemerintahan, penyelenggaraan ekosistem Teknologi Informasi dan Komunikasi Smart City, penyelenggaraan *government chief information officer* (GCIO), pengembangan sumber daya Teknologi Informasi dan Komunikasi pemerintah daerah dan masyarakat lingkup daerah, persandian dan statistik;
- c. pelaksanaan evaluasi dan pelaporan di bidang tugasnya; dan
 - d. pelaksanaan tugas-tugas lain yang diberikan oleh bupati sesuai dengan tugas dan fungsinya.

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor Pusat	Jl. Anwar Dalam Komplek Marakas, Kel Lesung Batang, Kec. Tanjungpandan, Kab Belitung, Prov Kepulauan Bangka Belitung 33412
2	Data Center	Jl. Anwar Dalam Komplek Marakas, Kel Lesung Batang, Kec. Tanjungpandan, Kab Belitung, Prov Kepulauan Bangka Belitung 33412
3	Disaster Recovery Center (DRC)	-

B. Nama /Jenis Layanan Publik:

Layanan Infrastruktur Data Center dan aplikasi sistem informasi yang dikelola oleh Dinas Komunikasi dan Informatika Kabupaten Belitung.

C. Aset TI yang kritikal:

1. Informasi:
 - Identitas ASN dan pegawai kontrak Pemerintah Kabupaten Belitung
 - Identitas Pegawai Desa di Kabupaten Belitung
 - Identitas Masyarakat Kabupaten Belitung
2. Aplikasi Utama
 - e-office ASN: <https://eoffice.belitung.go.id>
 - sistem keuangan desa: <https://siskeudes.belitung.go.id>
 - satu data: <https://data.belitung.go.id>
 - e-absensi : <https://e-kinerja.belitung.go.id>
 - saluran aspirasi dan pengaduan: <https://besadu.belitung.go.id>
 - sistem pelayanan administrasi kependudukan: <https://besilak.belitung.go.id>
 - sistem informasi layanan masyarakat: <https://sipmas.belitung.go.id>
 - webmail Belitung: <https://mail.belitung.go.id>
 - PPDB: <https://ppdb.belitung.go.id>
3. Server Utama

D. DATA CENTER (DC):

- ADA
 TIDAK ADA

Pengelolaan data center/ ruang server terpusat pada Diskominfo Pemkab Belitung dimana dalam pembangunan dan pengembangannya telah mengacu pada dokumen Rencana Induk Pengembangan Teknologi Komunikasi dan Informasi di Lingkungan Pemkab Belitung sesuai keputusan Kepala Dinas Kominfo Nomor: 045.2/077/KPTS/2020. Merujuk cetak biru Data Center dan Disaster Recovery Center serta dengan melihat secara langsung Data Center Pemkab Belitung, maka diperoleh keterangan adalah:

- 1) Pembangunan Data Center dimulai pada tahun 2017 dengan memperhatikan aspek persyaratan teknis diantaranya meliputi pertimbangan lokasi data center, bangunan dan arsitektur, kontrol akses dan keamanan, peringatan kebakaran, deteksi asap dan pemadam kebakaran.
- 2) Desain arsitektur fisik telah memenuhi komponen standar pembangunan data center yaitu:
 - a) penentuan/pemilihan lokasi, telah membuat kajian persyaratan lokasi data center yang menyesuaikan kebutuhan saat ini dan dapat dikembangkan (*expandable*) serta bebas dari interferensi peralatan elektronik yang dapat menimbulkan gangguan elektromagnetis. Ukuran luas bangunan yang digunakan diasumsikan cukup untuk pengembangan data center untuk periode 15 tahun kedepan.
 - b) *raised floor*, telah memperhatikan beberapa faktor seperti ketinggian lantai dan kemampuan lantai menahan beban
 - c) sistem pendinginan seluruh ruang server Data Center sampai dengan seluruh rak server menggunakan AC Split dan AC Inner yang dipasang pada lantai yang berlubang (*perforated tile*) sehingga menjaga aliran udara dingin pada tiap perangkat, dan membentuk lorong udara dingin (*cold aisle*), dan dibelakangnya membentuk lorong udara panas (*hot aisle*).
 - d) sistem listrik, untuk dapat beroperasi dengan waktu down yang minimal, data center telah diupayakan mempunyai sumber listrik yang stabil dengan konsep sumber daya cadangan ketika sumber data listrik utama tidak tersedia yaitu dengan UPS sejumlah 10 buah dan genset.
 - e) Pencahayaan telah memperhatikan faktor minimal pada bidang horizontal dan vertikal di atas lantai di tengah semua lorong antara rak.
 - f) sistem pengamanan terdiri dari pengamanan fisik dan non-fisik. Fitur sistem pengamanan fisik meliputi akses user ke data center. Akses berupa kunci untuk memasuki ruangan (kartu akses atau biometrik). Akses diberikan juga untuk petugas keamanan yang mengawasi keadaan data center (baik di dalam maupun di luar). Pengamanan fisik juga diterapkan pada ruang di data center yang terdiri dimana dari pintu akses (access door) baik yang menggunakan finger scan. Untuk monitoring keamanan yang berlangsung, telah diimplementasikan CCTV sejumlah 4 titik yang dapat dipantau secara realtime dalam kurun waktu 24/7. Untuk pengamanan non fisik dilakukan terhadap bagian software atau sistem yang berjalan pada perangkat tersebut, antara lain dengan memasang perangkat lunak keamanan seperti firewall, ditambahkan pula anti virus Kaspersky guna pengamanan VM yang akan digunakan sebagai virtualisasi data center.
 - g) sistem penanganan kebakaran, telah menyediakan pemasangan alat pemadam api ringan (APAR) sejumlah 3 unit.

E. DISASTER RECOVERY CENTER (DRC):

- ADA → Dikelola Internal Dikelola Vendor
 TIDAK ADA

Diskominfo Pemkab Belitung belum menerapkan konsep backup data center (*Disaster Recovery Center*) secara menyeluruh. Untuk saat ini DRC hanya untuk layanan LPSE yang bekerja sama dengan Kementerian Komunikasi dan Informatika.

Status Ketersediaan Dokumen Kerangka Kerja Sistem Manajemen Keamanan Informasi (SMKI)

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

No	Nama Kebijakan	Cakupan Dokumen	Ada/Tidak
1	Kebijakan Keamanan Informasi	<p>Menyatakan komitmen manajemen/pimpinan instansi/lembaga menyangkut pengamanan informasi yang didokumentasikan dan disahkan secara formal. Kebijakan keamanan informasi dapat mencakup antara lain:</p> <ul style="list-style-type: none"> • Definisi, sasaran dan ruang lingkup keamanan informasi • Persetujuan terhadap kebijakan dan program keamanan informasi • Kerangka kerja penetapan sasaran kontrol dan kontrol • Struktur dan metodologi manajemen risiko • Organisasi dan tanggungjawab keamanan informasi 	Ada
2	Organisasi, peran dan tanggungjawab keamanan informasi	Uraian tentang organisasi yang ditetapkan untuk mengelola dan mengkoordinasikan aspek keamanan informasi dari suatu instansi/lembaga serta uraian peran dan tanggungjawabnya. Organisasi pengelola keamanan informasi tidak harus berbentuk unit kerja terpisah	Ada
3	Panduan Klasifikasi Informasi	Berisi tentang petunjuk cara melakukan klasifikasi informasi yang ada di instansi/lembaga dan disusun dengan memperhatikan nilai penting dan kritikalitas informasi bagi penyelenggaraan pelayanan publik, baik yang dihasilkan secara internal maupun diterima dari pihak eksternal. Klasifikasi informasi dilakukan dengan mengukur dampak gangguan operasional, jumlah kerugian uang, penurunan reputasi dan legal manakala terdapat ancaman menyangkut kerahasiaan (<i>confidentiality</i>), keutuhan (<i>integrity</i>) dan ketersediaan (<i>availability</i>) informasi.	Tidak
4	Kebijakan Manajemen Risiko TIK	Berisi metodologi / ketentuan untuk mengkaji risiko mulai dari identifikasi aset, kelemahan, ancaman dan dampak kehilangan aspek kerahasiaan, keutuhan dan ketersediaan informasi termasuk jenis mitigasi risiko dan tingkat penerimaan risiko yang disetujui oleh pimpinan.	Ada

5	Kerangka Kerja Manajemen Kelangsungan Usaha (Business Continuity Management)	Berisi komitmen menjaga kelangsungan pelayanan publik dan proses penetapan keadaan bencana serta penyediaan infrastruktur TIK pengganti saat infrastruktur utama tidak dapat beroperasi agar pelayanan publik tetap dapat berlangsung bila terjadi keadaan bencana darurat. Dokumen ini juga memuat tim yang bertanggungjawab (ketua dan anggota tim), lokasi kerja cadangan, skenario bencana dan rencana pemulihan ke kondisi normal setelah bencana dapat diatasi/berakhir.	Ada
6	Kebijakan Penggunaan Sumber daya TIK	Berisi aturan penggunaan komputer (desktop/laptop/modem atau email dan internet).	Ada

No	Nama Prosedur/Pedoman	Cakupan Dokumen	Ada/Tidak
1	Pengendalian Dokumen	Berisi proses penyusunan dokumen, wewenang persetujuan penerbitan, identifikasi perubahan, distribusi, penyimpanan, penarikan dan pemusnahan jika tidak digunakan, daftar dan pengendalian dokumen eksternal yang menjadi rujukan	Ada
2	Pengendalian Rekaman	Berisi pengelolaan rekaman yang meliputi: identifikasi rekaman penting, kepemilikan, pengamanan, masa retensi, dan pemusnahan jika tidak digunakan lagi	Ada
3	Audit Internal SMKI	Proses audit internal: rencana, ruang lingkup, pelaksanaan, pelaporan dan tindak lanjut hasil audit serta persyaratan kompetensi auditor	Tidak
4	Tindakan Perbaikan & Pencegahan	Berisi tatacara perbaikan/pencegahan terhadap masalah/gangguan/insiden baik teknis maupun non teknis yang terjadi dalam pengembangan, operasional maupun pemeliharaan TI	Ada
5	Pelabelan, Pengamanan, Pertukaran & Disposal Informasi	Aturan pelabelan, penyimpanan, distribusi, pertukaran, pemusnahan informasi/daya "rahasia" baik softcopy maupun hardcopy, baik milik instansi maupun informasi pelanggan/mitra yang dipercayakan kepada Instansi	Tidak
6	Pengelolaan Removable Media & Disposal Media	Aturan penggunaan, penyimpanan, pemindahan, pengamanan media simpan informasi (tape/hard disk/Flashdisk/CD) dan penghapusan informasi ataupun penghancuran media	Ada
7	Pemantauan (Monitoring) Penggunaan Fasilitas TIK	Berisi proses monitoring penggunaan CPU, storage, email, internet, fasilitas TIK lainnya dan pelaporan serta tindak lanjut hasil monitoring	Ada
8	User Access Management	Berisi proses dan tatacara pendaftaran, penghapusan dan review hak akses user, termasuk administrator, terhadap sumber daya informasi (aplikasi, sistem operasi, database, internet, email dan internet)	Ada

9	Teleworking	Pengendalian dan pengamanan penggunaan hak akses secara remote (misal melalui modem atau jaringan). Siapa yang berhak menggunakan dan cara mengontrol agar penggunaannya aman.	Ada
10	Pengendalian instalasi software & Hak Kekayaan Intelektual	Berisi daftar software standar yang diijinkan di Instansi, permintaan pemasangan dan pelaksana pemasangan termasuk penghapusan software yang tidak diijinkan	Ada
11	Pengelolaan Perubahan (Change Management) TIK	Proses permintaan dan persetujuan perubahan aplikasi/infrastruktur TIK, serta pengkinian konfigurasi/database/versi dari asset TIK yang mengalami perubahan.	Ada
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi	Proses pelaporan & penanganan gangguan/insiden baik menyangkut ketersediaan layanan atau gangguan karena penyusupan/pengubahan informasi secara tidak berwenang. Termasuk analisis penyebab dan eskalasi jika diperlukan tindak lanjut ke aspek legal.	Ada

Dokumen yang diperiksa:

1. Peraturan Bupati Belitung Nomor 51 Tahun 2016 Tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, serta Tata Kerja Dinas Komunikasi dan Informatika Kabupaten Belitung;
2. Peraturan Daerah Kabupaten Belitung Nomor 3 Tahun 2019 tentang Rencana Pembangunan Jangka Menengah Daerah Kabupaten Belitung Tahun 2018-2023;
3. Perubahan Rencana Kerja Dinas Komunikasi dan Informatika Kabupaten Belitung Tahun 2021;
4. Rencana Kerja Dinas Komunikasi dan Informatika Kabupaten Belitung Tahun 2021;
5. Peraturan Bupati Belitung Nomor 25 Tahun 2020 tentang Pedoman Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik;
6. Keputusan Kepala Dinas Komunikasi dan Informatika Kabupaten Belitung Tahun 2020 tentang Rencana Induk Pengembangan TIK;
7. Keputusan Kepala Dinas Komunikasi dan Informatika Kabupaten Belitung Tahun 2020 tentang Kebijakan Keamanan Informasi;
8. Keputusan Kepala Dinas Komunikasi dan Informatika Kabupaten Belitung Tahun 2020 tentang Tata Cara Pemusnahan Barang TIK milik daerah Kab Belitung;
9. Keputusan Kepala Dinas Komunikasi dan Informatika Kabupaten Belitung Tahun 2020 tentang Pedoman Penggunaan Aset TIK;
10. Kebijakan Manajemen Aset TIK dan Klasifikasi Informasi;
11. Kebijakan Manajemen Insiden Keamanan Informasi;
12. Kebijakan Manajemen Risiko TIK;
13. Kebijakan Pengendalian Hak Akses TIK;
14. Kebijakan Pengendalian Keamanan Vendor;
15. Kebijakan Penggunaan Komputer, Internet dan Email;
16. Standar Operasional Prosedur Pengelolaan Log Server;
17. Standar Operasional Prosedur Pengendalian Dokumen dan Rekaman;
18. Standar Operasional Prosedur Pengendalian Hak Akses;
19. Standar Operasional Prosedur Penggunaan Komputer oleh Pihak Eksternal Dinas Kominfo;
20. Standar Operasional Prosedur Akses Ruangan Server;
21. Standar Operasional Prosedur Backup Server;
22. Standar Operasional Prosedur Pelaporan Insiden Keamanan Informasi;
23. Standar Operasional Prosedur Pemberian Remote Akses;
24. Standar Operasional Prosedur Penanganan Kondisi Darurat dan Rencana Kelangsungan;

25. Standar Operasional Prosedur Pengelolaan Gangguan/Permasalahan dan Permintaan Layanan;
26. Standar Operasional Prosedur Pengelolaan Hubungan dengan Pengguna Layanan;
27. Standar Operasional Prosedur Pengelolaan Kepatuhan;
28. Standar Operasional Prosedur Pelayanan Informasi Publik Pejabat Pengelola Informasi dan Dokumentasi Kabupaten Belitung;
29. Standar Operasional Prosedur Pemeliharaan Aset TIK oleh Penyedia Jasa Pemeliharaan;
30. Standar Operasional Prosedur Pemeliharaan Aset TIK;
31. Standar Operasional Prosedur Pemeliharaan Website Perangkat Daerah;
32. Standar Operasional Prosedur Pembuatan Nama Domain dan Subdomain Organisasi Perangkat Daerah;
33. Standar Operasional Prosedur Pengembangan Website Perangkat Daerah;
34. Keputusan Kepala Dinas Kominfo Kab Belitung tentang Perubahan Pertama atas Keputusan Kepala Diskominfo tentang Tim Implementasi SMKI;
35. Topologi Jaringan FTTH Kominfo;
36. Surat Permohonan Pembahasan Kerjasama dengan BsrE;
37. Surat Permohonan Pembahasan Kerjasama dengan Universitas Indonesia;
38. Surat Koordinasi Pelaksanaan Penilaian Indeks Keamanan Informasi (KAMI) Tahun 2021;
39. Surat Keputusan Bupati Belitung tentang Pembentukan Tim Evaluator Internal SPBE Kabupaten Belitung Tahun 2020;
40. Laporan SMKI Penilaian Mandiri Indeks KAMI Tahun 2021;
41. Laporan Implementasi SMKI Pembahasan Pembuatan Laporan Hasil Pemantauan dan Evaluasi Penyelenggaraan Urusan Persandian Pemerintah Kabupaten Belitung Tahun 2020;
42. Pakta Integritas Pencegahan dan Pemberantasan Korupsi, Kolusi dan Nepotisme;
43. Daftar Hadir Rapat Pembahasan Nota kesepakatan antara Kabupaten Belitung dan BSSN tentang pemanfaatan sertifikat elektronik pada sistem elektronik di lingkungan Pemerintah Kabupaten Belitung;
44. Perubahan Perjanjian Kinerja Diskominfo Kab Belitung Tahun 2021 an. Laila Asfiyani;
45. Perubahan Perjanjian Kinerja Diskominfo Kab Belitung Tahun 2021 an. Mohd. Isnaini;
46. Surat Penghapusan Aset BMN yang berupa aset TIK ke BPKAD Kab Belitung Tahun 2020;
47. Sasaran Kerja Pegawai Tahun 2019 an. Ikhwanudin;
48. Sasaran Kerja Pegawai Tahun 2020 an. Ikhwanudin;
49. Surat Penyampaian Laporan Hasil Pemantauan dan Evaluasi Penyelenggaraan Urusan Persandian Pemerintah Kabupaten Belitung Tahun 2020 ke Provinsi Kepulauan Bangka dan Belitung;
50. Laporan Instalasi Software Antivirus Perangkat Laptop Dell;
51. Laporan Pendahuluan Penyusunan Rancangan Kebijakan Arsitektur Keamanan Informasi Kabupaten Belitung;
52. Screenshot hasil koordinasi penyampaian laporan persandian via email sanapati;
53. Lampiran Berita Acara serah terima pekerjaan pengadaan monitor LED dan software antivirus;
54. Laporan Dokumentasi Pengkodean Aplikasi customize ILDIS JDIH DPRD Kab. Belitung;
55. Laporan Pembaharuan Secure Socket Layer (SSL) untuk subdomain <https://cloud.belitungkab.go.id>;
56. Laporan Update dan Konfigurasi Simda Integrated (<https://simcan.belitungkab.go.id>);
57. Kerangka Acuan Kerja (KAK) Kegiatan Pelaksanaan Keamanan Informasi Pemda Kabupaten/Kota Berbasis Elektronik dan Non Elektronik;
58. Kerangka Acuan Kerja (KAK) Kegiatan Pelaksanaan Analisis Kebutuhan dan Pengelolaan Sumber Daya Keamanan Informasi Pemda Kabupaten/Kota;
59. Kerangka Acuan Kerja (KAK) Kegiatan Penetapan Kebijakan Tata Kelola Keamanan Informasi dan Jaring Komunikasi Sandi Pemda Kabupaten/Kota;
60. Kartu Inventaris Ruangan Server per 31 Desember 2020;
61. Data SSL Pemerintah Kabupaten Belitung;

- 62. Dokumen Updating antivirus Smadav;
- 63. Dokumentasi Kegiatan Sosialisasi Keamanan Informasi Tahun 2018-2020;
- 64. Himbauan Tata Tertib Pengunjung Server;
- 65. IT Risk Register Dinas Kominfo Kabupaten Belitung Tahun 2021;
- 66. Daftar Aset dan Klasifikasi (Hardware Sarana Pendukung Ruang Server dan, Informasi, Sumber Daya Manusia Pengelola TIK, Software) Dinas Kominfo Kabupaten Belitung Tahun 2020;
- 67. Surat Rekomendasi Permohonan Penerbitan Sertifikat Elektronik OSD Lemsaneg Tahun 2021;
- 68. Analisis Jabatan Khusus Tim Implementasi SMKI Tahun 2021;
- 69. Checklist Pemeliharaan Server Simda Keuangan Online Tahun 2019;
- 70. Checklist Pemeliharaan Server Simda Perencanaan Online Tahun 2019
- 71. Sertifikat Pelatihan personil Dinas Kominfo Kabupaten Belitung Tahun 2018-2020;
- 72. Dokumen Draft Syarat-syarat khusus kontrak;
- 73. Jadwal Rentensi Arsip Fasilitatif Non Keuangan dan Non Kepegawaian di Lingkungan Pemkab Belitung;
- 74. Jadwal Retensi Arsip merujuk Perbup Nomor 36 Tahun 2019 tentang jadwal reteensi arsip substantif sektor perekonomian di lingkungan Pemkab Belitung.

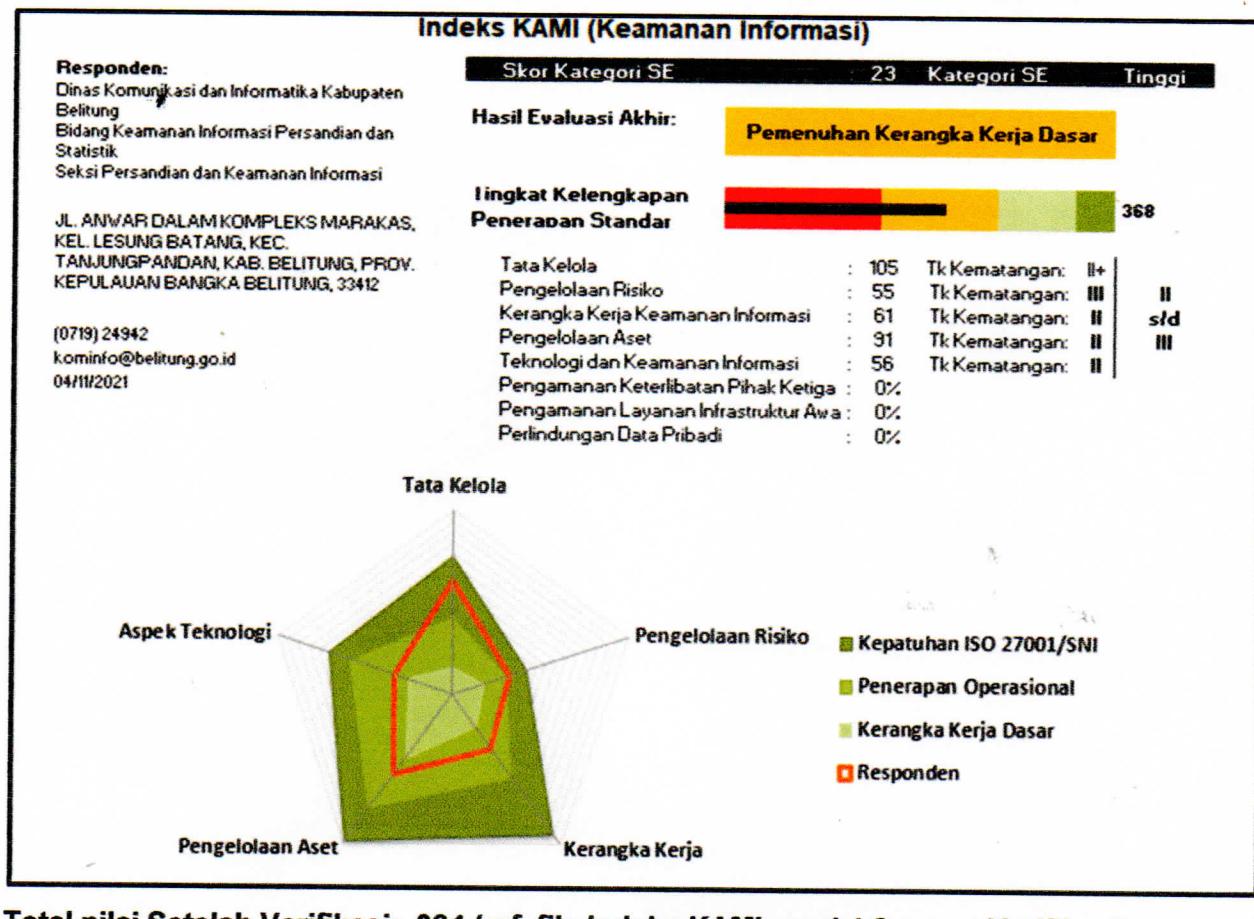
Berdasarkan verifikasi terhadap dokumen dan wawancara terhadap narasumber instansi/lembaga disimpulkan sbb:

I. KONDISI UMUM:

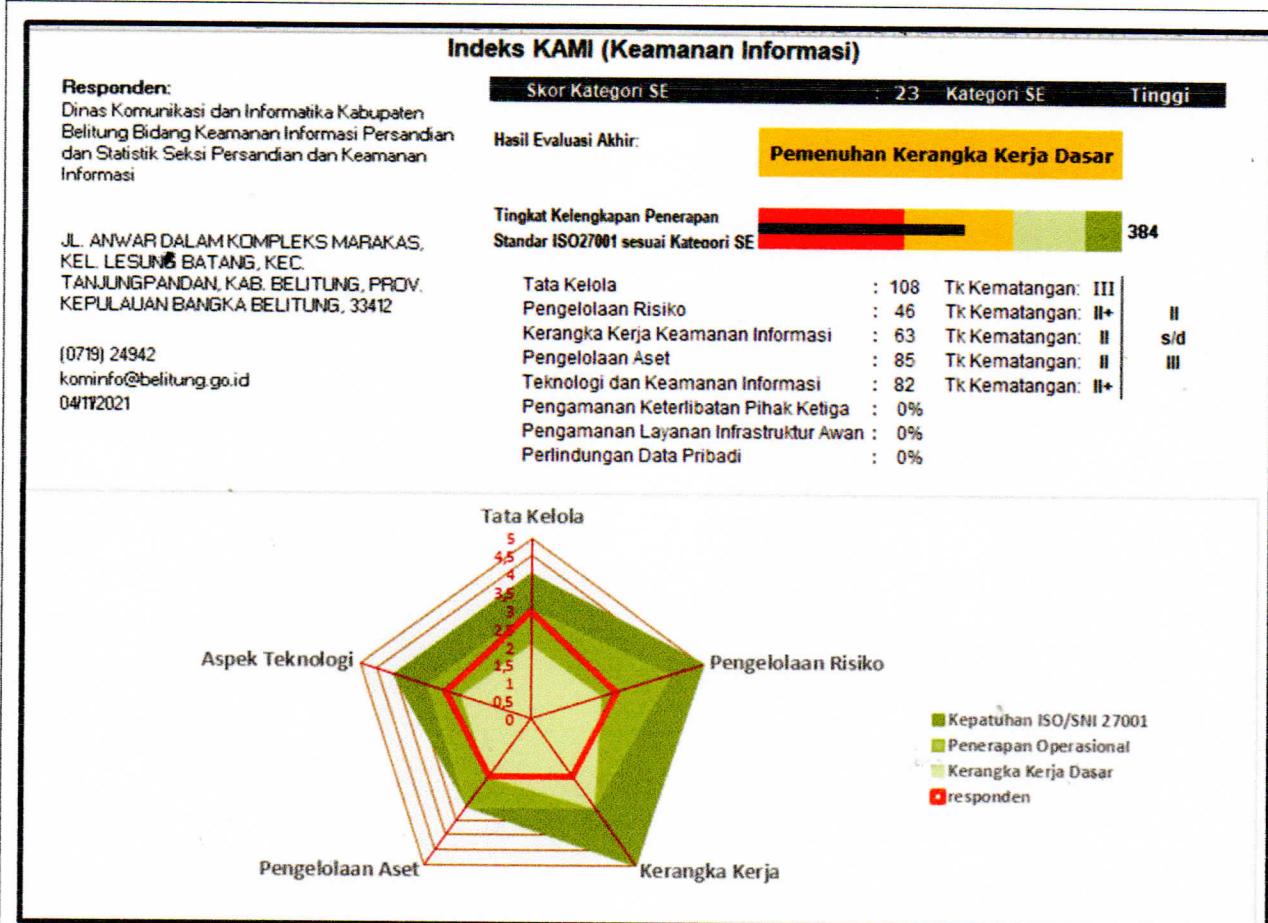
1. Struktur organisasi satuan kerja dalam ruang lingkup berada di bawah Dinas Komunikasi dan Informatika Kabupaten Belitung yang terdiri atas:
 - a. Sekretariat
 - b. Bidang Informasi dan Komunikasi Publik
 - c. Bidang Aplikasi Informatika
 - d. Bidang Keamanan Informasi, Persandian dan Statistik
2. SDM pengelola terdiri dari:
Jumlah pegawai di Dinas Komunikasi dan Informatika Kabupaten Belitung adalah 40 personil ASN dan non ASN.
3. Berdasarkan verifikasi terhadap hasil Self Assessment isian file Indeks KAMI diperoleh hasil sebagai berikut:

Dinas Komunikasi dan Informatika Kabupaten Belitung mengelola Sistem Elektronik dalam kategori Tinggi dengan hasil evaluasi akhir pada level Pemenuhan Kerangka Kerja Dasar dengan tingkat kelengkapan penerapan standar ISO 27001 sesuai kategori pada skor nilai 384.

Total nilai Sebelum Verifikasi: 369 (ref. file Indeks KAMI versi 4.1 pra Verifikasi)



Total nilai Setelah Verifikasi: 384 (ref. file Indeks KAMI versi 4.2 pasca Verifikasi)



II. ASPEK TATA KELOLA:

a. Kekuatan/Kematangan

1. Diskominfo Pemkab Belitung telah menetapkan kebijakan secara resmi dan bertanggung jawab terhadap pelaksanaan program keamanan informasi baik yang tertuang dalam program jangka menengah maupun jangka pendek.
2. Telah memiliki fungsi dan wewenang dengan sumber daya yang sesuai dalam pengelolaan keamanan informasi dan dituangkan dalam Tim Implementasi Sistem Manajemen Keamanan Informasi melalui Keputusan Kepala Dinas Komunikasi dan Informatika Nomor 188.46/088.a/KPTS/X/Diskominfo.
3. Telah memiliki program peningkatan kompetensi dan keahlian pengelolaan keamanan siber yang dilakukan secara berkelanjutan.
4. Telah mengintegrasikan persyaratan keamanan informasi dalam proses kerja yang ada mulai dari program jangka menengah dan pendek serta kebijakan keamanan informasi telah menjadi panduan dalam penerapan aktivitas program pengelolaan keamanan siber organisasi.
5. Telah diidentifikasi tanggungjawab pengelolaan keamanan informasi melalui koordinasi pihak pengelola asset informasi internal dan eksternal baik melalui perjanjian kerjasama dengan pihak ketiga maupun dengan Non Disclosure Agreement (NDA) yang telah disusun.
6. Program keamanan informasi telah menjadi konsideran dalam proses pengambilan keputusan strategis dan telah didefinisikan dalam metrik pengukuran kinerja yang dipantau ekskalasinya baik dari petugas sampai dengan pejabat (pimpinan organisasi).
7. Telah terdapat penerapan target dan sasaran pengelolaan keamanan informasi namun belum dilakukan evaluasi secara rutin sebagai tahap perbaikan dalam mencapai sasaran organisasi.
8. Telah memiliki definisi kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum.

b. Kelemahan/Kekurangan

1. Belum adanya pemetaan kebutuhan audit internal yang akan membantu penerapan sistem manajemen keamanan informasi.
2. Telah memiliki pendefinisian persyaratan kompetensi dan keahlian pengelola keamanan informasi namun masih terbatas pada uraian jabatan individu yang telah ditugaskan belum secara menyeluruh memiliki definisi persyaratan/standar kompetensi dan keahlian yang dibutuhkan secara ideal dengan mengacu pada standar kompetensi/keahlian yang memadai.
3. Telah dibuat daftar pemenuhan kompetensi analisis jabatan khusus tim implementasi sistem manajemen keamanan informasi berdasarkan sesuai kebutuhan dengan kondisi eksisting namun belum mengacu pada persyaratan/standar yang berlaku.(kesesuaian dengan daftar analisis jabatan pengelola keamanan informasi).
4. Telah memiliki program sosialisasi dan peningkatan pemahaman keamanan informasi namun belum memiliki program penilaian kepatuhan terhadap kebijakan yang telah ditetapkan baik secara internal (antar satker terkait) maupun pihak eksternal yang berkepentingan yang dilaporkan secara rutin kepada pimpinan.
5. Pengaturan data pribadi belum diidentifikasi secara khusus dalam proses kerja yang digunakan selanjutnya dalam penerapan pengamanan sesuai dengan peraturan perundang-undangan.
6. Telah didefinisikan BCP dan DRP dalam kebijakan keamanan informasi namun implementasi terhadap langkah keberlangsungan layanan TIK belum disusun dan dialokasikan dalam kebijakan.
7. Belum ada konsideran kebijakan keamanan informasi yang menjadi dasar regulasi yang dituangkan dalam daftar kebijakan yang harus dievaluasi tingkat kepatuhannya.

III. ASPEK RISIKO:

a. Kekuatan/Kematangan

1. Diskominfo Pemkab Belitung telah memiliki program, kerangka kerja dan definisi, hubungan tingkat klasifikasi aset informasi, tingkat ancaman, dampak kerugian dan penetapan ambang batas tingkat risiko pengelolaan risiko keamanan informasi melalui kebijakan manajemen risiko aset TIK yang telah digunakan secara resmi.
2. Telah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur dalam mengidentifikasi langkah mitigasi dalam program pengelolaan keamanan informasi yang akan dilakukan.
3. Telah memiliki dokumen IT Risk Register.

b. Kelemahan/Kekurangan

1. Telah menetapkan penanggung jawab manajemen risiko namun ekskalasi pelaporan belum dilakukan.
2. Telah didefinisikan kepemilikan namun pengelola aset informasi belum dicantumkan, untuk pengelompokan aset sudah dilakukan namun belum terlihat pada proses kerja utama dalam kebijakan manajemen risiko.
3. Telah melakukan identifikasi terhadap ancaman dan kelemahan yang terkait dengan aset informasi namun belum secara lengkap terhadap seluruh aset yang telah diidentifikasi dan belum ada penetapan aset utama yang juga perlu ditambahkan risiko-risiko lainnya.
4. Telah ditetapkan dampak kerugian terkait dengan terganggunya fungsi aset utama namun belum secara menyeluruh.
5. Telah menyusun 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 efektifitasnya terhadap kebijakan manajemen risiko yang dimiliki.

7. Kebijakan penyelesaian langkah mitigasi risiko telah ditetapkan namun implementasinya belum dilakukan pemantauannya secara berkala.
8. Telah terdapat profil risiko dan mitigasi yang perlu dikaji secara berkala dan dituangkan dalam penetapan kebijakan manajemen risiko namun belum terdapat implementasi maupun langkah aksi dalam proses keberlanjutannya dalam memastikan konsistensi dan efektifitasnya.
9. Kebijakan profil risiko telah tertuang dalam IT Risk Register namun masih dalam tahap awal perencanaan dan perlu dilakukan penyempurnaan dan review secara berkala.
10. Pengelolaan risiko telah menjadi tujuan dalam kebijakan manajemen risiko, namun belum terdapat monitoring dan evaluasi pengelolaan risiko.

IV. ASPEK KERANGKA KERJA:

a. Kekuatan/Kematangan

1. Diskominfo Pemkab Belitung telah memiliki kebijakan dan prosedur terkait keamanan informasi yang ditetapkan secara formal dan telah dipublikasikan kepada semua pegawai berupa keputusan Kepala Dinas Kominfo tentang Kebijakan Keamanan Informasi.
2. Telah tersedia kebijakan untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi dalam suatu SOP Pelaporan Insiden.
3. Telah memiliki SOP tentang akses ruangan server yang berisikan himbauan tata tertib masuk ruang server yang telah diimplementasikan dengan baik
4. Telah memiliki rencana dan program peningkatan keamanan informasi baik jangka pendek maupun menengah namun belum secara konsisten keterhubungan di antara dokumen tersebut berikut penerapannya.

b. Kelemahan/Kekurangan

1. Telah memiliki kebijakan SOP tentang pengendalian dokumen dan rekaman namun belum berisikan prosedur pengelolaan dokumen mulai dari distribusi penarikan dari peredaran dan penyimpanannya dan belum memiliki daftar induk dokumen keamanan informasi yang berisikan daftar dokumen Kebijakan dan SOP yang dimiliki serta ditambah keterangan telah dilakukan sosialisasi/belum.
2. Telah dilakukan kegiatan mengkomunikasikan kebijakan keamanan informasi dan perubahan yang dilakukan kepada pihak internal namun belum secara periodik dan belum melibatkan pihak ketiga.
3. Telah memiliki risk register yang berisikan mitigasi hasil kajian risiko namun karena mitigasi belum dilakukan secara menyeluruh terhadap seluruh asset yang dimiliki maka belum dapat merefleksikan kebutuhan kebijakan dan prosedur keamanan informasi.
4. Dalam dokumen NDA/syarat-syarat khusus kontrak (SSKK) dengan pihak ketiga telah mencantumkan aspek keamanan informasi yang meliputi menjaga kerahasiaan, HAKI namun belum terdapat klausul pelaporan insiden, tata tertib penggunaan dan pengamanan asset maupun layanan TIK yang dipertukarkan dengan user.
5. Telah memiliki kebijakan pengendalian hak akses, pengendalian keamanan vendor namun belum memiliki penerapan konsekwensi terhadap pelanggaran yang dilakukan pihak internal maupun eksternal.
6. Penerapan kebijakan pengelolaan implementasi security patch belum dilakukan secara berkesinambungan.
7. Aspek keamanan informasi telah menjadi bagian dalam pelaksanaan manajemen proyek namun belum dilakukan secara menyeluruh terhadap seluruh lingkup proyek organisasi maupun penerapan evaluasi risiko terkait rencana pembelian sistem baru dan upaya mengatasi permasalahan yang muncul sesuai dengan jadwal penyelesaian yang telah ditetapkan.
8. Telah memiliki kebijakan tentang pengelolaan kepatuhan instalasi software namun belum ada tahapan proses pengembangan secure SDLC.

9. BCP dan DRP telah menjadi bagian dari kebijakan keamanan informasi namun belum direalisasikan penyusunan dan implementasi serta pengujian dan pemantauannya secara berkelanjutan.
10. Telah memiliki kebijakan keamanan informasi namun implementasinya belum menjadi bagian dari strategi rencana kerja organisasi dan belum dilakukan penerapan serta pemutakhiran penggunaan teknologi keamanan informasi yang disesuaikan dengan kebutuhan dan perubahan profil organisasi.
11. Telah memiliki audit internal yaitu tim evaluator SPBE namun belum mencakup evaluasi terhadap keseluruhan aset informasi, kebijakan dan prosedur keamanan yang telah dimiliki secara konsisten, mengukur kepatuhan serta mengkaji langkah pencegahan sebagai upaya peningkatan dan perbaikan kinerja keamanan informasi yang dilaporkan kepada pimpinan.
12. Di dalam kebijakan keamanan informasi telah terdapat lingkup *business continuity management*/BCM yang berisikan tentang pentingnya mengukur dampak namun belum dituangkan secara spesifik (khusus).
13. Belum adanya tahap pengujian dan evaluasi terhadap kepatuhan program keamanan informasi yang memastikan rencana aksi yang ditetapkan telah efektif dan sesuai dengan langkah pemberian yang diperlukan.

V. ASPEK PENGELOLAAN ASET:

a. Kekuatan/Kematangan

1. Diskominfo Pemkab Belitung telah memiliki definisi klasifikasi aset informasi dan melakukan proses evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingannya melalui update aplikasi SIMDA yang dilakukan per semester dengan bentuk berupa laporan mutasi barang.
2. Telah memiliki mekanisme proses penyidikan/investigasi penyelesaian insiden keamanan informasi.
3. Telah 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. Telah memiliki prosedur kebijakan pengendalian hak akses yang mengatur user yang mutasi/keluar baik pegawai tetap maupun tenaga kontrak.
5. Telah memiliki peraturan pengamanan lokasi kerja penting (ruang server) berupa tata tertib himbauan masuk bagi pengguna/pengunjung layanan data center.

b. Kelemahan/Kekurangan

1. Telah memiliki daftar inventaris aset informasi dengan format sesuai BKAD namun belum terdapat inventaris aset aplikasi dan layanan.
2. Telah memiliki kebijakan tingkatan akses yang berbeda dari setiap klasifikasi aset informasi, namun belum memiliki *user access metrik* yang dapat merekam alokasi akses tersebut.
3. 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.
4. Telah tersedia proses merilis aset baru yang merujuk pada kebijakan tentang pengelolaan BMD dan telah terekam pada aplikasi SIMDA namun belum ada proses pemutakhiran inventaris aset.
5. Pendefinisian tanggung jawab pengamanan informasi telah dilakukan pada pegawai ASN namun belum diberlakukan pada pegawai non ASN.
6. Telah memiliki kebijakan dan SOP terkait penggunaan komputer, email dan internet, namun perlu perbaikan dan penambahan tata tertib intranet
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. Telah memiliki mekanisme penggunaan data pribadi melalui permohonan ke PPID,

- namun belum ada standar prasyarat ijin tertulis sebagai bentuk serah terima atau pengaturan penggunaan data pribadi agar tidak disalahgunakan oleh pihak yang tidak bertanggungjawab.
9. Belum memiliki kebijakan proses otentikasi dan sanksi pelanggaran.
 10. Belum memiliki kebijakan klasifikasi data sampai dengan waktu penyimpanan dan metode pemusnahannya.
 11. Belum memiliki kebijakan terkait dengan pertukaran data dengan pihak eksternal.
 12. Telah memiliki kebijakan atau prosedur backup server dan mekanisme akses ruang server namun belum memiliki proses backup dan restore secara berkala serta belum memiliki kebijakan keamanan fisik dan lingkungan (perimeter fisik, akses masuk, pengamanan CCTV).
 13. 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).
 14. Telah memiliki tata cara pemusnahan barang TIK namun belum mencantumkan pemusnahan data/aset yang membedakan klasifikasi aset yang dimiliki organisasi.
 15. Telah memiliki kebijakan pengendalian hak akses namun belum ada langkah pemberian apabila terjadi ketidaksesuaian.
 16. Telah tersedia daftar data/informasi yang harus dibackup namun masih terbatas di server.
 17. Telah tersedia prosedur rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya namun belum dilakukan dokumentasi secara berkelanjutan
 18. Telah memiliki kebijakan pengendalian vendor namun di dalamnya belum terdapat mekanisme prosedur untuk memastikan kepatuhan terhadap kebijakan dan kontrak terkait dengan HAKI dan penggunaan perangkat keras/lunak.
 19. Telah dilakukan penerapan keamanan fasilitas fisik namun terbatas hanya pada data center, untuk ruang lingkup lainnya di Diskominfo belum diberlakukan.
 20. Telah memiliki proses pengelolaan alokasi kunci masuk fisik dan elektronik namun terbatas hanya pada data center, untuk ruang lingkup lainnya di Diskominfo belum diberlakukan.
 21. Telah memiliki prosedur perlindungan terhadap infrastruktur komputasi dari dampak lingkungan maupun gangguan pasokan listrik namun penerapan dan evaluasi belum dilakukan secara berkala dalam menjaga ketersediaan dan keamanan layanan TIK di dalamnya.
 22. Belum memiliki peraturan *mobile computing* dan teleworking, kebijakan peminjaman/pemindahan aset TIK berikut formulirnya, proses perawatan peralatan komputasi dan mekanisme terkait dengan implementasi kebijakan pengendalian vendor seperti berita acara, form masuk keluar barang dan mekanisme kirim terima informasi melalui email dinas.
 23. Telah tersedia proses pengamanan lokasi kerja data center dengan menggunakan kaidah yang ditetapkan, namun untuk ruang kerja belum diberlakukan aspek pengamanannya.

VI. ASPEK TEKNOLOGI

a. Kekuatan/Kematangan

1. Diskominfo Pemkab Belitung telah menggunakan mekanisme perlindungan dengan antivirus, firewall dan SLL serta pengamanan dengan password dan telah melakukan segmentasi jaringan sesuai dengan kepentingannya.
2. Proses keamanan sistem pada seluruh aset jaringan, sistem dan aplikasi telah mengikuti perkembangan seperti access point telah terlindungi dengan mode WPA2, GeoTrust SSL namun belum dilengkapi dengan kebijakan pengendalian/pengelolaan konfigurasi.
3. Telah memiliki monitoring infrastruktur jaringan, sistem dan aplikasi dengan menggunakan dashboard Centos Web Panel yang digunakan untuk melakukan

manage user, cPanel untuk pengaturan layanan web hosting, proxmox untuk mengelola proses virtualisasi, UniFi Controller untuk pengendali perangkat WiFi.

4. Terdapat proses perekaman dalam setiap perubahan dalam sistem informasi secara otomatis pada aplikasi eBesilak dan catatan pada log database simda.
5. Telah memiliki perekaman upaya akses oleh pihak yang tidak berkepentingan melalui Centos Web Panel dan cPanel yang digunakan dalam melakukan pengelolaan fitur hosting dan analisa statistik website.
6. Telah dilakukan penerapan penggantian password secara otomatis pada aplikasi webmail dan dibuat kebijakan penggunaan kompleksitas password dan aktivasi autentikasi dua faktor dengan menggunakan cPanel web hosting.
7. Telah diberlakukan pembatasan waktu akses otomatisasi dengan durasi *destroy session time out* adalah selama 30 menit.
8. Telah dilakukan perlindungan terhadap seluruh perangkat desktop dan server. Untuk linux dengan firewall dan windows dengan *kaspersky small office security* yang dipelihara lisensinya secara rutin setiap tahunnya.
9. Telah menggunakan mekanisme sinkronisasi waktu secara akurat dengan *Network Time Protocol*.

b. Kelemahan/Kekurangan

1. Belum adanya proses analisa kepatuhan penerapan konfigurasi sesuai standar yang ada.
2. Telah dilakukan kegiatan *vulnerability assessment* namun belum dilakukan secara berkala baik pada penjadwalannya maupun keseluruhan sistem dan aplikasi yang telah dimiliki.
3. Belum memiliki konsep penyediaan redundant terhadap keseluruhan infrastruktur jaringan, sistem dan aplikasi yang dimiliki, masih sebatas back up database dan aplikasi.
4. Analisa log telah dilakukan namun belum secara berkala, masih bersifat insidentil dan belum ada penjadwalan yang dilakukan secara periodik.
5. Belum adanya implementasi penggunaan enkripsi sesuai kebijakan yang telah ditetapkan termasuk penerapan pengamanan pengelolaan kunci enkripsi yang digunakan.
6. Telah menerapkan pengelolaan sistem dengan bentuk pengamanan berlapis yaitu pada aplikasi LPSE dengan menggunakan captcha dan aplikasi siskeudes menggunakan metode MFA dengan dua kali login. Penerapan tersebut belum diimplementasikan pada keseluruhan sistem yang dimiliki.
7. Telah menerapkan mekanisme pendeteksian dan pencegahan penggunaan akses jaringan dengan menggunakan firewall, belum menggunakan IDS/IPS.
8. Telah dilakukan pemutakhiran versi terkini perangkat desktop dan server namun terbatas pada sistem operasi linux yaitu dengan Ubuntu versi 20, untuk sistem operasi windows masih menggunakan window server 2016 (hal ini dilakukan karena untuk menjaga lisensi sistem operasi didalamnya supaya tetap available)
9. Belum adanya mekanisme proses analisa secara rutin terhadap jejak audit antivirus/antimalware.
10. Belum dilakukan mekanisme laporan adanya penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan yang juga didokumentasikan.
11. Telah menetapkan kebijakan prasyarat pelaksanaan penetration testing terhadap setiap aplikasi yang dikembangkan namun belum dilakukan penerapan dan penjadwalan pengujian tersebut yang didokumentasikan sebagai bagian dari proses pengembangan aplikasi yang perlu dilakukan pemantauannya.
12. Telah menerapkan lingkungan pengembangan dan uji coba sesuai kriteria keamanan namun belum berlaku pada seluruh siklus hidup sistem yang telah dibangun.
13. Telah melibatkan pihak independen (BSSN) untuk mengkaji kehandalan keamanan informasi baik pada sistem manajemen keamanan informasi maupun aplikasi yang dimiliki namun belum dilakukan secara rutin dan terjadwal (untuk kegiatan penetration testing belum secara rutin sedangkan kegiatan verifikasi penilaian indeks kami telah dilakukan secara rutin tiap tahunnya).

VIII. REKOMENDASI

1. Perlu adanya pemetaan kebutuhan audit internal keamanan informasi yang akan membantu penerapan dan pengelolaan sistem manajemen keamanan informasi (SMKI) secara lebih efektif. Dimana audit internal merupakan salah satu prasyarat utama dalam pemenuhan implementasi SMKI selain komponen lainnya seperti kebijakan, tanggung jawab manajemen, mekanisme peninjauan ulang dan proses peningkatan berkelanjutan
2. Perlu dilakukan reviu kembali terhadap persyaratan/standar kompetensi dan keahlian yang dibutuhkan secara ideal tiap personil yang bertugas dalam lingkup keamanan informasi dengan mengacu pada standar kompetensi/keahlian yang memadai.
3. Perlu adanya penambahan program penilaian kepatuhan terhadap kebijakan yang telah ditetapkan baik secara internal (antar satker terkait) maupun pihak eksternal yang berkepentingan yang dilaporkan secara rutin kepada pimpinan sebagai bahan evaluasi perbaikan penerapan SMKI.
4. Perlu menyusun dan menetapkan kebijakan terkait dengan data pribadi yang merujuk pada PP. 71 Tahun 2019 dan Perkominfo Nomor 20 Tahun 2016.
5. Perlu dilakukan penyusunan dokumen BCP dan DRP sebagai upaya dalam menjaga keberlangsungan bisnis proses dalam menghadapi adanya gangguan terhadap operasional layanan Pemkab Belitung. Dalam dokumen tersebut meliputi tahap persiapan, pengujian dan pemutakhiran tindakan-tindakan yang diperlukan dalam melindungi keseluruhan aset dan bisnis proses kritis terhadap adanya kegagalan sistem dan jaringan yang ada. Di dalam BCP juga terdapat *business impact analysis* yang akan membantu organisasi untuk memetakan dampak dari identifikasi risiko yang akan timbul dari adanya ancaman keamanan informasi.
6. Perlu menetapkan landasan yuridis sebagai konsideran pelaksanaan kebijakan keamanan informasi yang harus dievaluasi tingkat kepatuhannya secara berkala.
7. Perlu perbaikan kebijakan manajemen risiko dalam proses kerangka kerja dan dasar dalam implementasi manajemen risiko yang akan digunakan dalam proses evaluasi secara rutin.
8. Perlu memperbarui dan menambahkan daftar risiko dalam dokumen IT Risk Register dengan menerapkan kontrol perbaikan yang disesuaikan dengan kriteria penerimaan risiko.
9. Perlunya penambahan tahapan penanggulangan risiko sampai dengan level kriteria penerimaan risiko/ *Risk Acceptance Criteria* (RAC), langkah prioritas dan target serta penanggung jawab penyelesaian risiko serta metode memastikan efektifitasnya terhadap kebijakan manajemen risiko yang dimiliki.
10. Perlu dibuat program implementasi terhadap profil risiko telah tertuang dalam IT Risk register sebagai bentuk monitoring dan evaluasi penerapan pengamanan organisasi.
11. Perlunya *update risk register*, pelaksanaan evaluasi sebagai bahan penyampaian rekomendasi ke pimpinan dalam pembelian sistem dan mengatasi permasalahan keamanan informasi.
12. Perlu menambahkan tahapan proses ekskalasi pelaporan pelaksanaan manajemen risiko yang perlu ditambahkan dalam kebijakan manajemen risiko atau dokumen BCP (prosedur *call tree response*).
13. Perlu pencantuman pengelola aset informasi untuk memudahkan pengontrolan/pihak yang bertanggung jawab saat terjadi kerusakan atau kehilangan aset.
14. Perlunya penambahan penetapan aset utama yang juga perlu ditambahkan risiko-risiko lainnya sebagai upaya mitigasi dan perlindungan terhadap adanya ancaman pada tiap tingkat klasifikasi aset yang dimiliki.
15. Terhadap kebijakan keamanan informasi yang saat ini telah ditetapkan dalam peraturan Kepala Dinas Kominfo, saran untuk pengaturan yang lebih luas pada seluruh perangkat daerah yang ada di Pemkab Belitung maka kebijakan tersebut dapat ditingkatkan menjadi Peraturan Bupati dimana kewenangan Diskominfo sesuai tugas dan fungsi dalam menjaga keamanan informasi seluruh Pemkab akan terwujud dan relatif mudah dalam proses pengendalian dan monitoring terhadap implementasi kebijakan keamanan lainnya yang terkait.
15. Perlunya prosedur pengelolaan dokumen mulai dari distribusi penarikan dari peredaran

- dan penyimpanannya dan daftar induk dokumen keamanan informasi yang berisikan daftar dokumen Kebijakan maupun SOP yang dimiliki dan ditambahkan keterangan telah dilakukan sosialisasi/belum sebagai tahapan dalam monitoring implementasi kebijakan.
16. Perlu dilakukan kegiatan *sharing session* secara rutin terhadap adanya kebijakan keamanan informasi dan perubahannya yang dilakukan kepada pihak internal dan eksternal (pihak ketiga) baik melalui forum formal maupun non formal (berbagi informasi melalui platform media sosial).
 17. Perlunya penambahan kriteria aspek keamanan informasi berupa klausul pelaporan insiden, tata tertib penggunaan dan pengamanan aset maupun layanan TIK yang dipertukarkan dengan user baik pada NDA maupun SSSK.
 18. Perlunya penerapan konsekwensi terhadap pelanggaran yang dilakukan pihak internal maupun eksternal.
 19. Perlu penambahan SOP *security patch*, keamanan operasional yang mencakup perlindungan terhadap sistem elektronik yang dimiliki, monitoring keamanan infrastruktur, jaringan server dan manajemen kerentanan.
 20. Perlunya melakukan penguatan terhadap fungsi audit internal yaitu tim evaluator SPBE harus mematuhi ketentuan yang tertuang dalam panduan pelaksanaan audit antara lain diidentifikasi dan disepakati, dibuat persyaratan audit dalam melakukan akses ke sistem dan data serta seluruh akses dilakukan pemantauan dan pencatatan untuk menghasilkan rekam referensi.
 21. Perlunya penambahan proses pengembangan *secure SDLC* yang disesuaikan dengan kerangka kerja pengembangan sistem aplikasi.
 22. Perlunya penambahan prosedur dan kebijakan BCP termasuk pengujinya.
 23. Perlunya untuk mengidentifikasi dampak yang akan terjadi melalui dokumen/kebijakan khusus atau terpisah dari BCM dan dilakukan identifikasi dari seluruh aset yang dimiliki sebagai upaya untuk memulihkan bisnis proses operasional organisasi dari adanya potensi ancaman dan gangguan keamanan informasi.
 24. Perlu dibuat daftar inventaris aset informasi secara lengkap (termasuk aplikasi dan layanan) yang berisikan kode dan kepemilikan inventaris serta perlu dilakukan klasifikasi tingkat aset tersebut.
 25. Perlu dibuatkan kebijakan Manajemen Perubahan yang akan membantu memastikan bahwa metode standar dan prosedur yang digunakan sudah termonitor, efisien dan mendorong penanganan dari semua perubahan dan untuk meminimalkan dampak perubahan terkait insiden pada kualitas layanan.
 26. Perlu dibuatkan SOP lainnya terkait mekanisme otentikasi dan sanksi pelanggaran penggunaan identitas elektronik.
 27. Perlu updating proses pendefinisian tanggung jawab pengamanan informasi yang jelas terhadap seluruh pegawai baik tetap maupun tidak tetap.
 28. Perlu perbaikan terhadap prosedur tata tertib penggunaan komputer, email sesuai standar dan perlu penambahan kebijakan tata tertib intranet.
 29. Perlu menyusun kebijakan dan implementasi mekanisme pengamanan dan penggunaan aset organisasi terkait HAKI seperti penggunaan lisensi resmi untuk aplikasi yang digunakan dan formulir daftar instalasi software, peminjaman aset TI.
 30. Perlu standar prasyarat pengaturan penggunaan data pribadi dan menyertakan formulir daftar data pribadi yang dikelola serta berita acara penggunaan data pribadi.
 31. Perlu menetapkan standar/kebijakan mekanisme otentikasi dan otorisasi termasuk sanksi pelanggaran terhadap kebijakan yang ditetapkan.
 32. Perlu membuat klasifikasi data yang berbeda antara arsip publik dan arsip terbatas, saran waktu penyimpanan dan pemusnahan untuk klasifikasi data perlu disesuaikan kembali.
 33. Perlu dibuatkan kebijakan/prosedur pertukaran data dengan pihak eksternal.
 34. Perlunya pendalaman terhadap proses investigasi penyelesaian insiden yang telah dilakukan dengan menambahkan sumber serangan dan melakukan analisis log.
 35. Perlu membuat standar/flowchart backup dan restore dan berita acara backup dan restore sebagai bagian dari *disaster recovery plan*.
 36. Perlu disusun SOP keamanan fisik dan lingkungan yang melingkupi perimeter fisik,

- akses masuk, pengamanan cctv dan perimeter keamanan fisik lainnya.
37. Pada SOP Pelaporan Insiden Keamanan Informasi perlu ditambahkan pihak eksternal selain penegak hukum, misalnya CSIRT Provinsi, BSSN Gov-CSIRT, Nat-CSIRT.
 38. Perlu dibuatkan SOP turunan dari kebijakan keamanan informasi yang mengatur tentang pemusnahan data/aset dengan membedakan klasifikasi asetnya.
 39. Perlu memperbaiki SOP Pengendalian hak akses dengan memasukkan langkah pemberahan terhadap ketidaksesuaian dan pemberian sanksi pelanggaran.
 40. Perlu penambahan klausul dalam SOP Kebijakan Pengendalian Keamanan Vendor yang mengikat prosedur penggunaan perangkat keras dengan contoh perlu didaftarkan terlebih dahulu perangkat yang digunakan sebelum mengakses sistem. Pengamanan akses yang digunakan juga harus ditambahkan misalnya vendor hanya diberikan akses Wifi yang terpisah dengan yang digunakan oleh internal organisasi.
 41. Perlunya penambahan kebijakan/prosedur akses masuk tamu ke ruangan diskominfo, penerapan pengamanan fisik, pembagian area penanggung jawab dan penambahan perangkat pengamanan fisik sehingga tidak terbatas pada keamanan di wilayah data center.
 42. Perlu adanya kebijakan/prosedur perawatan peralatan komputasi.
 43. Perlu penambahan mekanisme kebijakan pengendalian keamanan vendor, ada berita acara, form keluar masuk barang dan proses kirim terima informasi melalui email dinas.
 44. Perlu mekanisme perlindungan pada Wifi. Kelemahan suatu parameter pada protokol dapat menjadi celah dan mempengaruhi keamanan secara keseluruhan, sehingga meskipun telah menggunakan mode pengamanan WPA2 maka perlu penambahan fitur pengamanan diantaranya adalah enkripsi data offline, SSL dan PGP.
 45. Perlunya menyusun kebijakan/prosedur pengelolaan/pengendalian konfigurasi perangkat keras dan lunak sehingga setiap terdapat perubahan akan tercatat dalam *Log Change*.
 46. Melakukan pemindaian/*vulnerability assessment* terhadap sistem elektronik yang meliputi jaringan, sistem dan seluruh aplikasi yang dimiliki secara berkala.
 47. Perlunya ketersediaan alokasi DRC yang akan membantu menyimpan dan mengolah data dan informasi, menempatkan sistem, aplikasi dan data cadangan ketika terjadi gangguan atau bencana.
 48. Perlunya dilakukan review log secara berkala dan terjadwal, dengan bukti form review sebagai upaya dalam akurasi dan validitas serta kelengkapan isinya.
 49. Perlu dibuat turunan kebijakan dari kebijakan keamanan informasi berupa standar/prosedur penerapan kriptografi yang digunakan untuk melindungi informasi rahasia atau sensitif, atau untuk memberikan kepastian keamanan dimana kontrol yang ada masih dianggap kurang memadai dengan standar yang disesuaikan dengan kebutuhan misal enkripsi dalam transfer informasi, standar penerapan kriptografi yang digunakan, pembuatan kunci untuk password dan lainnya.
 50. Perlu dibuat SOP penggunaan password, penerapan Tanda Tangan Elektronik yang terintegrasi dengan sistem elektronik dimana terdapat skala prioritas untuk penambahan fitur pengamanannya.
 51. Perlu melakukan pencatatan jejak rekam untuk pendekripsi malware dan perbaikan perangkat lunak yang berisikan laporan pembaharuan antivirus yang telah dilakukan secara rutin dan perlu adanya mekanisme audit internal khususnya pada update antivirus.
 52. Perlu membuat kebijakan/prosedur penyampaian laporan adanya penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan serta didokumentasikan sebagai proses pembelajaran pada periode mendatang atau bahan *information sharing and analysis center*.
 53. Perlunya penerapan pengembangan dan uji coba sesuai kriteria keamanan pada seluruh siklus hidup sistem yang telah dibangun.
 54. Perlunya melakukan pengkajian kehandalan keamanan informasi yang dilakukan pihak independen secara rutin dan berkelanjutan sebagai proses peningkatan dan perbaikan proses penerapan SMKI dan keamanan aplikasi.
 55. Perlunya melakukan monitoring secara rutin terhadap lingkungan fisik data center seperti:

- a. Menjaga perimeter keamanan fisik mulai dari saat registrasi sampai dengan melakukan akses ke zona pemeliharaan.
 - b. Kelembaban suhu/udara untuk menjaga kestabilan dan suhu harus relatif merata di setiap sudut ruangan, dapat dilakukan pemasangan termometer dan hidrometer pada beberapa lokasi data center serta pengecekan secara berkala.
 - c. Kestabilan sumber daya listrik dari adanya pemadaman listrik, selain telah memiliki back up yang telah disediakan baik UPS dan genset, perlu mempertimbangkan efektifitas UPS yang bergantung pada kekuatan baterai (perlunya perawatan secara rutin terhadap baterai-baterai yang telah terpasang). Kemudian juga perlu menjaga kapasitas UPS supaya tidak kelebihan beban sehingga dapat memberikan daya dalam waktu yang cukup sebelum sumber daya cadangan beroperasi. Untuk genset, harus dipastikan ketersediaan bahan bakar dalam jumlah yang cukup dan dapat beroperasi dalam jangka waktu beberapa hari dan perlunya melakukan uji coba menghidupkan selama beberapa saat minimal sepekan sekali untuk memastikan kinerja genset tersebut dan perlu melakukan *load test* yang dilakukan minimal setahun sekali.
 - d. Perlunya upaya dari antisipasi kebakaran dengan langkah berupa gladi/simulasi penanggulangan kebakaran yang dapat dilakukan secara berkala terhadap APAR yang dimiliki, dengan juga memastikan *smoke detector* dan alarm data center berfungsi sebagai pendekksi adanya asap/api yang muncul.
56. Perlunya kartu pemeliharaan ruang server dan perangkat lainnya sebagai tahapan monitoring yang dapat dilakukan setiap bulan dengan rutin melakukan pengecekan, perbaikan dan penggantian spare part dan penyesuaian *reliabilitas*.
57. 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, peggunaan 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.
58. Perlu untuk 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.
59. Untuk penilaian periode berikutnya, perlu untuk melakukan penilaian terhadap area suplemen sebagai fondasi dalam peningkatan kinerja keamanan informasi Pemkab Belitung.

Tanjungpandan, 23 Desember 2021

Narasumber Instansi:
Diskominfo Pemkab Belitung

1. Mohammad Iqbal, ST.



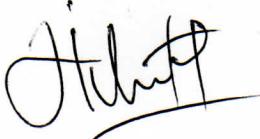
2. Laila Asfiyani, SIP, M.Si.



3. Mohd.Isnaini, S.Sos.



4. Ichsan Zainul Hakim, ST



5. Ikhwanudin, S.Si



Assessor Indeks KAMI:

1. Lead Assessor :

Guruh Prasetyo Putro, S.ST.,M.Si (Han)

2. Assessor :

Diah Sulistyowati, S.Kom.