



# LAPORAN ONSITE ASSESSMENT INDEKS KAMI



INDEKS  
KEAMANAN  
INFORMASI

**Instansi/Perusahaan:**  
Pemerintah Kabupaten Sumedang

**Unit Kerja:**  
Dinas Komunikasi, Informatika, Persandian,  
dan Statistik (Diskominfosanditik)

**Alamat:**  
Jl. Angrek No. 103 Sumedang  
45323

**Email:**  
diskominfosanditik@sumedangkab.go.id

**Narasumber Instansi/Perusahaan:**

1. Mamat Rohimat, S.Pd., M.Pd
2. Agus Ramdan Sutarsa, S.Sos
3. Hendri Wiguna, S.Kom
4. Roza Hidayat, S.Kom
5. Alfan Fathurohman, S.T
6. Yadi Apriyadi
7. Musni

**Tel:** (0261) 201255

**Pimpinan Unit Kerja:**

Kepala Dinas Komunikasi, Informatika,  
Persandian, dan Statistik (Diskominfosanditik)

## A. Ruang Lingkup:

Pengelolaan Data Center dan Aplikasi Sistem informasi Kabupaten Sumedang

1. Instansi / Unit Kerja:  
Dinas Komunikasi, Informatika, Persandian, dan Statistik Kabupaten Sumedang.

### 2. Fungsi Kerja:

Sebagaimana Peraturan Bupati Nomor 38 Tahun 2016 Tentang Kedudukan, Susunan Organisasi, Tugas, Fungsi dan Tata Kerja Perangkat Daerah Kabupaten Sumedang, Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang mempunyai tugas melaksanakan Urusan Pemerintahan yang menjadi kewenangan Daerah dalam rangka pelaksanaan sebagian tugas Bupati di bidang komunikasi, informatika, persandian dan statistik. Dalam menyelenggarakan tugas pokok diatas, Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang memiliki fungsi sebagai berikut:

- a. Perumusan kebijakan bidang komunikasi, bidang informatika, bidang persandian dan bidang statistik;
- b. Pelaksanaan kebijakan bidang komunikasi, informatika, persandian dan statistik;
- c. Pelaksanaan evaluasi dan pelaporan bidang komunikasi, informatika, persandian dan statistik;
- d. Pelaksanaan administrasi dinas bidang komunikasi, informatika, persandian dan statistik; dan
- e. Pelaksanaan fungsi lain yang diberikan oleh Bupati sesuai dengan tugas dan fungsinya.

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor Pusat	Jl. Angkrek No. 103 Kel. Situ Kec. Sumedang Utara
2	Data Center	Jl. Angkrek No. 103 Kel. Situ Kec. Sumedang Utara (Kantor Diskominfosanditik Kab. Sumedang)
3	Command Center	JL Prabu Gajah Agung, RT 4 RW 2, Situ, Kec. Sumedang Utara, Lantai 3
4	Disaster Recovery Center (DRC)	Kerjasama dengan Kementerian Komunikasi dan Informatika dengan lokus berada di Jakarta (hanya LPSE)

B. Nama /Jenis Layanan Publik:

Layanan Infrastruktur Data Center (NOC, Jaringan, Server) dan Aplikasi Sistem informasi (e-office ASN, e-Office Desa, SIMPEG) yang dikelola oleh Diskominfosanditik Kab Sumedang.

C. Aset TI yang kritikal:

1. Informasi:
  - Identitas ASN Pemerintah Kabupaten Sumedang
  - Identitas Pegawai Desa di Kabupaten Sumedang
  - Identitas Masyarakat Kabupaten Sumedang
2. Aplikasi Utama
  - e-office ASN : [www.e-office.sumedangkab.go.id](http://www.e-office.sumedangkab.go.id)
  - e-office Desa : [e-desa.sumedangkab.go.id](http://e-desa.sumedangkab.go.id)
  - sistem kepegawaian : [simpeg.sumedangkab.go.id](http://simpeg.sumedangkab.go.id)

D. DATA CENTER (DC):

ADA, pengelolaan data center/ruang server seluruh perangkat daerah telah terpusat di Diskominfosanditik Kabupaten Sumedang. Pembangunan data Center Diskominfosanditik Kabupaten Sumedang merujuk pada ketentuan Rencana Induk Pengembangan Teknologi Informasi Komunikasi dengan mengacu pada desain standar *Telecommunications Industry Association (TIA-942)*.

Berdasarkan hasil observasi/pengamatan ke ruangan data center diperoleh hasil sebagai berikut:

- Ruangan Data Center berada satu Gedung dengan kantor Diskominfosanditik Kabupaten Sumedang dan berada pada lantai 1. (dengan merujuk pada ketentuan kelayakan lokasi data center dapat menjadi pertimbangan terkait perlunya bangunan khusus yang terpisah dari bangunan gedung lainnya).
- Pengelolaan akses ke data center melewati tiga kunci masuk yaitu pintu utama kantor, pintu ruangan monitoring dan pintu menuju data center. Namun akses menuju data center masih dilakukan secara fisik (belum menerapkan pengamanan kunci digital seperti *fingerprint* atau sensor RFID).

- Permitri pengukuran suhu, kelembaban, power/suplai ketersediaan listrik (UPS dan genset), tegangan pada ruangan Data Center telah dilakukan pemantauannya secara rutin dan manual oleh petugas pengelola Data Center namun durasi waktu pengawasannya terbatas pada jam operasional kantor (belum adanya penerapan monitoring perimitri di atas yang dilakukan berkesinambungan oleh operator yang bertugas 24 jam/7 hari).
- Peralatan keamanan monitoring fisik yaitu CCTV pada Data Center telah berjalan dengan baik dan recorder CCTV disimpan dalam periode jangka waktu dua bulan. Salah satu perangkat CCTV terpasang di luar ruangan Data Center dengan tujuan adalah untuk memberikan informasi aktivitas keluar masuk personil.
- Sistem utilitas penangkal petir telah ada namun dalam mencegah adanya bahaya petir maka perlu dilakukan monitoringnya secara rutin, dilakukan secara tertulis sebagai bukti dalam pemeliharaan. Selain itu perlu ditentukan PIC (penanggung jawab pengelolaan *grounding* data center)
- Sarana pendukung untuk kondisi kebakaran di dalam Data Center sudah di akomodir dengan menggunakan APAR sebanyak 1 (satu) unit. Untuk memastikan APAR berfungsi saat terjadi insiden kebakaran maka perlu monitoring dan pengujian secara rutin dan berkelanjutan.
- 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):**

- 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.
- Berdasarkan layanan pengelolaan TIK pada Kabupaten Sumedang jangkauannya telah sampai dengan seluruh Perangkat Daerah dan sampai dengan Desa dan mengingat saat ini serangan siber semakin meningkat, maka terhentinya layanan apabila terjadi serangan menjadi downtime yang dapat mengakibatkan reputasi dan dampak negatif bagi Kabupaten Sumedang. Perlunya mempertimbangkan kemampuan melakukan *fail-over* dan *fail-back* dengan durasi toleransi waktu yang ditentukan dapat menjadi salah satu dasar dalam pentingnya penggunaan hosting DRC bagi Kabupaten Sumedang untuk seluruh layanan TIK yang telah dimiliki sebagai proses pemulihan adanya bencana dari konsisi darurat.
- Perlunya penjajakan kembali terhadap rencana kerjasama dengan Kementerian Komunikasi dan Informatika dalam penyediaan DRC baik dalam bentuk fisik maupun virtual (cloud) sebagai upaya dalam menjaga keberlangsungan layanan TIK di Kabupaten Sumedang.

**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"> <li>• Definisi, sasaran dan ruang lingkup keamanan informasi</li> <li>• Persetujuan terhadap kebijakan dan program keamanan informasi</li> <li>• Kerangka kerja penetapan sasaran kontrol dan kontrol</li> <li>• Struktur dan metodologi manajemen risiko</li> <li>• Organisasi dan tanggungjawab keamanan informasi</li> </ul>	Ada (draft)
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/k 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).	Tidak
---	--------------------------------------	---	-------

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	Tidak
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	Tidak
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	Tidak
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)	Tidak
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.	Tidak
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	Tidak
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.	Tidak

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.	Tidak
----	--	--	-------

**Dokumen yang diperiksa:**

1. Peraturan Bupati Sumedang Nomor 17 Tahun 2017 tentang Uraian Tugas Jabatan Struktural pada Dinas Komunikasi dan Informatika, Persandian dan Statistik.
2. Rencana Kerja Tahun 2020 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.
3. Peraturan Bupati Sumedang Nomor 39 Tahun 2019 tentang Rencana Strategis Dinas Komunikasi, Informatika, Persandian, dan Statistik Kabupaten Sumedang Tahun 2018 – 2023.
4. Peraturan Bupati Sumedang Nomor 45 Tahun 2017 tentang Peraturan Pelaksanaan Peraturan Daerah Nomor 6 Tahun 2015 tentang Penyelenggaraan Administrasi Kependudukan.
5. Peraturan Bupati Sumedang Nomor 50 Tahun 2021 tentang Manajemen SPBE dan Audit TIK.
6. Peraturan Bupati Sumedang Nomor 89 Tahun 2020 tentang Pemanfaatan Sertifikat Elektronik.
7. Draf Peraturan Bupati Sumedang tentang Sistem Manajemen Keamanan Informasi.
8. Rencana Induk Pengembangan E-Government Kabupaten Sumedang 2016 – 2020.
9. DPA Bidang Persandian.
10. Surat Edaran 046/2310/DISKIPAS tanggal 15 April 2020 tentang Penetration Testing (Pentest) bagi SKPD yang memiliki aplikasi.
11. Surat Perintah Tugas Nomor KP.11.01/3291/2021 tanggal 20 Mei 2021 tentang Tim Auditor dan Auditee Aplikasi.
12. Surat Perintah Tugas Nomor KP.11.01/3290/2021 tanggal 20 Mei 2021 tentang Tim Auditor dan Auditee Jaringan.
13. Dokumen Analisis Jabatan Bidang Persandian.
14. Pakta Integritas Manajemen Risiko SPBE.
15. Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP) Data Center.
16. SOP Pelaksanaan Pendaftaran Sertifikat Elektronik.
17. SOP Pelaksanaan Pengubahan Data Sertifikat Elektronik.
18. SOP Pengembangan/ Pembuatan Sistem/Aplikasi.
19. SOP Pengawasan dan Pengendalian Data Center.
20. Pedoman Teknis Pengelolaan dan Syarat Ruang Data Center/ Ruang Server Terpusat.
21. 046/27/Bidang Persandian tentang Nota Dinas perihal Laporan Hasil Kegiatan P12 dan Evaluasi SE di Kecamatan Jatigede.
22. Surat Pengantar Nomor B/407/PL.08/V/2021 tentang Penyampaian Daftar Aset TIK dari Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang Tahun 2021.
23. Kartu Inventaris Barang (KIB).
24. SPK Nomor 05/SPK/FIREWALL/DISKOMINFOSANDITIK/2021 tanggal 22 Februari 2021 perihal Belanja Lisensi Firewall.
25. Surat Perjanjian Nomor 01/ISB/P2102-3676164/DISKOMINFOSANDITIK/2021 tanggal 19 April 2021 perihal Belanja Internet SKPD.
26. TEL/BASO/TK.000/R3W-3F460000/2021 tentang Berita Acara Siap Operasi Penggunaan Layanan Monitoring Wifi Station Diskominfosanditik Kabupaten Sumedang 2021.
27. SPK Nomor K.TEL/HK.820/R3W-3F460000/2021 tanggal 4 Januari 2021 perihal Layanan Monitoring Wifi Diskominfosanditik Kabupaten Sumedang 2021.
28. Sertifikat Pelatihan

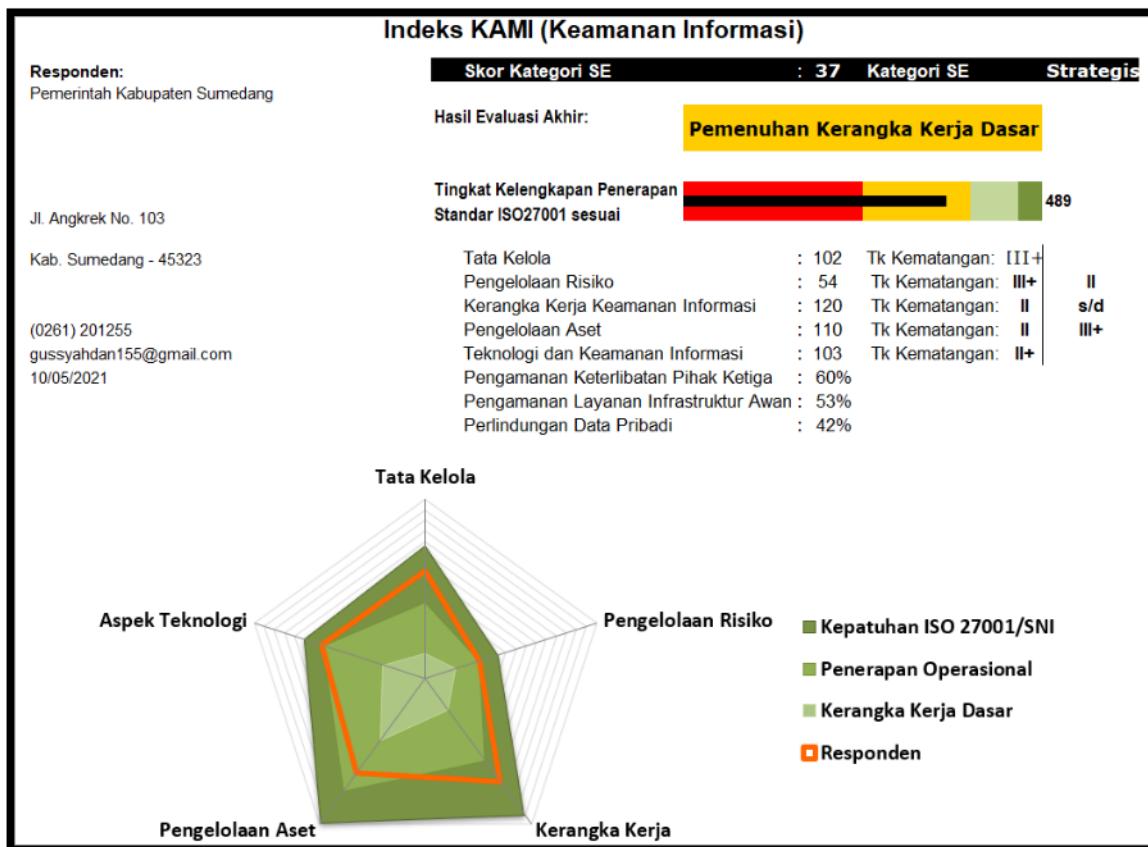
29. Perjanjian Kerahasiaan Penetration Testing (Pentest)
30. Laporan Penetration Test.
31. Laporan Tindak Lanjut Hasil Penetration Test.
32. Laporan Audit Aplikasi.
33. Laporan Audit Infrastruktur Tata Kelola Manajemen Kabupaten Sumedang.
34. Permohonan Kabupaten Sumedang untuk VPS Layanan Pusat Data Nasional Sementara (Government Cloud).
35. Berita Acara Serah Terima Hibah Smartphone.
36. Data user accountOpenVPN Diskominfosanditik Kabupaten Sumedang.
37. Notula Backup Pusat Data Pemerintah Daerah Kabupaten Sumedang.
38. Aplikasi SILPA, aplikasi e-office ASN, aplikasi e-office Desa, SIMPEG.
39. Screenshot Command Center, CCTV Diskominfosanditik Kabupaten Sumedang, penangkal petir, Data Center.
40. Screenshot Firewall, ModSecurity, monitoring traffic router SKPD, MRTG OPD, server customer dan kapasitas, log server.
41. Tingkat kematangan layanan jaringan intra instansi pusat/pemerintah daerah lingkup Pemkab Sumedang.
42. Perjanjian Kerja Dinas Komunikasi, Informatika, Persandian, dan Statistik Kabupaten Sumedang.
43. Capture Rencana Induk Pengembangan e-Government Kabupaten Sumedang 2021-2025

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

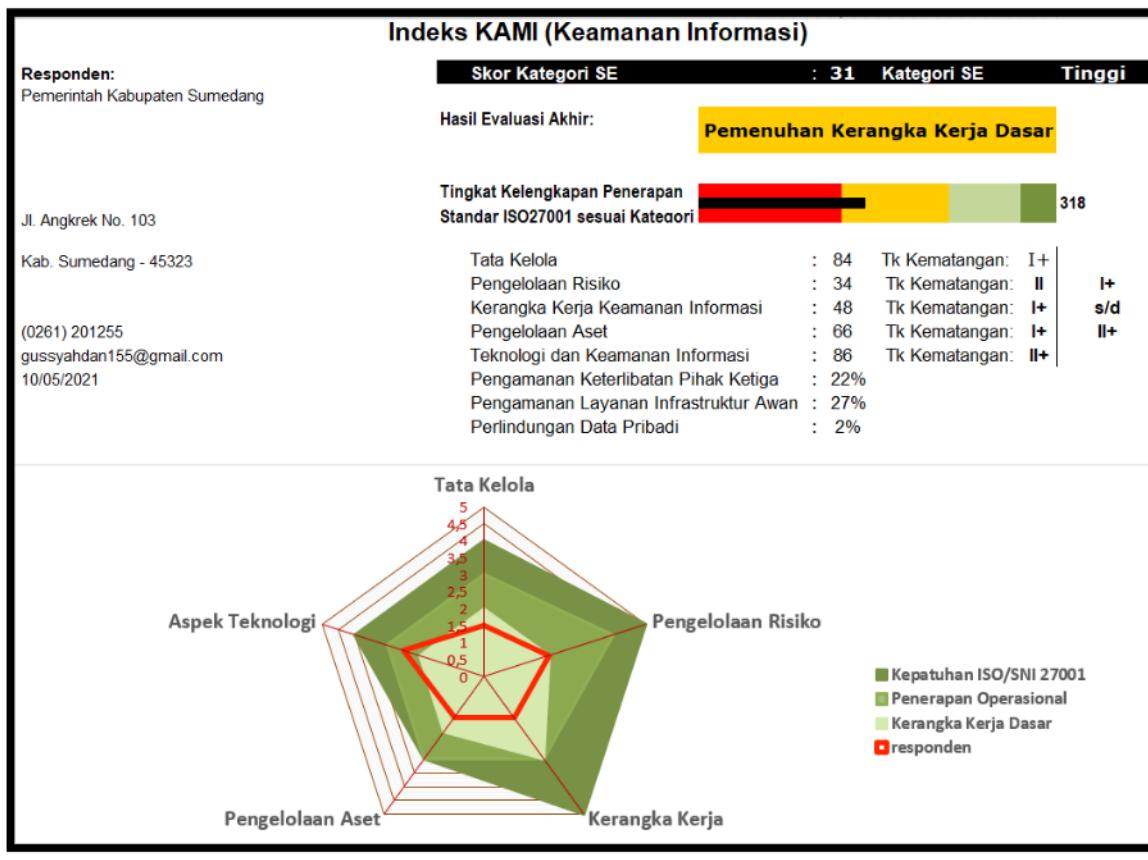
#### **I. KONDISI UMUM:**

1. Struktur organisasi satuan kerja dalam ruang lingkup berada di bawah Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang terdiri atas:
  - a. Bidang Komunikasi
  - b. Bidang Informatika
  - c. Bidang Persandian
  - d. Bidang Statistik
2. SDM pengelola terdiri dari:  
Jumlah pegawai di Diskominfosanditik Kabupaten Sumedang adalah 80 personil ASN dan non ASN.
3. Berdasarkan verifikasi terhadap hasil Self Assessment instrumen Indeks KAMI versi 4.2 diperoleh hasil sebagai berikut:

**Total Score Sebelum Verifikasi: 489 (ref. Instrumen Indeks KAMI pra Verifikasi)**



**Total Score Setelah Verifikasi: 318 (ref. Instrumen Indeks KAMI pasca Verifikasi)**



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

### a. Kekuatan/Kematangan

1. Pimpinan dari Diskominfosanditik Kabupaten Sumedang sudah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen diantaranya sudah ada penetapan kebijakan keamanan informasi melalui Renstra dan Peraturan Bupati Sumedang.
2. Tanggungjawab pengelolaan keamanan informasi telah mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasi persyaratan/kebutuhan pengamanan.
3. Kondisi dan permasalahan keamanan informasi yang ada sudah menjadi bagian dalam proses pengambilan keputusan strategis di Diskominfosanditik Kabupaten Sumedang.
4. Diskominfosanditik Kabupaten Sumedang sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya.
5. Target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan telah dilakukan untuk semua bidang pada Diskominfostandi, dievaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan, serta melaporkan statusnya pada pimpinan melalui kegiatan rutin berupa rapat triwulan.

### b. Kelemahan/Kekurangan

1. Peran pelaksana pengamanan informasi yang mencakup semua keperluan belum dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan.
2. Diskominfosanditik Kabupaten Sumedang belum menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi.
3. Belum adanya identifikasi data pribadi yang digunakan dalam proses kerja dan penerapan pengamanan sesuai dengan peraturan perundungan yang berlaku.
4. Belum optimalnya koordinasi proaktif dengan staker terkait (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.
5. Belum optimalnya pelaksanaan dan pengelolaan kelangsungan layanan TIK melalui dokumen BCP dan DRP yang telah disusun.
6. Belum optimalnya proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanannya, pemantauannya dan eskalasi pelaporannya.
7. Masih belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

## **III. ASPEK RISIKO:**

### a. Kekuatan/Kematangan

1. Pemerintah Kabupaten Sumedang telah memiliki program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi yang menjadi bagian dari Peraturan Bupati nomor 50 tahun 2021 tentang Manajemen Sistem Pemerintahan Berbasis Elektronik dan Audit Teknologi Informasi dan Komunikasi.

2. Pemerintah Kabupaten Sumedang telah memiliki kerangka kerja pengelolaan risiko SPBE dengan merujuk pada Permenpan nomor 5 Tahun 2020 tetapi masih dalam tahap implementasi.
  3. Telah menetapkan penanggung jawab manajemen risiko dan menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap indentifikasi aset informasi yang dimiliki dan tertuang dalam pakta integritas manajemen risiko SPBE.
  4. Pemerintah Kabupaten Sumedang telah menyusun dan menentukan langkah mitigasi risiko yang disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang dapat diterima dengan meminimalisir dampak terhadap operasional layanan TIK.
- b. Kelemahan/Kekurangan
1. Penetapan tanggung jawab manajemen risiko telah ditetapkan, namun belum terdapat eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan.
  2. Belum adanya kesesuaian antara program kerja pengelolaan risiko keamanan informasi sebagaimana yang telah tertuang pada Peraturan Bupati nomor 50 tahun 2021 dengan pakta integritas manajemen risiko SPBE.
  3. Identifikasi risiko yang telah tertuang dalam pakta integritas belum dilakukan secara menyeluruh terhadap ruang lingkup aspek keamanan informasi yang berkaitan dengan pengelolaan risiko TIK.
  4. Identifikasi risiko yang telah dilakukan belum mencantumkan pihak pemilik risiko sesuai dengan klasifikasi penentuan aset yang dilakukan mitigasinya.
  5. Belum adanya mekanisme evaluasi secara periodik yang menjadi bagian dari pemantauan terhadap rencana penanggulangan risiko/mitigasi risiko yang harus dilakukan maupun pengkajian ulang profil risiko dan kerangka kerja pengelolaan risiko untuk memastikan/meningkatkan efektivitasnya.

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

- a. Kekuatan/Kematangan
1. Diskominfosanditik Kabupaten Sumedang telah menjalankan kegiatan keamanan informasi baik secara internal maupun eksternal lingkup Diskominfosanditik dan memiliki kebijakan keamanan informasi yang dituangkan dalam rancangan Peraturan Bupati Sumedang tentang Sistem Manajemen Keamanan Informasi.
  2. Telah memiliki sebagian kebijakan dan prosedur keamanan informasi yang merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan pimpinan organisasi.
  3. Telah mencantumkan aspek keamanan informasi yang meliputi penjagaan rahasia, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga.
  4. Diskominfosanditik Kabupaten Sumedang telah menjadikan aspek keamanan informasi menjadi bagian dari manajemen proyek dan menerapkan proses tersebut sebagai tahapan dari evaluasi risiko terhadap implementasi sistem baru serta menjadi upaya dalam menganggulangi permasalahan yang ada.
  5. Telah memiliki kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsiderans keamanan informasi dan penjadwalan uji cobanya namun belum diimplementasikan secara optimal.

b. Kelemahan/Kekurangan

1. Kebijakan dan prosedur terkait keamanan informasi dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk penerapannya yang berupa kebijakan terkait SMKI masih berupa draft belum ditetapkan secara resmi.
2. Prosedur pengelolaan suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindaklanjuti konsekwensinya masih belum terdapat implementasinya secara menyeluruh.
3. Mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya masih belum berjalan secara berkelanjutan dan didokumentasikan secara tertulis dalam prosedur/formulir.
4. Belum dilakukannya mekanisme proses yang mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga secara optimal, tertulis dan berkesinambungan.
5. Belum berjalannya proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan secara berkelanjutan.
6. Konsekwensi dari pelanggaran kebijakan keamanan informasi masih belum didefinisikan, dikomunikasikan dan ditegakkan, baik di internal maupun eksternal Diskominfosanditik Kabupaten Sumedang.
7. Belum melakukan penerapan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis security patch baru, hingga memastikan pemasangan dan melaporkannya.
8. Penerapan proses pengembangan sistem yang aman (*Secure SDLC*) dengan menggunakan prinsip atau metode sesuai standar platform teknologi telah dilakukan namun masih secara sporadis dan belum ditetapkan dalam kebijakan/prosedur yang perlu dilakukan secara berkesinambungan dan konsisten.
9. Seluruh kebijakan dan prosedur keamanan informasi masih dalam tahap konsep/draft dan belum terdapat tahapan evaluasi kelayakannya yang dilakukan secara berkala.
10. Strategi penerapan keamanan informasi masih belum disusun dan diimplementasikan sebagai bagian untuk penyesuaian dengan hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi.
11. Belum adanya evaluasi berupa audit internal yang dilakukan secara konsisten dan berkelanjutan dalam rangka mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi.
12. Analisa untuk menilai aspek finansial ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya apabila ada keperluan merevisi kebijakan dan prosedur yang berlaku masih belum dilakukan secara optimal.

**V. ASPEK PENGELOLAAN ASET:**

a. Kekuatan/Kematangan

1. Diskominfosanditik Kabupaten Sumedang telah memiliki daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi namun belum secara lengkap, akurat dan terpelihara (termasuk kepemilikan aset ).
2. Telah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi namun belum disesuaikan secara periodik

terhadap seluruh aset informasi yang dimiliki sesuai dengan adanya perubahan yang terjadi.

3. Diskominfosanditik Kabupaten Sumedang telah memiliki dokumen analisis jabatan yang berisi definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Diskominfosanditik Kabupaten Sumedang.
4. Diskominfosanditik Kabupaten Sumedang telah memiliki penerapan infrastruktur komputasi yang terpasang dan sudah terlindungi dari gangguan pasokan listrik atau dampak dari petir.
5. Konstruksi ruang penyimpanan perangkat pengolah informasi penting sudah menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung yang sesuai, yang tertuang di Rencana Induk Pengembangan E-government.

b. Kelemahan/Kekurangan

1. Definisi identifikasi dan klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku masih belum tersedia secara menyeluruh memenuhi semua aspek yang diinginkan seperti pemilik informasi/barang serta kualifikasinya misal kritikal atau non kritikal.
2. Belum dilakukan proses evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi dan keperluan pengamanannya.
3. Diskominfosanditik Kabupaten Sumedang belum memiliki proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi serta proses pengelolaan konfigurasi yang diterapkan secara konsisten dan belum didokumentasikan.
4. Diskominfosanditik Kabupaten Sumedang masih belum memiliki tata tertib pengamanan dan penggunaan aset terkait HAKI serta peraturan terkait instalasi piranti lunak di aset TIK.
5. Belum memiliki peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.
6. Pengelolaan identitas elektronik dan proses otentikasi (username & password) telah dilakukan namun belum dilakukan secara menyeluruh terhadap sistem elektronik yang dikelola, termasuk kebijakan terhadap pelanggarannya. Selain itu, juga prosedur pengelolaan/pemberian hak akses, otentikasi dan otorisasi untuk menggunakan aset informasi belum sepenuhnya diterapkan.
7. Belum memiliki prosedur ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data yang sudah tidak diperlukan.
8. Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi serta pelaporan insiden tersebut kepada pihak eksternal ataupun pihak yang berwajib masih belum dilaksanakan dan didokumentasikan secara berkelanjutan.
9. Diskominfosanditik Kabupaten Sumedang belum memiliki proses pengecekan latar belakang SDM dan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
10. Masih belum tersedia daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya.
11. Belum tersedianya proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris).

## **VI. ASPEK TEKNOLOGI:**

### a. Kekuatan/Kematangan

1. Diskominfosanditik Kabupaten Sumedang telah memiliki ruangan tersendiri yang dikhurasukan untuk melakukan operasional dan pengelolaan perangkat server.
2. Pengamanan pada layanan TIK yang menggunakan internet sudah dilakukan lebih dari satu lapis. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll). Hal ini dapat dilihat dari topologi jaringan pada Diskominfosanditik Kabupaten Sumedang.
3. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada.
4. Setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log.
5. Akses yang digunakan dalam mengelola sistem (administrasi sistem) telah menggunakan bentuk pengamanan khusus yang berlapis serta sudah menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi yaitu dengan open VPN.
6. Sistem operasi untuk setiap perangkat desktop dan server di Data Center telah dimutakhirkan dengan versi terkini. Selain itu keseluruhan jaringan, sistem dan aplikasi juga sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada.

### b. Kelemahan/Kekurangan

1. Diskominfosanditik Kabupaten Sumedang telah menerapkan keamanan sistem keseluruhan aset jaringan, sistem dan aplikasi namun belum memiliki konfigurasi standar yang perlu dituangkan dan ditetapkan dalam kebijakan tertulis.
2. Diskominfosanditik Kabupaten Sumedang belum memiliki kebijakan standar penggunaan enkripsi.
3. Belum menggunakan pendingin khusus untuk ruang server seperti PAC.
4. Semua sistem dan aplikasi masih belum menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama.
5. Belum memiliki kontrol terhadap penggunaan password sesuai dengan standar konfigurasi password.
6. Belum dilakukan pemindaian terhadap sistem elektronik yang meliputi jaringan, sistem dan seluruh aplikasi yang dimiliki secara berkala.
7. Belum seluruh sistem elektronik dipasang antivirus/antimalware.

## **VIII. REKOMENDASI**

1. Dalam rangka untuk memastikan berjalannya pengelolaan SMKI secara berkesinambungan, maka perlu ditetapkan tim implemetasi pelaksana pengamanan informasi yang mencakup tugas, tanggung jawab dan wewenang termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan dengan tujuan untuk menjamin pengelolaan keamanan informasi dapat memberikan nilai tambah dalam pelaksanaan dan pengembangan e-government di Kabupaten Sumedang.
2. Perlu menerapkan 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)
3. Perlu meningkatkan kegiatan sosialisasi/literasi keamanan informasi baik 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 Pemerintah Kabupaten Sumedang.
4. Perlu menyusun laporan implemetasi SMKI secara berkala dengan periode waktu tiap bulan dan disampaikan kepada pimpinan untuk dapat dilakukan evaluasi penerapan serta langkah perbaikan dalam menjaga terwujudnya keamanan informasi di Pemkab Sumedang secara menyeluruh pada seluruh pemangku kepentingan yang ada dari pusat sampai dengan desa.
5. Perlu 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.
6. Perlu adanya pelaksanaan dan pengelolaan baik *Business Continuity Plan* dan *Disaster Recovery Plan* (DRP) sebagai upaya dalam menjaga kelangsungan TIK dan menjadi bagian rencana tindakan (response plan) dalam mengantisipasi terjadinya bencana. Dalam penyusunannya, 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 Kabupaten Sumedang 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.
7. Menyusun identifikasi data pribadi yang digunakan dalam proses kerja dan penerapan pengamanan pada tiap aplikasi yang dikelola oleh Diskominfosanditik Pemkab Sumedang sesuai dengan peraturan perundangan yang berlaku dengan merujuk pada Perkominfo 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik, Peraturan Bupati Nomor 45 Tahun 2017 dan referensi hukum lainnya terkait dengan data pribadi.
8. Perlunya menyusun pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanannya, pemantauannya dan

eskala pelaporannya. Hal ini dapat dituangkan dalam karta 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.

9. 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.
10. Perlunya perbaikan dan peningkatan penerapan secara menyeluruh terhadap seluruh ruang lingkup pengelolaan TIK pada Diskominfosanditik Pemerintah Kabupaten Sumedang dimana perlu pembagian peran dan penanggung jawab sampai dengan eskala pelaporan status pengelolaan risiko yang perlu diimplementasikan melalui hasil evaluasi penanganan risiko dan disampaikan kepada pimpinan secara periodik.
11. Dalam kerangka kerja pengelolaan risiko, perlu penyesuaian di dokumen risk register yang telah disusun yaitu identifikasi risiko per aset yang dimiliki. Ditambahkan juga dengan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
12. Perlu menyusun laporan evaluasi penyelesaian langkah mitigasi yang sudah diterapkan. Lalu melakukan pengkajian ulang profil risiko dan kerangka kerja pengelolaan risiko untuk meningkatkan efektivitasnya.
13. Perlunya perbaikan terhadap penilaian risiko yang telah disusun, dengan keterangan adalah sebagai berikut:
  - a) Identifikasi risiko dilakukan berdasarkan kritikalitas aset untuk setiap kategori aset yaitu Perangkat Keras, Perangkat Lunak, Sistem Aplikasi, Jaringan Komunikasi, Personil (pegawai tetap dan non tetap serta pihak ketiga yang terlibat), Informasi, dan Sarana Pendukung yang digunakan dalam penyelenggaraan layanan-layanan TI oleh Diskominfosanditik Kabupaten Sumedang.
  - b) Perlunya penambahan identifikasi risiko-risiko lainnya yang perlu diidentifikasi dari aset utama/penting berikut kontrol yang ada saat ini, rencana kontrol tambahan dan penetapan status penyelesaian dengan mengacu pada risk treatment plan yang telah dibuat.
  - c) Merefer pada Permenpan 5/2020 maka perlu penyesuaian terhadap informasi yang tercantum dalam dengan definisi bahwa kejadian dapat diidentifikasi dari terjadinya suatu peristiwa yang menimbulkan Risiko SPBE yang diperoleh dari riwayat peristiwa dan/atau prediksi terjadinya peristiwa di masa yang akan datang, dalam hal ini kejadian menjadi Risiko dari pelaksanaan SPBE.
  - d) Perlu tambahan definisi pemilik dan pengelola aset, misal terjadi kerusakan atau kehilangan aset, maka perlu penanggung jawab dan penerapan kebijakan manajemen risiko yang akan diimplementasikan.
14. Penyusunan kebijakan dan prosedur terkait keamanan informasi perlu mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya. Begitu pula terkait pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindaklanjuti konsekwensinya, juga perlu disusun prosedur secara tertulis.

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 untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk selanjutnya ditindaklanjuti.
19. Dalam kebijakan SMKI perlu dicantumkan konsekwensi dari pelanggaran kebijakan keamanan informasi, dikomunikasikan dan ditegakkan, baik di internal maupun eksternal Diskominfosanditik Kabupaten Sumedang.
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 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 ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya.
27. 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.
28. Penyusunan 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.
29. Melakukan identifikasi keseluruhan aset yang dimiliki baik aset informasi pada sistem elektronik maupun aset lainnya berdasarkan kategori yang berkaitan dengan pengelolaan sistem elektronik.
30. Melakukan definisi tingkatan hak akses sesuai dengan klasifikasi sistem elektronik yang dikelola.
31. Melakukan dokumentasi terhadap adanya pengelolaan maupun perubahan konfigurasi sistem elektronik.

32. 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*.
33. Menyusun tata tertib pengamanan dan penggunaan aset yang di dalamnya tertuang peraturan HAKI serta instalasi piranti lunak di aset TI.
34. Menyusun peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi yang tertuang dalam dokumen berita acara.
35. Perlu menyusun kebijakan/prosedur pengelolaan identitas elektronik dan proses otentikasi (username & password), termasuk kebijakan terhadap pelanggarannya. Selain itu, juga menyusun prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi.
36. Perlu menyusun dokumentasi riwayat pemeliharaan terhadap aset yang berkaitan dengan pengelolaan sistem elektronik.
37. Perlu 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.
38. 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.
39. Menyusun prosedur terkait penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi serta pelaporan insiden tersebut kepada pihak eksternal ataupun pihak yang berwajib.
40. Perlu membuat prosedur dalam pengecekan latar belakang SDM dan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
41. Daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya perlu dibuatkan prosedurnya, secara dapat dimasukkan di kebijakan SMKI atau menjadi kebijakan teknis terpisah yang tertuang dalam prosedur bagian dari kebijakan keamanan informasi.
42. Menyusun prosedur dalam memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris).
43. Melakukan penerapan pengamanan fisik pada lingkungan data center dengan mekanisme pengamanan kunci digital seperti *fingerprint*, biometrik atau sensor RFID
44. Melakukan pemindaian terhadap sistem elektronik yang meliputi jaringan, sistem dan seluruh aplikasi yang dimiliki secara berkala.
45. Melakukan pemasangan antivirus dan antimalware pada sistem elektronik yang dikelola.
46. Mencantumkan standar dalam menggunakan enkripsi (penerapan kriptografi) di kebijakan SMKI, serta membuat dokumen turunan dari kebijakan tersebut.
47. 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.
48. 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 Diskominfosanditik Pemkab Sumedang diharapkan dapat menyesuaikan dan memperhatikan standar pengelolaan dan syarat ruang data center sesuai yang tercantum dalam pedoman teknis yang telah ditetapkan.
49. 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.
50. 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*).

**Sumedang, 13 Desember 2021**  
Narasumber Instansi:  
Diskominfosanditik Kab. Sumedang

1. Mamat Rohimat, S.Pd., M.Pd

2. Agus Ramdan Sutarsa, S.Sos.

3. Hendri Wiguna, S.Kom.

4. Roza Hidayat, S.Kom.

5. Alfan Fathurohman, S.T.

6. Yadi Apriyadi

7. Musni

**Assessor Indeks KAMI:**

1. Assessor : Diah Sulistyowati, S.Kom.



2. Assessor : Ivan Bashofi, S.S.T.TP.



3. Assessor : Carissa Mega Y., S.Tr.TP.

