



LAPORAN ONSITE ASSESSMENT INDEKS KAMI



INDEKS
KEAMANAN
INFORMASI

Instansi/Perusahaan: PEMERINTAH DAERAH KABUPATEN SUMBAWA BARAT	Narasumber Instansi/Perusahaan: 1. Endang Suprihatin, S.Kom. 19790525 200604 2 020 2. Rosihan, S.Kom. 19830623 201001 1 016 3. Rama Fitriansyah 19830710 201001 1 028 4. Dhedet Pratama, S.Kom. 19921103 202012 1 002 5. Tri Fidrian Arya, S.Kom. 19951223 202012 1 001
Unit Kerja: DINAS KOMUNIKASI DAN INFORMATIKA	
Alamat: Jl. Bung Hatta No.5 Komplek KTC Taliwang, Sumbawa Barat, Nusa Tenggara Barat	Tel : (0372) 61223 Fax : (0372) 81765
Email: persandian@sumbawabaratkab.go.id	Pimpinan Unit Kerja: Drs. Burhanuddin, M.M. 19641212 198903 1 028
<p>A. Ruang Lingkup:</p> <p>1. Instansi / Unit Kerja: Layanan Data Center (Ruang Server) dan Sistem Informasi yang dikelola oleh Dinas Komunikasi dan Informatika Kabupaten Sumbawa Barat (Diskominfo KSB).</p> <p>2. Fungsi Kerja: Sebagaimana Peraturan Bupati Sumbawa Barat Nomor 26 Tahun 2017 tentang Rincian Tugas, Fungsi dan Tata Kerja Dinas Komunikasi dan Informatika, Diskominfo KSB memiliki tugas membantu Bupati melaksanakan urusan pemerintahan Daerah di bidang komunikasi dan informatika dan tugas pembantuan yang diberikan kepada Daerah. Dalam menyelenggarakan tugas tersebut, Diskominfo KSB memiliki fungsi sebagai berikut :</p> <ul style="list-style-type: none"> a. Perumusan kebijakan teknis di bidang komunikasi dan informatika; b. Pelaksanaan kebijakan teknis di bidang komunikasi dan informatika; c. Pelaksanaan evaluasi dan pelaporan pelaksanaan tugas di bidang komunikasi dan informatika; d. Pelaksanaan administrasi dinas sesuai dengan lingkup tugasnya; dan e. Pelaksanaan fungsi lain yang diberikan oleh Bupati sesuai dengan tugas dan fungsinya. 	

3. Lokasi:

No	Nama Lokasi	Alamat
1	Diskominfo KSB	Jl. Bung Hatta No.5 Komplek KTC Taliwang, Sumbawa Barat, Nusa Tenggara Barat
2	Ruang Server	Jl. Bung Hatta No.5 Komplek KTC Taliwang, Sumbawa Barat, Nusa Tenggara Barat

B. Nama /Jenis Layanan Publik:

Layanan informasi website sumbawabaratkab.go.id.

C. Aset TI yang kritikal:

1. Informasi:

- Data pegawai Pemerintah KSB
- Data keuangan
- Data konfigurasi sistem

2. Aplikasi:

Total kurang lebih sebanyak 100 aplikasi, beberapa aplikasi utama di antaranya :

- bangjago.sumbawabaratkab.go.id
- ekinerja.sumbawabaratkab.go.id
- bkd.sumbawabaratkab.go.id
- mysimpatda.sumbawabaratkab.go.id
- mysptpd.sumbawabaratkab.go.id
- owncloud.sumbawabaratkab.go.id
- siatanda.sumbawabaratkab.go.id
- simantar.sumbawabaratkab.go.id
- simantar2019.sumbawabaratkab.go.id – Tata ruang.
- simike.sumbawabaratkab.go.id
- simpeg.sumbawabaratkab.go.id
- sister.sumbawabaratkab.go.id
- smartdesa.sumbawabaratkab.go.id
- sumbawabaratkab.go.id

3. Server:

- Server sumbawabaratkab.go.id

4. Infrastruktur Jaringan/Network:

- Telkom (utama) – Asti Net

D. DATA CENTER (DC):

ADA, dalam ruangan khusus (Ruang server dikelola internal)

ADA, jadi satu dengan ruang kerja

TIDAK ADA

Pengelolaan data center/ruang server masih belum terpusat untuk seluruh perangkat daerah di Diskominfo Kabupaten Sumbawa Barat. Berdasarkan hasil observasi/pengamatan ke ruangan data center diperoleh hasil sebagai berikut:

- Ruangan Data Center berada satu Gedung dengan kantor Diskominfo Kabupaten Sumbawa Barat dan berada pada lantai 1. (dengan merujuk pada ketentuan kelayakan lokasi data center dapat menjadi pertimbangan terkait dengan perlunya bangunan khusus yang terpisah dari bangunan gedung lainnya).
- Pengelolaan akses ke data center melewati tiga kunci masuk yaitu pintu utama kantor, pintu ruangan Kepala Bidang dan pintu menuju data center. Kemudian akses menuju data center sudah dilakukan pengamanan kunci secara digital seperti sensor RFID.
- Permitri pengukuran suhu, kelembaban, power/suplai ketersediaan listrik (UPS dan genset), tegangan pada ruangan Data Center masih belum dilakukan pemantauannya secara rutin oleh petugas pengelola Data Center karena belum adanya penerapan monitoring permitri di atas yang dilakukan berkesinambungan oleh operator yang bertugas 24 jam /7 hari).
- Sarana pendukung untuk kondisi kebakaran di dalam Data Center masih belum di akomodir secara komprehensif, karena alat yang digunakan untuk memadamkan api pada Data Center yang kondisinya dipenuhi dengan komputer atau alat elektronik lainnya, membutuhkan alat yang berbeda dengan APAR atau hydrant fire. Tujuannya, ketika terjadi kebakaran, cara mematikan api tidak akan merusak alat elektronik lainnya.
- Belum adanya panduan/aturan/informasi tertulis yang memberikan penjelasan terkait dengan hal yang diperbolehkan/dilarang dilakukan pada ruangan Data Center (misal tidak boleh menggunakan handphone, membuat dokumentasi (foto/video), membawa makanan/minuman, dll).

E. DISASTER RECOVERY CENTER (DRC):

- ADA → Dikelola Internal Dikelola Vendor : Lintasarta
 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		Tdk	-
3	Panduan Klasifikasi Informasi		Tdk	-
4	Kebijakan Manajemen Risiko TIK		Tdk	-
5	Kerangka Kerja Manajemen Kelangsungan Usaha (Business Continuity Management)		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 & Disposal Informasi		Tdk	-
6	Pengelolaan Removable Media & Disposal Media		Tdk	-
7	Pemantauan (Monitoring) 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 Daerah Kabupaten Sumbawa Barat Nomor 11 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah;
2. Peraturan Bupati Sumbawa Barat Nomor 26 Tahun 2017 tentang Rincian Tugas, Fungsi dan Tata Kerja Dinas Komunikasi dan Informatika;
3. Rencana Induk Teknologi Informasi dan Komunikasi (TIK) Tahun 2019-2023;
4. Keputusan Bupati Sumbawa Barat Nomor 188.4.45 1417 Tahun 2021 tentang Implementasi Sistem Informasi Persuratan Elektronik Terpadu Pemerintah KSB "Sister KSB" dan Penggunaan Tanda Tangan Elektronik di Lingkup Pemerintah KSB;

5. Peraturan Bupati Sumbawa Barat Nomor 55 Tahun 2020 tentang Penerapan Tanda Tangan Elektronik Tersertifikasi di Lingkungan Pemerintah KSB;
6. Peraturan Bupati Sumbawa Barat Nomor 14 Tahun 2018 tentang Tata Kelola Teknologi Informasi dan Komunikasi;
7. Keputusan Bupati Sumbawa Barat Nomor 188.4.45 1521 Tahun 2021 tentang Pembentukan dan Penetapan Besaran Belanja Jasa Tim Pendamping *Information Technology* pada Diskominfo KSB Tahun Anggaran 2021;
8. SOP-046/168.1, SOP Layanan Pemulihan Insiden Siber;
9. SOP-046/168.2, Pelayanan Sertifikasi Tandatangan Elektronik;
10. SOP-046/168.3, Pelaksanaan Penetration Testing;
11. SOP-046/168.4, Pelaksanaan Jaming;
12. SOP-046/168.5, Pengiriman Surat melalui Email SANAPATI
13. SOP-046/168.6, Pelaksanaan Pengiriman dan Penyampaian Berita Lainnya Melalui Web Email (SANAPATI);
14. SOP-046/168.7, Pengiriman Surat Sandi/ Klasifikasi Rahasia;
15. SOP-046/168.8, Penerimaan Berita Berklasifikasi Rahasia;
16. SOP-046/168.9, Pembuatan Surat Sandi/ Surat Berklasifikasi Rahasia;
17. SOP-046/168.10, Penyusunan Indeks Keamanan Informasi.

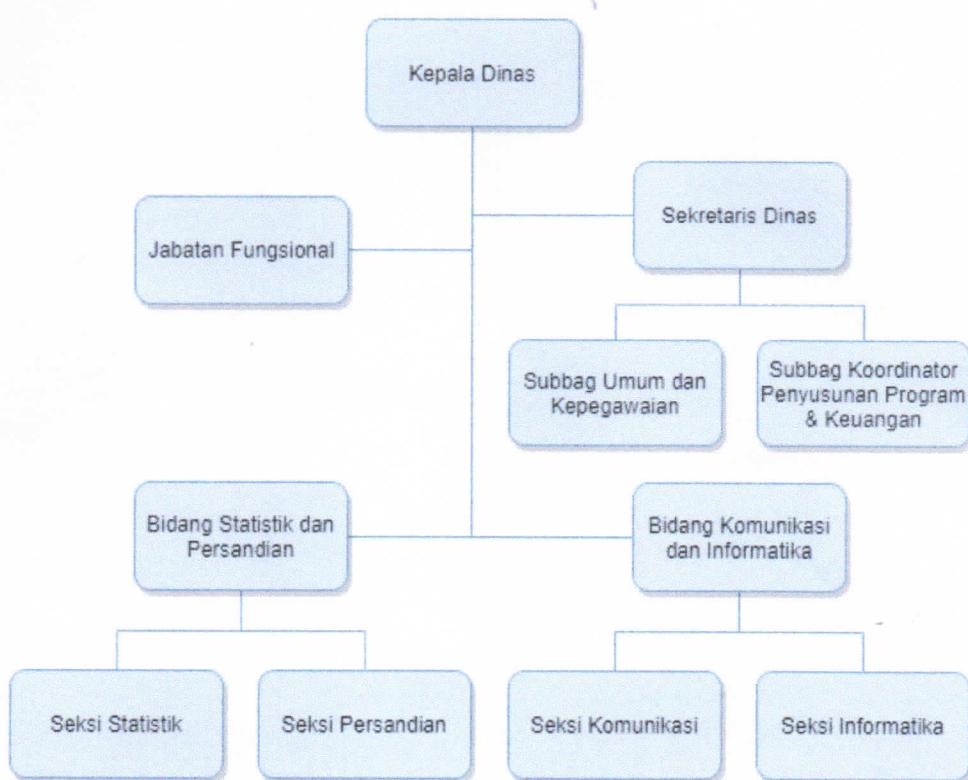
Bukt-bukti (rekaman/arsip) penerapan SMKI:

1. Data Center Diskominfo KSB;
2. Lembar Disposisi output dari aplikasi siMAYA tentang Permohonan URL;
3. Laporan Kegiatan Sosialisasi Keamanan/ Pengamanan Data dan Informasi Tingkat KSB Tahun Anggaran 2017;
4. Berita Acara Permintaan Kronologis Kejadian oleh BSSN tahun 2020;
5. Laporan Pelaksanaan Investigasi dan Forensik Digital terhadap Server Situs <http://emonev.sumbawabaratkab.go.id> yang Terlapor Terjadi Web Defacement;
6. Laporan IT Security Assessment oleh BSSN Tahun 2021;
7. *Screenshoot* Monitoring Server;
8. *Screenshoot* VPN;
9. *Screenshoot* Firewall;
10. *Screenshoot* Antivirus.

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

I. KONDISI UMUM:

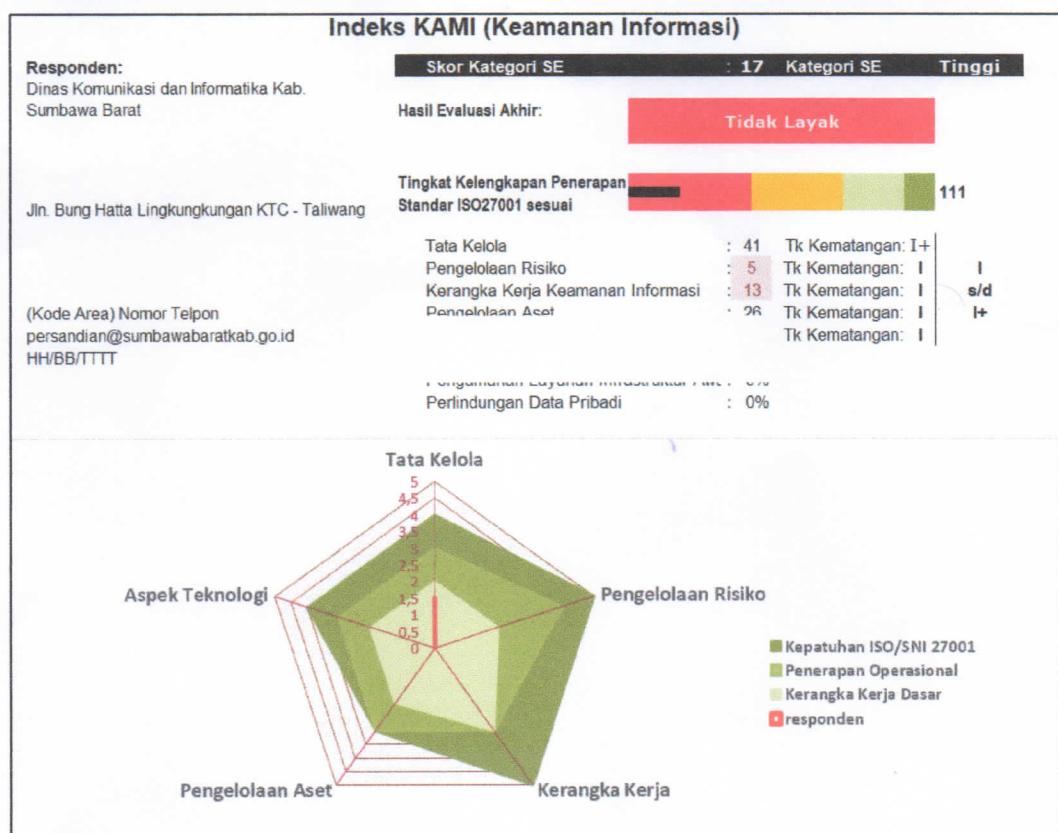
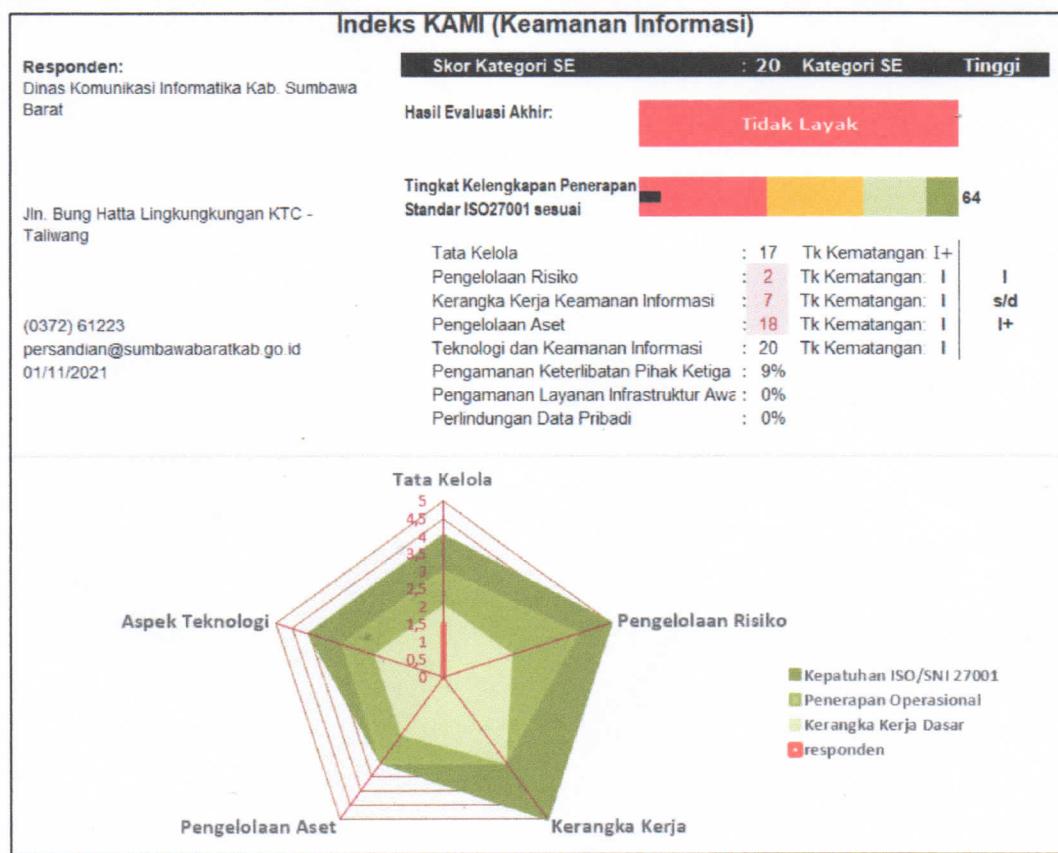
1. Struktur organisasi satuan kerja dalam ruang lingkup Diskominfo KSB dibentuk berdasarkan Peraturan Daerah Kabupaten Sumbawa Barat Nomor 11 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah dan menjalankan tugas dan fungsinya berdasarkan Peraturan Bupati Sumbawa Barat Nomor 26 Tahun 2017 tentang Rincian Tugas, Fungsi dan Tata Kerja Dinas Komunikasi dan Informatika. Adapun struktur Diskominfo KSB adalah sebagai berikut:



2. SDM pengelola terdiri dari:
Jumlah pegawai Diskominfo KSB adalah 19 personil ASN dan 20 personil Non ASN (PTT). Sedangkan jumlah pegawai pada Seksi Persandian sebanyak 4 personil ASN/Non ASN dan pada Seksi Informatika sebanyak 5 personil ASN/Non ASN.
3. Berdasarkan verifikasi terhadap hasil Self Assessment isian file Indeks KAMI diperoleh hasil sebagai berikut:

Tahun 2021 ini Penilaian Mandiri Indeks KAMI dilakukan dengan ruang lingkup Layanan Data Center (Ruang Server) dan Sistem Informasi yang dikelola oleh Dinas Komunikasi dan Informatika Kabupaten Sumbawa Barat (Diskominfo KSB). dengan kategori **TINGGI** dan hasil evaluasi akhir **TIDAK LAYAK** dengan total nilai 64.

Pada tahun 2021 baru kali pertama Diskominfo KSB melakukan penilaian mandiri dan dilakukan verifikasi oleh Tim BSSN, sehingga kegiatan verifikasi difokuskan pada setiap butir pertanyaan, verifikasi data dukung dan mengarahkan mempersiapkan data dukung beserta contohnya untuk meningkatkan penilaian verifikasi di tahun mendatang.

Total Score Sebelum Verifikasi: 111 (ref. file Indeks KAMI pra Verifikasi)**Total Score Setelah Verifikasi: 64 (ref. file Indeks KAMI pasca Verifikasi)**

II. ASPEK TATA KELOLA:

A. Kekuatan/Kematangan

1. Memiliki dasar hukum dalam pelaksanaan tugas dan fungsi organisasi dalam pengamanan informasi yang tertuang pada Perda 11 tahun 2016 dan Perbup 26 Tahun 2017.
2. Memiliki dasar hukum dalam penerapan sertifikat elektronik pada kegiatan pemerintahan yang tertuang pada Kepbup Nomor 188.4.45 1417 Tahun 2021 dan Perbub55 Tahun 2020.
3. Menjadikan aspek keamanan informasi pada sebagian proses kegiatan yang dilakukan, namun belum menjadikan aspek keamanan informasi sebagai bahan pengambilan keputusan pimpinan.
4. Memiliki penanggung jawab pengelolaan keamanan informasi untuk berkoordinasi dengan pihak internal maupun eksternal, meskipun belum terdokumentasi dengan baik dan belum proaktif dalam berkoordinasi.
5. Menjadikan tugas keamanan informasi sebagai penilaian kinerja para pengelola keamanan informasi melalui aplikasi ekinerja.

B. Kelemahan/Kekurangan

1. Fungsi pengamanan informasi di organisasi sudah ada, namun belum melaksanakan tugas dan fungsinya sesuai kewenangannya secara optimal.
2. Belum pernah dilakukan audit internal, hal ini perlu didahului adanya kebijakan audit internal pengamanan informasi, termasuk juga jadwal pelaksanaan (*timeline*) audit.
3. Belum melaksanakan program sosialisasi/ himbauan terkait keamanan informasi, tren serangan siber dan antisipasinya kepada pegawai KSB secara umum dan pegawai Diskominfo secara khususnya.
4. Belum menyusun standar kompetensi dan keahlian serta melakukan program peningkatan kompetensi dan keahlian para pengelola keamanan informasi.
5. Belum memiliki kebijakan dan prosedur dalam pengelolaan dan pengamanan data pribadi.
6. Belum memiliki *Bussiness Contiuunity Plan* (BCP) dan *Disaster Recovery Plan* (BCP).
7. Belum memiliki program kerja yang bertujuan untuk menumbuhkan kedisiplinan pegawai terhadap keamanan informasi, khususnya aset informasi yang menjadi tanggung jawabnya.
8. Belum menyusun laporan yang memuat keamanan informasi di lingkungan organisasi yang berisikan informasi target dan sasaran pengelolaan keamanan informasi serta evaluasinya.
9. Belum memiliki kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum baik pidana maupun perdata.

III. ASPEK RISIKO:

A. Kekuatan/Kematangan

1. Memiliki dokumen Masterplan atau Rencana Induk Teknologi Informasi dan Komunikasi (TIK) tahun 2019-2023 yang didalamnya sudah mencangkap strategi pengelolaan TIK, namun sebagian besar belum diimplementasikan.

B. Kelemahan/Kekurangan

1. Belum memiliki dokumen manajemen risiko, yang didalamnya dapat mencangkap dokumen *risk register* dan *risk treatment plan*.
2. Belum memiliki daftar aset baik fisik maupun non-fisik dan aset informasi sekaligus penanggungjawab, pemiliknya, ancaman dan kelemahan, dampak kerugian, mitigasi risiko dan diurutkan berdasarkan klasifikasinya sesuai dengan dokumen *risk register* yang telah disusun.

3. Belum memiliki prosedur manajemen risiko, misalkan proses ekskalasi pelaporan manajemen risiko, penambahan aset, evaluasinya, dsb.
4. Belum memiliki dokumen manajemen risiko, sehingga belum melakukan analisis/ kajian risiko keamanan informasi pada seluruh aset yang ada sebagai identifikasi langkah mitigasi.
5. Belum melakukan pemantauan terhadap efektifitas manajemen risiko yang telah disusun diselaraskan dengan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang dapat diterima.
6. Belum melakukan pemantauan dan evaluasi langkah mitigasi risiko secara berkala sehingga dapat melakukan pembaruan jika terjadi perubahan pada profil risiko yang dimiliki.
7. Belum melakukan pengkajian ulang terhadap prosedur/ kerangka kerja pengelolaan risiko yang dimiliki secara berkala untuk melihat efektifitas dan meningkatkannya.
8. Belum menggunakan pengelolaan risiko menjadi kriteria proses penilaian kinerja pengamanan yang ada.

IV. ASPEK KERANGKA KERJA:

- A. Kekuatan/Kematangan
1. Memiliki program pengamanan informasi yang dituangkan ke dalam DPA sebagai strategi penerapan keamanan informasi.
 2. Memiliki rencana dan program peningkatan keamanan informasi untuk jangka menengah yang dituangkan ke dalam Renstra Diskominfo KSB dan Rencana Induk TIK 2019-2023, namun belum diimplementasikan dan diterapkan secara konsisten.
 3. Memiliki rencana terkait strategi penerapan keamanan informasi dan penggunaan TI pada Rencana Induk TIK 2019-2023, namun belum diimplementasikan.
 4. Memiliki beberapa SOP terkait keamanan informasi yang tertuang pada SOP-046/168.1 s.d. SOP-046/168.10.
 5. Memiliki prosedur untuk mengidentifikasi yang membahayakan keamanan informasi dan penetapan sebagai insiden keamanan informasi yang tertuang pada SOP-046/168.1.
- B. Kelemahan/Kekurangan
1. Belum memiliki kebijakan tentang Sistem Manajemen Keamanan Informasi (SMKI) yang ditetapkan secara formal dan dipublikasikan.
 2. Belum memiliki prosedur dari turunan kebijakan SMKI.
 3. Belum memiliki prosedur untuk mengelola dokumen kebijakan dan prosedur keamanan informasi serta mengkomunikasikannya kepada seluruh pihak terkait.
 4. Belum memiliki prosedur dengan pihak ketika yang menyatakan di dalam kontrak bahwa aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HKI, tata tertib penggunaan dan pengamanan asset maupun layanan TIK.
 5. Belum memiliki prosedur untuk pelanggaran keamanan informasi.
 6. Belum memiliki kebijakan dan prosedur untuk pengelolaan *security patch*, penanggung jawab monitoring rilis *security patch* baru, implementasi, dan pelaporannya.
 7. Belum memiliki prosedur dan melakukan evaluasi risiko terkait rencana pembelian atau implementasi sistem baru dan mitigasinya.
 8. Belum memiliki kebijakan dan prosedur dalam pengembangan sistem yang aman (Secure SDLC).
 9. Belum memiliki prosedur *compensating control* sebagai akibat adanya risiko baru atau ketidakpatuhan terhadap kebijakan yang ada.
 10. Belum mengimplementasikan BCP dan BCP serta *Disaster Recovery Plan* (DCP).
 11. Belum melakukan evaluasi terhadap seluruh kebijakan dan prosedur keamanan informasi secara berkala.
 12. Belum memiliki prosedur dan melakukan kegiatan audit internal yang dilakukan oleh pihak independen dengan cakupan seluruh aset informasi, kebijakan dan prosedur keamanan yang dimiliki dengan agenda mengevaluasi tingkat kepatuhan, konsistensi

- dan evektifitas penerapan keamanan informasi serta pelaporan hasil audit internal ke pimpinan.
13. Belum melakukan evaluasi terhadap prosedur dan pelaksanaan kegiatan audit internal untuk mengidentifikasi pemberahan dan pencegaran maupun inisiatif peningkatan kinerja keamanan inforamsi.
 14. Belum memiliki prosedur atau kegiatan analisis terhadap rencana revisi kebijakan dan prosedur yang ada untuk menilai aspek finansial (dampak biaya) maupun perubahan infrastruktur dan pengelolaannya sebagai syarat untuk penerapan kebijakan atau prosedur yang baru.
 15. Belum melakukan pengujian dan evaluasi tingkat kepatuhan program keamanan informasi secara periodik untuk memastikan keseluruhan inisiatif dan langkah pemberahannya dilakukan secara efektif.

V. ASPEK PENGELOLAAN ASET:

A. Kekuatan/Kematangan

1. Memiliki daftar asset register (KIB), namun hanya server dan belum seluruh aset masuk ke dalamnya.
2. Sudah menerapkan pengelolaan terhadap sistem, proses bisnis dan proses teknologi informasi, namun belum memiliki prosedurnya.
3. Definisi tanggungjawab pengamanan informasi secara individual untuk seluruh personil Diskominfo KSB telah tertuang di Peraturan Bupati 53/2020, namun belum diimplementasikan secara konsisten.
4. Memiliki prosedur investigasi untuk penyelesaian insiden dan pelaporannya baik kepada pihak eksternal maupun pihak berwajib.
5. Memiliki prosedur (SOP-046/168.7, SOP-046/168.8 dan SOP-046/168.9) dan daftar rekaman keamanan informasi dan bentuk pengamanan sesuai klasifikasinya.
6. Telah menerapkan pengamanan fasilitas fisik sesuai dengan klasifikasi aset informasi (akses kontrol masuk ruang server), namun belum berlapis.
7. Menerapkan sebagian kontrol pengamanan ruang server dengan menerapkan rest floor dan pendingin ruangan (AC).
8. Menggunakan UPS sebagai cadangan listrik ketika terjadi gangguan pasokan listrik, hal ini belum sepenuhnya aman ketika belum menerapkan gardu terpisah, genset dan penangkal petir.
9. Melakukan pencatatan dalam pemindahan aset (form peminjaman dan pengembalian aset), namun belum tertuang ke dalam prosedur yang baku dan dilakukan pengawasan.
10. Memiliki perencanaan dalam dokumen Rencana Induk TIK, untuk perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai, namun belum diimplementasikan.

B. Kelemahan/Kekurangan

1. Belum menerapkan kontrol pengamanan ruang server/ infrastruktur komputasi seperti APAR dan alat pendeteksi suhu.
2. Belum memiliki dokumen yang memuat klasifikasi aset informasi serta prosedur untuk mengevaluasinya.
3. Belum memiliki proses pengelolaan konfigurasi yang diterapkan secara konsisten.
4. Belum memiliki prosedur untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
5. Belum memiliki dan menerapkan kontrol keamanan di antaranya :
 - a. Tata tertib penggunaan komputer, email, internet dan intranet.
 - b. Tata tertib pengamanan dan penggunaan aset instansi terkait HAKI.
 - c. Peraturan terkait instalasi piranti lunak di aset TI milik instansi.
 - d. Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.

- e. Pengelolaan identitas elektronik dan proses otentikasi (*username & password*) termasuk kebijakan terhadap pelanggarannya.
- f. Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi.
- g. Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data.
- h. Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya.
- i. Prosedur back-up dan uji coba pengembalian data (*restore*) secara berkala.
- j. Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya.
- k. Proses pengecekan latar belakang SDM.
- l. Prosedur penghancuran data/aset yang sudah tidak diperlukan.
- m. Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya (*user access rights*) berikut langkah pemberahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku.
- n. Prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
- 6. Belum memiliki daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur *backup*-nya.
- 7. Belum memiliki prosedur pengelolaan alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik.
- 8. Belum memiliki kebijakan pengamanan perangkat komputasi milik instansi ketika digunakan di luar kantor.
- 9. Belum memiliki peraturan untuk inspeksi dan perawatan aset.
- 10. Belum memiliki kebijakan pengamanan dalam pengiriman aset informasi yang melibatkan pihak ketiga.
- 11. Belum memiliki kebijakan untuk pengamanan lokasi kerja yang vital (misalkan ruang server, ruang arsip) dari risiko yang ada.
- 12. Belum memiliki prosedur pengamanan lokasi kerja dari adanya pihak ketiga.

VI. ASPEK TEKNOLOGI:

A. Kekuatan/Kematangan

- 1. Telah mengimplementasikan antivirus, VPN (sebagian kecil untuk pengelola IT), SSL, dan Firewall pada sebagian besar aset pada server yang dikelola.
- 2. Telah melakukan pemindaian untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi, namun belum konsisten dilaksanakan.
- 3. Keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) dan ketersediaan kapasitas yang cukup sesuai kebutuhan/persyaratan yang ada dengan aplikasi yang telah dibangun secara mandiri.
- 4. Telah menerapkan perekaman log pada sistem informasi yang dikelola, namun belum terpusat.
- 5. Telah menerapkan enkripsi (VPN) untuk melindungi aset infomrasi penting, namun belum ada kebijakan yang menjadi dasarnya.
- 6. Telah memiliki kebijakan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, namun belum diimplementasikan.
- 7. Menerapkan pengamanan khusus untuk melindungi akses dari luar instansi menggunakan kartu akses.
- 8. Melakukan pemutakhiran versi terkini pada setiap perangkat server ketika ada rekomendasi dan menerapkan antivirus/ antimalware bundling dengan cpanel (imunify).
- 9. Melibatkan pihak independent untuk mengkaji kehandalan keamanan informasi, namun belum secara konsisten penerapannya.

- B. Kelemahan/Kekurangan
1. Jaringan komunikasi belum terpusat dan disegmentasi sesuai dengan kepentingannya (pembagian instansi, kebutuhan aplikasi, jalur akses khusus, dll).
 2. Belum memiliki konfigurasi standar untuk keamanan sistem bagi keseluruhan asset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan dan kebutuhan serta belum secara rutin menganalisa kepatuhan penerapan konfigurasinya.
 3. Belum memastikan log yang tersimpan memuat pencatatan upaya akses oleh yang tidak berhak.
 4. Belum melalukan analisa secara berkala pada log untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik).
 5. Belum memiliki kebijakan standar dalam penerapan enkripsi untuk melindungi asset informasi penting.
 6. Belum seluruh sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama, serta pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses.
 7. Belum menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi.
 8. Belum memiliki catatan atau rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis.
 9. Belum memiliki laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan.
 10. Belum memastikan keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada.
 11. Pada proses pengembangan dan uji coba aplikasi, belum melakukan verifikasi terhadap spesifikasi dan fungsi keamanan.
 12. Belum menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun.

VIII. REKOMENDASI

1. Menyusun, mengesahkan, mengimplementasikan, dan mengevaluasi kebijakan Sistem Manajemen Keamanan Informasi (SMKI) dan turunannya, dengan mengimplementasikan SMKI ini akan sangat membantu dalam peningkatan Keamanan Informasi di lingkungan Diskominfo KSB dan secara linier meningkatkan nilai Indeks KAMI Diskominfo KSB.
2. Menyusun dan secara rutin memperbarui Daftar Induk Dokumen (DID), untuk membantu dalam pengelolaan/ inventarisasi kebijakan, pedoman, juknis, SOP dan sebagainya.
3. Melaksanakan secara maksimal kebijakan-kebijakan yang telah disusun, di antaranya Keputusan Bupati Nomor 188.4.45 1417 Tahun 2021, Perbub Nomor 55 Tahun 2020 dan Nomor 14 Tahun 2018, serta Rencana Induk TIK 2019-2023.
4. Melaksanakan dan mendokumentasikan tugas dan fungsi pengamanan informasi sesuai dengan kewenangannya.
5. Menyusun kebijakan dan prosedur, mengimplementasikan, melaporkan dan mengevaluasi pelaksanaan audit internal keamanan informasi secara terjadwal.
6. Menyusun, melaksanakan, melaporkan dan mengevaluasi program sosialisasi/ himbauan terhadap keamanan infomrasi secara konsisten dan berkelanjutan, karena perkembangan kerawanan dan ancaman terhadap keamanan informasi terus berkembang. Dapat dilakukan secara offline maupun menggunakan media sosial yang interaktif dan menarik sehingga kebutuhan update keamanan informasi menjadi suatu hal yang penting dan ditunggu oleh seluruh pengguna keamanan informasi di KSB.
7. Melaksanakan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi sesuai dengan standar kompetensi yang

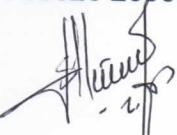
disusun bagi pengelola keamanan informasi. Hal ini dapat ditunjukkan melalui kesesuaian/keselarasan jumlah personil dimana kompetensi dan keahlian yang telah sesuai dengan kebutuhan yang telah dituangkan dalam dokumen gap analisis kebutuhan kualifikasi SDM pengelola keamanan informasi. (kesesuaian peningkatan kualitas SDM mengacu pada dokumen analisis jabatan).

8. Menyusun dan melaksanakan *Business Continuity Plan* dan *Disaster Recovery Plan* (DRP) sebagai upaya dalam menjaga kelangsungan TIK dan menjadi bagian rencana tindakan (*response plan*) dalam mengantisipasi terjadinya bencana. Dalam penyusunannya, DRP memerlukan beberapa proses seperti pencatatan seluruh aset (layanan TI) yang dimiliki oleh organisasi, pencatatan risiko-risiko negatif yang berpotensi menjadi sebuah bencana bagi organisasi, serta analisis dampak bisnis sebagai pertimbangan keputusan dalam penyusunan dokumen DRP. Selanjutnya DRP akan menjadi panduan yang dipersiapkan Diskominfo KSB dalam menghadapi bencana sehingga proses bisnis/layanan tetap dilanjutkan dan dapat menjaga konsistensi data apabila akibat bencana berdampak pada gangguan maupun kerusakan terhadap layanan teknologi informasi.
9. Meningkatkan kerjasama secara proaktif baik secara internal SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak. Penerapan akan kepatuhan akan dapat diimplementasikan saat kebijakan terkait keamanan informasi telah ditetapkan, disosialisasikan dan dievaluasi penerapan dari uraian kebijakan di dalamnya.
10. Menyusun identifikasi data pribadi yang digunakan dalam proses kerja dan penerapan pengamanan pada tiap aplikasi yang dikelola oleh Diskominfo KSB sesuai dengan peraturan perundungan yang berlaku dengan merujuk pada Perkominfo 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik dan referensi hukum lainnya terkait dengan data pribadi.
11. Menyusun pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanannya, pemantauannya dan eskalasi pelaporannya. Hal ini dapat dituangkan dalam kerta kerja pengukuran penerapan kebijakan keamanan informasi yang selanjutnya dapat diintegrasikan dengan pengukuran kinerja organisasi sehingga pemantauannya dilakukan secara periodik dan berkesinambungan untuk menjaga proses pengelolaan keamanan informasi telah berjalan sesuai dengan periode waktu dan target yang telah ditetapkan dalam kebijakan maupun sesuai dengan arahan pimpinan pengelola keamanan informasi.
12. Menyusun kebijakan/prosedur yang mendefinisikan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata). Dokumen tersebut berisikan definisi dan langkah-langkah penanganan yang harus dilakukan dalam mengantisipasi adanya gangguan dan insiden keamanan informasi dengan mengklasifikasikan jenis pelanggaran hukum terkait.
13. Menyusun dokumen *risk register* dan *risk treatment plan* yang memuat seluruh aset yang dimiliki terkait penyelenggaraan keamanan informasi. Dalam kerangka kerja pengelolaan risiko, pada dokumen *risk register* yang akan disusun memuat identifikasi risiko per aset yang dimiliki dan mitigasinya. Ditambahkan juga dengan kepemilikan dan pihak pengelola (*custodian*) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
14. Melakukan pemantauan dan evaluasi langkah mitigasi risiko secara berkala sehingga dapat melakukan pembaruan jika terjadi perubahan pada profil risiko yang dimiliki, kemudian melakukan pengkajian ulang atau profil risiko dan kerangka kerja pengelolaan risiko untuk meningkatkan efektivitasnya.
15. Perlu melakukan identifikasi kebijakan dan prosedur yang menjadi turunan kebijakan keamanan informasi dan melakukan sosialisasi secara kontinu dan berkelanjutan baik pihak internal maupun eksternal yang terkait dengan pengelolaan sistem elektronik.
16. Perlu membuat mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya yang berupa SOP pengelolaan dokumen.

17. Menyediakan proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga.
18. Melakukan penyusunan prosedur penanganan insiden yang spesifik, misalnya insiden *web defacement*, *ransomware*, *illegal access*, dan lainnya untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkannya sebagai insiden keamanan informasi untuk selanjutnya ditindaklanjuti.
19. Dalam kebijakan SMKI perlu dicantumkan konsekuensi dari pelanggaran kebijakan keamanan informasi, dikomunikasikan dan ditegakkan, baik di internal maupun eksternal Diskominfo KSB.
20. Penyusunan kebijakan dan prosedur operasional dapat berupa SOP pengelolaan *patch* untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, hingga memastikan pemasangan dan melaporkannya.
21. Menyusun kebijakan dan prosedur untuk menerapkan proses pengembangan sistem yang aman (*Secure SDLC*) dengan menggunakan prinsip atau metode sesuai standar platform teknologi.
22. Melakukan evaluasi kelayakan secara berkala pada seluruh kebijakan dan prosedur keamanan informasi .
23. Melakukan penjadwalan kegiatan audit internal terhadap kebijakan implementasi SMKI setelah ditetapkan kebijakan tersebut secara resmi sebagai salah satu bentuk kepatuhan terhadap penerapannya.
24. Menyusun strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi, dapat dituangkan berupa telaah staf atau kertas kerja penerapan SMKI.
25. Melakukan evaluasi terhadap program audit internal, antara lain mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi dan disusun laporan dari evaluasi tersebut.
26. Membuat laporan analisa dalam merevisi kebijakan dan prosedur yang berlaku untuk menilai aspek finansial (dampak biaya) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya sebagai syarat untuk penerapan kebijakan atau prosedur yang baru.
27. Menerapkan kontrol keamanan pada ruang server/ infrastruktur komputasi, misalnya adanya penyekatan ruangan antara ruang server dan ruang kerja pengelolaan server, APAR, CCTV, alat pengukur suhu, dan lain sebagainya sebagai kontrol keamanan.
28. Penyusunan kebijakan/prosedur berupa SOP manajemen aset untuk mendefinisikan klasifikasi aset informasi. Begitu pula evaluasinya sesuai tingkat kepentingan aset bagi instansi dan keperluan pengamanannya yang berupa laporan evaluasi yang secara umum dapat dicantumkan di kebijakan SMKI.
29. Menyusun kebijakan SOP pengelolaan konfigurasi dan SOP manajemen perubahan untuk mengelola perubahan terhadap sistem, proses bisnis dan proses teknologi informasi serta proses pengelolaan konfigurasi yang diterapkan secara konsisten.
30. Mengidentifikasi keseluruhan aset yang dimiliki baik aset informasi pada sistem elektronik maupun aset lainnya berdasarkan kategori yang berkaitan dengan pengelolaan sistem elektronik.
31. Mendefinisikan tingkatan hak akses sesuai dengan klasifikasi sistem elektronik yang dikelola.
32. Melakukan dokumentasi terhadap adanya pengelolaan maupun perubahan konfigurasi sistem elektronik.
33. Membuat prosedur rilis aplikasi yang perlu dituangkan dalam SOP manajemen rilis aplikasi dengan tujuan untuk menyediakan aplikasi yang sesuai dengan spesifikasi tingkat akurasi yang telah ditetapkan dan menjamin *quality assurance* terhadap aplikasi yang akan naik ke *production*.
34. Menyusun tata tertib pengamanan dan penggunaan aset yang di dalamnya tertuang penggunaan komputer, email, internet dan intranet, peraturan HAKI serta instalasi piranti lunak di aset TI.
35. Menyusun peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi yang tertuang dalam dokumen berita acara.

36. Menyusun kebijakan/prosedur pengelolaan identitas elektronik dan proses otentifikasi (*username & password*), termasuk kebijakan terhadap pelanggarannya. Selain itu, juga menyusun prosedur pengelolaan/pemberian akses, otentifikasi dan otorisasi untuk menggunakan aset informasi.
37. Perlu menyusun dokumentasi riwayat pemeliharaan terhadap aset yang berkaitan dengan pengelolaan sistem elektronik.
38. Menyusun kebijakan terkait dengan standar aplikasi sistem elektronik yang akan membantu dalam melakukan pengawasan dan pemberian izin ke perangkat daerah saat akan menggunakan atau akan mengembangkan aplikasi sistem elektronik.
39. Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data yang sudah tidak diperlukan perlu disusun kebijakannya yang dapat ditambahkan dalam kebijakan SMKI dan dibuatkan turunan berupa prosedur dari kebijakan tersebut.
40. Menyusun kebijakan pengamanan perangkat komputasi milik instansi ketika digunakan di luar kantor.
41. Menyusun prosedur terkait penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi serta pelaporan insiden tersebut kepada pihak eksternal ataupun pihak yang berwajib.
42. Membuat prosedur dalam pengecekan latar belakang SDM dan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.
43. Menyusun prosedur terkait daftar data/informasi yang harus *di-backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya, secara dapat dimasukkan di kebijakan SMKI atau menjadi kebijakan teknis terpisah yang tertuaang dalam prosedur bagian dari kebijakan keamanan informasi.
44. Menyusun prosedur dalam memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris).
45. Memusatkan jaringan komunikasi di Diskominfo KSB dan melakukan segmentasi sesuai dengan kepentingannya (pembagian instansi, kebutuhan aplikasi, jalur akses khusus, dll).
46. Menyusun konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan dan kebutuhan serta belum secara rutin menganalisa kepatuhan penerapan konfigurasinya.
47. Mengimplementasikan *Security Information and Event Management* (SIEM) yang dapat berfungsi sebagai analisis keamanan, pendekripsi gangguan, analisis data log, pemantauan integritas file, pendekripsi kerentanan, penilaian konfigurasi, membantu dalam tanggap insiden, kepatuhan terhadap kebijakan, pemantauan keamanan *cloud*.
48. Menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi, misalnya membuat SSID yang tersegmentasi khusus bagi pengunjung atau pihak ketiga.
49. Melakukan penerapan pengamanan fisik pada lingkungan data center dengan mekanisme pengamanan kunci digital seperti fingerprint, biometrik atau sensor RFID, serta diimbangi dengan adanya kebijakan/prosedur-nya.
50. Melakukan pemindaian terhadap sistem elektronik yang meliputi jaringan, sistem dan seluruh aplikasi yang dimiliki secara berkala.
51. Melakukan pemasangan antivirus dan antimalware pada sistem elektronik yang dimiliki dan dikelola.
52. Memastikan keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada.
53. Menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun
54. Mencantumkan standar dalam menggunakan enkripsi (penerapan kriptografi) di kebijakan SMKI, serta membuat dokumen turunan dari kebijakan tersebut.
55. Semua sistem dan aplikasi menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama. Pengaturan tersebut disarankan untuk dituangkan dalam prosedur penggunaan *password*.

56. Penentuan lokasi data center sesuai standar TIA 942 mensyaratkan bahwa lokasi harus dapat disesuaikan dengan kebutuhan sekarang dan dapat dikembangkan (*expandable*). Data center dapat menempati satu ruangan dari sebuah bangunan, satu atau lebih lantai, atau seluruh bangunan. Pertimbangan lokasi menjadi syarat terpenting pertama yang harus dipenuhi dalam mengantisipasi kebutuhan IT yang selalu meningkat, terutama pertambahan hardware. Dalam Standar TIA 942 dipersyaratkan bahwa lokasi data center harus bebas dari interferensi peralatan elektronik yang dapat menimbulkan gangguan elektromagnetis. Pengembangan data center/ ruang server Diskominfo KSB diharapkan dapat menyesuaikan dan memperhatikan standar pengelolaan dan syarat ruang data center sesuai yang tercantum dalam pedoman teknis yang telah ditetapkan.
57. Sistem pendingin ruangan pada Data Center memiliki fungsi dan peran khusus sebagai *thermal management* bagi perangkat IT dan server agar tidak terjadi *overheating* pada perangkat yang berada di dalamnya, maka perlu pendingin khusus seperti Precision Air Conditioning (PAC) yang akan membantu menstabilkan suhu/temperature dan kelembaban (*relatif humidity*) secara konstan dan akan mempertahankan suhu dan kelembaban yang telah disesuaikan sesuai dengan kebutuhan perangkat komputer di dalam ruangan tersebut.
58. Dengan merujuk pada standar TIA-942, maka topologi standar data center yang dipersyaratkan setidaknya memiliki 4 komponen utama yang perlu diperhatikan, yaitu jalur akses (pintu utama), ruang telekomunikasi, ruangan utama dan beberapa ruangan distribusi atau ruangan operasional. Dengan memperhatikan keempat komponen utama tersebut, maka diharapkan pengelolaan data center menjadi lebih murah, mudah untuk digunakan, dipelihara dan diperluas. Filosofi dasar pembuatan data center terkait erat dengan 5 prinsip dimana desain data center harus sederhana (*simplicity*), desain data center memiliki ukuran yang relatif (*scalability*), desainnya harus bersifat modular (*modularity*) dan fleksibel (*flexibility*) dan mampu menunjang kebutuhan penggunaan jangka panjang sehingga diperlukan ruang kerja yang nyaman dan aman (*sanity*).

<p>Sumbawa Barat, 14 Desember 2021</p> <p>Narasumber Instansi/Perusahaan:</p> <p>Dinas Komunikasi dan Informatika Kabupaten Sumbawa Barat</p> <p>1. Endang Suprihatin, S.Kom. 19790525 200604 2 020</p>  <p>2. Rosihan, S.Kom. 19830623 201001 1 016</p>  <p>3. Rama Fitriansyah 19830710 201001 1 028</p>  <p>4. Dhedet Pratama, S.Kom. 19921103 202012 1 002</p>  <p>5. Tri Fidrian Arya, S.Kom. 19951223 202012 1 001</p> 	<p>Sumbawa Barat, 14 Desember 2021</p> <p>Asessor Indeks KAMI:</p> <p>1. Asesor Utama: Ivan Bashofi, S.S.T.TP.</p> <p>2. Assesor Pendamping: Mochamad Jazuly, S.S.T.TP.</p>
---	---