



LAPORAN VERIFIKASI INDEKS KAMI



INDEKS
KEAMANAN
INFORMASI

Instansi/Perusahaan:

Dinas Komunikasi dan Informatika DIY

Narasumber Instansi/Perusahaan:

1. Mohamad Zainuri
2. Anik Budiati
3. Isnoor
4. Muhammad Nur Isa Roechan

Unit Kerja:

Bidang Manajemen Informatika
Dinas Komunikasi dan Informatika DIY

Alamat:

Gedung Unit 7 Lt. 2, Komplek Kepatihan,
Danurejan, Yogyakarta

Tel:

(0274) 563543

Email:

bidangmi.kominfo@jogjaprov.go.id

**Pimpinan Unit Kerja/Kepala Dinas Kominfo
DIY:**

Ir. Rony Primanto Hari, MT

A. Ruang Lingkup:

1. Proses/Layanan:
 - Pengelolaan Infrastruktur Data Center dan Pengelolaan LPSE Pemda DIY
2. Informasi:
 - Data Penyedia jasa
3. Aplikasi:
 - Sistem Pengadaan Secara Elektronik
4. Infrastruktur Jaringan/Network:

Jaringan internet disediakan oleh:

 - GMedia;
 - JMN (Jogja Medianet)
5. Lokasi
 - a. DATA CENTER (DC):
 - ☒ Lokasi di Kantor Dinas Kominfo DIY

b. DISASTER RECOVERY CENTER (DRC):

☒ Lokasi DRC di Batam dan dikelola oleh Pihak Ketiga (PT Mora Telematika Indonesia)

**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 (ref. kebijakan yang disyaratkan ISO 27001)	✓		Rilis
2	Syarat & Ketentuan Penggunaan Sumber Daya TI (Email, Internet, Aplikasi)	✓		Rilis
3	Sasaran TI / Keamanan Informasi	✓		Rilis
4	Organisasi Keamanan Informasi/ Fungsi Keamanan TI)	✓		Rilis
5	Metodologi Manajemen Risiko TI	✓		Rilis
6	Business Continuity Plan	✓		Rilis
7	Klasifikasi Informasi	✓		Rilis
8	Standar software dekstop	✓		Rilis
9	Metode Pengukuran Efektivitas Kontrol	✓		Rilis
10	Non Disclosure Agreement (NDA)	✓		Rilis
	Prosedur- Prosedur:			
1	Pengendalian Dokumen	✓		Rilis
2	Pengendalian Rekaman/Catatan	✓		Rilis
3	Tindakan Perbaikan	✓		Rilis
4	Audit Internal	✓		Rilis
5	Penanganan (Handling) Informasi: pelabelan, penyimpanan, pertukaran, penghancuran	✓		Rilis
6	Pengelolaan Media Removable & Disposal	✓		Rilis
7	Pengelolaan Perubahan Sistem TI (Change Control Sistem TI)	✓		Rilis
8	Pengelolaan Hak Akses (User Access Management)	✓		Rilis
9	Teleworking (Akses Remote)	✓		Rilis
10	Pengelolaan & Pelaporan Gangguan / Insiden Keamanan Informasi	✓		Rilis
11	Pemantauan (Monitoring) Sumber Daya TI:	✓		Rilis

	a. Monitoring Kapasitas b. Log Penggunaan User			
12	Instalasi & Pengendalian Software	✓		Rilis
13	Back-up & restore (prosedur/jadwal)	✓		Rilis

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

Dokumen yang diperiksa:

1. Masterplan Jogja Smart Province (JSP), 2018
2. Lampiran Masterplan Jogja Smart Province (JSP), Roadmap 2019-2023
3. Peraturan Gubernur DIY, nomor 2 Tahun 2018 tentang Tata Kelola TIK
4. Peraturan Gubernur DIY, nomor 31 Tahun 2016 tentang Sistem Manajemen Keamanan Informasi
5. Blueprint Teknologi Informasi dan Komunikasi, Pemda DIY 2018-2023
6. Statement of Applicability, Dinas Kominfo DIY, nomor 480/04370 tahun 2016
7. Kebijakan dan Prosedur Pengendalian Akses, 2018 (LPSE.SMKI.PRO.04)
8. Kebijakan dan Prosedur Pengamanan dan Pengelolaan Aset SMKI, 2018 (LPSE.SMKI.PRO.02)
9. Konteks dan Ruang Lingkup Sistem Manajemen, ver 2.0, 2018 (LPSE.SM.PRO.02)
10. Kebijakan dan Prosedur Instalasi Perangkat Lunak, 2018 (LPSE.SMKI.PRO.02)
11. Kebijakan dan Prosedur Perubahan Fasilitas DC, 2018 (LPSE.SMKI.PRO.08)
12. Kebijakan dan Prosedur kepatuhan Keamanan Informasi, 2018 (LPSE.SMKI.PRO.06)
13. Kebijakan dan Prosedur Perubahan Fasilitas DC, 2018 (LPSE.SMKI.PRO.08)
14. Kebijakan dan Prosedur Audit Internal (LPSE.SM.PRO.01)
15. Kebijakan dan Prosedur Penanganan Ketidaksesuaian dan Peningkatan Ver 2.0 (LPSE.SM.PRO.04)
16. Kebijakan dan Prosedur Tinjauan Manajemen, ver 2.0, 2018 (LPSE.SM.PRO.08)
17. Kebijakan dan Prosedur Manajemen Risiko, ver 2.0, 2018 (LPSE.SM.PRO.03)
18. Kebijakan dan Prosedur Manajemen Sistem manajemen, ver 2.0, 2018 (LPSE.SM.PRO.06)
19. Kebijakan dan Prosedur Manajemen Kapasitas, ver 1.3 (LPSE.SMKI.PRO.09)
20. Kebijakan dan Prosedur keamanan SDM ver 1.3 (LPSE.SMKI.PRO.13)
21. Kebijakan dan Prosedur Pengamanan Pihak Ketiga, ver 1.3 (LPSE.SMKI.PRO.12)
22. Kebijakan dan Prosedur Pengelolaan Data Center, ver 1.3 (LPSE.SMKI.PRO.10)
23. Kebijakan dan Prosedur Klasifikasi dan Penanganan Informasi, ver 1.3 (LPSE.SMKI.PRO.01)
24. Kebijakan dan Prosedur Pengendalian Dokumentasi, ver 2.0 (LPSE.SM.PRO.05)
25. Kebijakan dan Prosedur Peningkatan Pemahaman Kesadaran dan Komunikasi, ver 2.0 (LPSE.SM.PRO.07)
26. Kebijakan dan Prosedur Pengelolaan Insiden Keamanan Informasi, ver 1.3 (LPSE.SMKI.PRO.05)
27. Kebijakan dan Prosedur Kelangsungan Bisnis dan Keamanan Informasi, ver 1.3 (LPSE.SMKI.PRO.07)
28. Rencana Pemulihan dan keberlanjutan Bisnis, ver 1.2 (LPSE.SMKI.DOK.01)

Bukti-bukti (rekaman/arsip) penerapan SMKI:

1. Review Hak Akses LPSE, 1 November 2018
2. Formulir Permintaan Perubahan, 25 Juli 2017
3. Instalasi software
4. Serah terima aset

5. Evaluasi pihak ketiga
6. Notulen Review insiden
7. Rencana pemulihan BCP
8. Formulir pengukuran SMKI
9. Formulir Pemeliharaan Aset
10. Formulir operasional lainnya

I. RINGKASAN EKSEKUTIF

Penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik mengingat peran TIK yang semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik (*Good Corporate Governance*).

Untuk meningkatkan kesadaran akan pentingnya keamanan informasi dalam penyelenggaraan Tata Kelola TIK, Badan Siber dan Sandi Negara (BSSN) telah melakukan sosialisasi dan bimbingan teknis yang kemudian ditindaklanjuti dengan kegiatan kajian keamanan informasi kepada instansi penyelenggara pelayanan publik menggunakan alat bantu evaluasi Indeks Keamanan Informasi (KAMI). Alat evaluasi ini ditujukan untuk memberikan gambaran kondisi kesiapan (kelengkapan dan konsistensi) keamanan informasi dan identifikasi tingkat kematangan penerapan pengamanan informasi kepada pimpinan Instansi, yang diidentifikasi berdasarkan kondisi saat ini dan menghasilkan rekomendasi untuk keperluan pembenahan dan/atau peningkatan berkelanjutan terhadap Tata Kelola Keamanan Informasinya.

Analisis dilakukan terhadap tingkat kelengkapan dokumentasi serta kematangan implementasi kontrol keamanan sesuai kategorisasi tingkat kepentingan Sistem Elektronik (SE) di Dinas Kominfo DIY. Area yang dievaluasi meliputi **Tata Kelola Keamanan Informasi, Pengelolaan Risiko Keamanan Informasi, Kerangka Kerja Keamanan Informasi, Pengelolaan Aset Informasi, serta Teknologi dan Keamanan Informasi.**

Dari hasil **Desktop Assessment dan Onsite Assessment** menggunakan Indeks KAMI versi 3.1 berbasis SNI ISO/IEC 27001:2013 yang telah dilakukan oleh BSSN, tingkat kematangan dan score Indeks Kami di Dinas Kominfo DIY adalah sebagai berikut:

- Kategori Sistem Elektronik: **TINGGI**
- Score Tingkat Kesiapan dan Kematangan: **547 dari maksimum score 645 (84,8%)**
- Tingkat Kematangan Area:

AREA ASSESSMENT	LEVEL
Tata Kelola	III+
Pengelolaan Risiko	V
Kerangka Kerja Keamanan Informasi	V
Pengelolaan Aset	III
Teknologi dan Keamanan Informasi	II

Berdasarkan nilai dan kategori Sistem Elektronik (SE) tersebut, Dinas Kominfo DIY telah menerapkan Sistem Manajemen Keamanan Informasi dengan baik sesuai Peraturan Menteri Kominfo nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi.

Peningkatan dan perbaikan perlu dilakukan secara terus menerus khususnya pada area: **Tata Kelola, Pengelolaan Aset dan Teknologi**. Sedang konsistensi penerapan harus terus dipelihara untuk aspek **Pengelolaan Risiko** dan **Kerangka Kerja Keamanan Informasi**.

Terlampir disajikan hasil Desktop Assessment dan Onsite Assessment yang memvalidasi terhadap kajian mandiri keamanan informasi di Dinas Kominfo DIY dalam bentuk *bar chart*, *radar chart* dan tabel capaian nilai masing-masing area, kekuatan dan kekurangan aspek kerangka kerja dan aspek penerapan yang dimiliki, serta rekomendasi dari Tim Pengkaji sebagai bahan pertimbangan untuk memberikan peningkatan Sistem Tata Kelola Keamanan Informasi yang telah diterapkan.

SCORING INDEKS KAMI:

Total Score Sebelum Verifikasi: 555 (ref. file Indeks KAMI sebelum Verifikasi)

Indeks KAMI (Keamanan Informasi)

Responden:
Bidang Manajemen Informatika
Dinas Komunikasi dan Informatika DIY

Hasil Evaluasi Akhir:

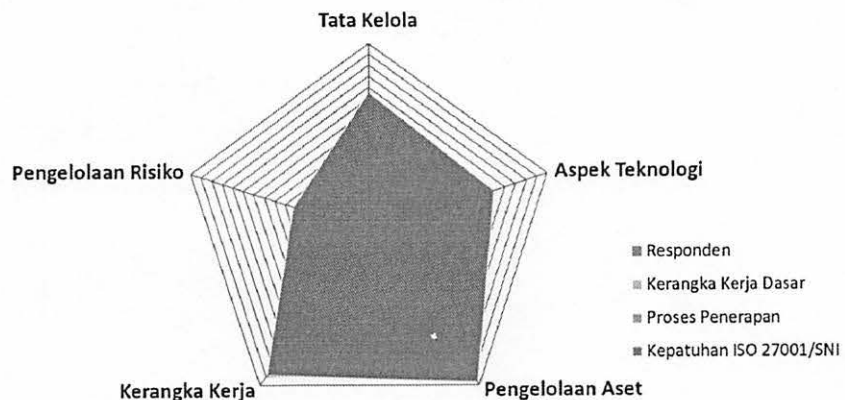
Cukup

Gedung Unit 7 Lt. 2, Komplek Kepatihan, Danurejan,
Yogyakarta

Tingkat Kelengkapan Penerapan
Standar ISO27001 sesuai Kategori SE  555

(0274) 563543
bidangmi.kominfo@jogjapro.go.id
23/10/2018

Skor Kategori SE	: 26	Kategori SE	Tinggi
Tata Kelola	: 117	Tk Kematangan: III+	
Pengelolaan Risiko	: 72	Tk Kematangan: V	II
Kerangka Kerja Keamanan Informasi	: 149	Tk Kematangan: V	s/d
Pengelolaan Aset	: 148	Tk Kematangan: III	V
Teknologi dan Keamanan Informasi	: 69	Tk Kematangan: II	



Total Score Setelah Verifikasi: 547 (ref. file Indeks KAMI pasca Verifikasi)

Indeks KAMI (Keamanan Informasi)

Responden:
Bidang Manajemen Informatika
Dinas Komunikasi dan Informatika DIY

Hasil Evaluasi Akhir:

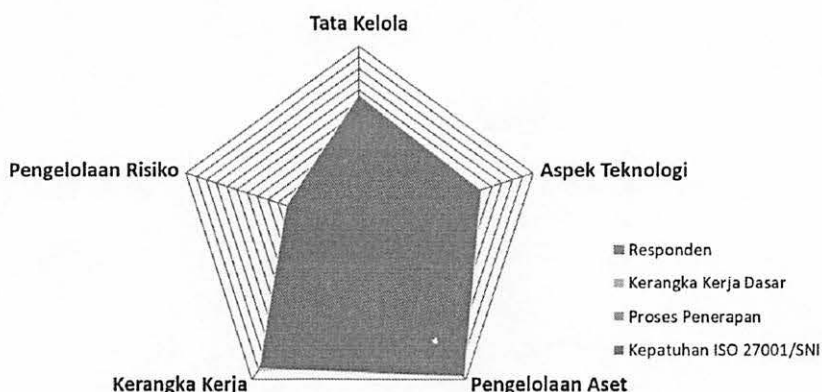
Cukup

Gedung Unit 7 Lt. 2, Komplek Kepatihan, Danurejan,
Yogyakarta

(0274) 563543
bidangmi.kominfo@jogjapro.go.id
23/10/2018

Tingkat Kelengkapan Penerapan
Standar ISO27001 sesuai Kategori SE : 547

Skor Kategori SE	: 29	Kategori SE	Tinggi
Tata Kelola	: 106	Tk Kematangan: III+	
Pengelolaan Risiko	: 72	Tk Kematangan: V	II
Kerangka Kerja Keamanan Informasi	: 149	Tk Kematangan: V	s/d
Pengelolaan Aset	: 142	Tk Kematangan: III	V
Teknologi dan Keamanan Informasi	: 78	Tk Kematangan: II	



II. KEKUATAN/KEMATANGAN

1. Aspek Komitmen dan Ketersediaan Kerangka Kerja

- Dinas Kominfo DIY telah menunjukkan komitmen yang kuat terhadap penerapan program keamanan informasi sesuai Peraturan Menteri Kominfo nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI)
- Dinas Kominfo DIY telah mendapatkan sertifikasi standar ISO 27001:2013 sejak tahun 2016 dan telah menjalani *Audit Surveillance* secara rutin dari Badan Sertifikasi BSI
- Memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya
- Mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan
- Menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan
- Ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi
- Dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan
- Kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya
- Sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan
- Sudah tersedia kerangka kerja perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya
- Perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk

- l. Sudah memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada
- m. Sudah mempunyai kebijakan akses kontrol untuk *operating system*, *network* dan *database*

2. Aspek Penerapan

- a. Sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) khususnya untuk melindungi aset TI yang ada di Kantor Dinas Kominfo DIY, khususnya untuk layanan LPSE dan infrastruktur Data Center dan DRC
- b. Lokasi DC/DRC terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya
- c. Jaringan internet Kominfo DIY memiliki backup dari penyedia jaringan yang berbeda dari penyedia jaringan utama
- d. Infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada
- e. Mayoritas bukti-bukti implementasi telah didokumentasikan dengan baik.
- f. Pemantauan dan perawatan perangkat pendukung seperti AC, CCTV, termasuk test beban Genset telah dilakukan dengan baik

III. KELEMAHAN/KEKURANGAN

- a. Belum ditetapkan standar parameter untuk SUHU, KELEMBABAN dan Batas ambang (*Threshold*) kapasitas sumber daya TI seperti CPU, Memori, utilisasi *bandwidth* jaringan
- b. *Grounding system* untuk penangkal petir sulit dilakukan perawatan dan pengukuran karena tidak memiliki bak kontrol
- c. Sinkronisasi waktu dan *review user access fingerprint* belum dapat dilakukan secara konsisten karena:
 - Perangkat tidak mendukung dilakukannya sinkronisasi waktu secara otomatis
 - Password user *administrator access control fingerprint* sudah tidak dapat ditelusuri sehingga tidak dapat dilakukan review terhadap hak akses
- d. Perangkat jaringan (*switch*) dipasang tanpa perlindungan yang memadai, misalnya perangkat *switch* yang dipasang di sebelah komputer di ruang *bidding* dan di sekitar pintu masuk DC

IV. REKOMENDASI PERBAIKAN

- Dilakukan penetapan standar parameter untuk SUHU, KELEMBABAN dan Batas ambang (*Threshold*) kapasitas sumber daya TI
- Perlu direncanakan perbaikan terhadap *grounding system* untuk menjaga aset TI di Data Center khususnya dan di kantor Dinas Kominfo DIY umumnya agar terhindar dari risiko gangguan petir
- Perlu dipasang tanda Larangan Merokok di Area Genset dan pemasangan/pemindahan kamera CCTV untuk memantau area Genset
- Memasang perangkat-perangkat jaringan dan perangkat lainnya dengan perlindungan yang memadai

V. REKOMENDASI PENINGKATAN (IMPROVEMENT)

- Kontrol dalam dokumen *Statement of Applicability* berikut perlu direvisi dari "Tidak diterapkan" menjadi "Diterapkan":

14.2.9 System acceptance testing karena UAT dilakukan terhadap aplikasi SPSE bersama LKPP pada saat udprgrade ataupun instalasi SPSE

- Implementasi Sistem Manajemen Keamanan Informasi perlu diperluas untuk pengembangan dan aplikasi e-Government dengan melakukan hal-hal sebagai berikut:
 1. Menyusun standar Pengembangan Aplikasi secara aman (*Secure Software Development Life Cycle – SDLC*) dan menerapkannya dalam fase pengembangan aplikasi
 2. Memasukkan persyaratan-persyaratan keamanan aplikasi dalam *User Requirement* (seperti minimum panjang password, *maximum failed login attempt*, *session timeout*, *password history*) dan melakukan *security testing* sebelum aplikasi masuk ke lingkungan produksi
 3. Melakukan *vulnerability assessment* dan/atau *penetration testing* terhadap aplikasi dan infrastruktur e-Government untuk memastikan keamanannya dari ancaman intrusi dari user yang tidak berwenang.

Yogyakarta, 07 Desember 2018

Narasumber Dinas Kominfo DIY:

1. Mohamad Zainuri

2. Anik Budiati

3. Isnoor

4. Muhammad Nur Isa Roechan

Assessor Indeks KAMI:




1. Assessor Utama:
Haryatno

2. Assessor Pendamping:
Mohamad Heri Herman Aji

3. Assessor Pendamping:
Johanes Widhi Candra

Daftar Hadir Review Indeks Keamanan Informasi
Pemerintah Provinsi DIY


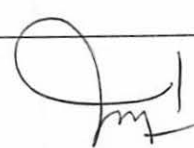
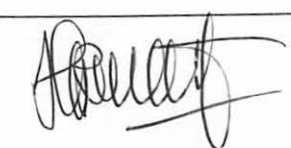
4-8 Desember 2018

No	Nama	Jabatan	No telepon/E-mail	Paraf
1	M. Nur Afri			
2				
3	Haryadno		0812 235 2575	
4	M Heri Herman Aji		0811 96 1103	
5				

No	Nama	Jabatan	No telepon/E-mail	Paraf
6				
7				
8				
9				
10				
11				
12				

Daftar Hadir Review Indeks Keamanan Informasi
Pemerintah Provinsi DIY



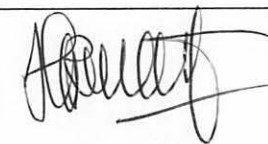
4-8 Desember 2018

No	Nama	Jabatan	No telepon/E-mail	Paraf
1	M. Nur Afif			
2				
3	Haryahw		08122352579	
4	M. Heri Herman Aji		0811961103	
5				

No	Nama	Jabatan	No telepon/E-mail	Paraf
6				
7				
8				
9				
10				
11				
12				

Daftar Hadir Review Indeks Keamanan Informasi
Pemerintah Provinsi DIY

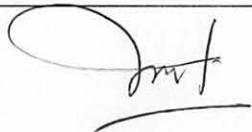

4-8 Desember 2018

No	Nama	Jabatan	No telepon/E-mail	Paraf
1	M. Nur Afif			
2				
3	Haryahw		08122352579	
4	M. Heri Herman Aji		0811961103	
5				

No	Nama	Jabatan	No telepon/E-mail	Paraf
6				
7				
8				
9				
10				
11				
12				

Daftar Hadir Review Indeks Keamanan Informasi
Pemerintah Provinsi DIY

4-8 Desember 2018

No	Nama	Jabatan	No telepon/E-mail	Paraf
1				
2	M Nur Aji			
3	Haryanto		0812.235 2579	
4	M HERI HERMAN Aji		0811961103	
5				

No	Nama	Jabatan	No telepon/E-mail	Paraf
6				
7				
8				
9				
10				
11				
12				