



## BADAN SIBER DAN SANDI NEGARA

Jalan Harsono RM. Nomor 70, Ragunan, Jakarta 12550

Telepon (021) 7805814, Faksimile (021) 78844104

Website: <http://www.bssn.go.id>, E-mail: [humas@bssn.go.id](mailto:humas@bssn.go.id)

### BERITA ACARA PEMERIKSAAN DOKUMEN

Pada hari ini *Selasa* dan *Rabu* tanggal *tiga puluh dan tiga puluh satu bulan Oktober* tahun *dua ribu delapan belas* bertempat di Kantor Dinas Kominfo Provinsi Jateng, Kami selanjutnya disebut sebagai PIHAK II :

1. Egia Kerta Anggara
2. Rakean Bagus M.R.
3. Eduar Fardji

Telah melakukan pemeriksaan dokumen dalam rangka Desktop Assessment dan Onsite Visit Pemeringkatan Indeks Keamanan Informasi untuk kepentingan Dinas Kominfo Provinsi Jawa Tengah

Pemeriksaan Dokumen dilakukan terhadap dokumen-dokumen hardcopy berikut :

1. Pergub Jateng No. 45 Thn 2013 Tentang Penyelenggaraan TIK Pemprov Jateng
2. Pergub Jateng No. 70 Thn 2016 Tentang Organisasi dan Tata Kerja Dinas Komunikasi dan Informatika Provinsi Jawa Tengah
3. Pergub Jateng No. 89 Thn 2016 Tentang Sistem Manajemen Informasi Terintegrasi Pemprov Jateng
4. KepGub Jateng No. 550/36 Thn 2017 Tentang Pembentukan Tim Pengarah dan Tim Pelaksana Government Resources Management System (GRMS) Dalam Penyelenggaraan Pemerintahan Provinsi Jawa Tengah
5. Master Plan TI Pemerintah Provinsi Jawa Tengah 2018-2023

File-file Kebijakan dan Prosedur berikut, diperlihatkan kepada Tim Asesor dalam bentuk tampilan di layar presentasi. Seluruh file berikut ini dibuat pada tahun 2013 dan pada saat diperlihatkan masih dalam bentuk draft, belum disahkan oleh pejabat yang berwenang :

6. Kebijakan dan Prosedur Co-Location Server
7. Kebijakan dan Prosedur Klasifikasi dan Penanganan Informasi
8. Kebijakan dan Prosedur Pengamanan dan Pengelolaan Aset
9. Konteks dan Ruanglingkup SMKI
10. Kebijakan dan Prosedur Instalasi Perangkat Lunak
11. Kebijakan dan Prosedur Pengendalian Akses
12. Sasaran dan Rencana Kerja SMKI
13. Kebijakan dan Prosedur Pengelolaan Insiden
14. Kebijakan dan Prosedur Pengendalian Dokumentasi
15. Kebijakan dan Prosedur Kepatuhan Keamanan Informasi
16. Kebijakan dan Prosedur Peningkatan Pemahaman (Awerness) dan Komunikasi
17. Kebijakan dan Prosedur Keberlanjutan Bisnis dan Keamanan Informasi
18. Kebijakan dan Prosedur Pengukuran



19. Kebijakan dan Prosedur Audit Internal
20. Kebijakan dan Prosedur Manajemen Perubahan Fasilitas Data Center
21. Kebijakan dan Prosedur Keamanan Jaringan
22. Kebijakan dan Prosedur Tinjauan Manajemen
23. Kebijakan dan Prosedur Manajemen Kapasitas
24. Kebijakan dan Prosedur Penanganan Ketidaksesuaian dan Peningkatan
25. Kebijakan dan Prosedur Manajemen Risiko
26. Kebijakan dan Prosedur Pengelolaan Data Center
27. Kebijakan dan Prosedur Pengamanan Pihak Ketiga
28. Kebijakan dan Prosedur Keamanan Sumber Daya Manusia

Pada saat dilakukan Onsite Visit ke Data Center rekaman Bukti-bukti (rekaman/arsip) penerapan SMKI yang diperlihatkan adalah sbb:

1. Buku Tamu di Data Center
2. Buku aktivitas pemeliharaan Genset

Dokumen-dokumen tersebut diserahkan oleh Dinas Kominfo Provinsi Jawa Tengah Untuk kepentingan Desktop Assessment dan Onsite Visit Pemeringkatan Indeks Keamanan Informasi, sudah dilakukan diskusi tatap muka dengan selanjutnya disebut PIHAK I :

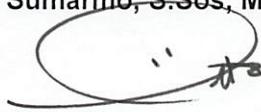
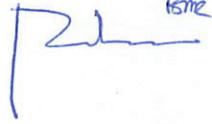
1. Eny Soelastri, SH.
2. Eka Suprapti, ST,MM.
3. Toto Sumarmo, S.Sos, M.Kom

Dokumen-dokumen tersebut di atas sudah dikembalikan oleh PIHAK II kepada PIHAK I pada saat Berita Acara ini dibuat.

Sehubungan dengan hal tersebut, PIHAK II sepakat melakukan penjagaan kerahasiaan informasi dan/atau dokumen yakni dengan:

- 1) memperlakukan informasi dan/atau dokumen milik PIHAK I dengan hati-hati dan bijaksana agar terjamin keutuhan dokumen, terhindar dari kerusakan atau kehilangan, dan tidak memberikannya kepada PIHAK lain, mempublikasikan, atau menyebarluaskannya, sama seperti memperlakukan informasi dan/atau dokumen miliknya sendiri yang tidak ingin diberikan kepada PIHAK lain, dipublikasikan, atau disebarluaskan;
- 2) memanfaatkan informasi dan/atau dokumen milik PIHAK I sesuai tujuan diberikannya informasi dan/atau dokumen tersebut yakni hanya untuk kegiatan Pemeringkatan Indeks KAMI; dan
- 3) mengembalikan seluruh informasi dan/atau dokumen PIHAK I setelah seluruh kegiatan Desktop Assessment Pemeringkatan Indeks KAMI selesai.

Ketentuan penjagaan kerahasiaan yang dibuktikan dengan membuat surat pernyataan menjaga kerahasiaan yang merupakan lampiran yang tidak terpisahkan dari Berita Acara Pemeriksaan Dokumen dan/atau Dokumen ini.

<p>Jakarta, 1 November 2018</p> <p>Narasumber :</p> <p>Dinas Kominfo Prov Jateng :</p> <p>1. Eny Soelastri, SH.</p>  <p>2. Eka Suprapti, ST,MM.</p>  <p>3. Toto Sumarmo, S.Sos, M.Kom</p> 	<p>Assessor Indeks KAMI:</p> <p>1. Assessor Utama: Egia Kerta Anggara</p>  <p>2. Assessor Pendamping: Rakean Bagus M.R.</p>  <p>3. Assessor Pendamping: Eduar Fardji</p> 
---	---



	<b>LAPORAN VERIFIKASI INDEKS KAMI</b>	 <b>INDEKS KEAMANAN INFORMASI</b>												
<b>Instansi/Perusahaan:</b> Dinas Komunikasi dan Informatika Provinsi Jawa Tengah	<b>Narasumber Instansi/Perusahaan:</b> 1. Eny Soelastri, SH. 2. Eka Suprapti, ST,MM. 3. Toto Sumarmo, S.Sos, M.Kom													
<b>Alamat:</b> Jl. Menteri Supeno 1 / 2 Semarang, Jawa Tengah 50243	<b>Tel :</b> (024)8319140 <b>Fax:</b> (024)8443916													
<b>Email:</b>	<b>Pimpinan Unit Kerja:</b> Dadang Somantri, ATD,MT													
<p>A. <u>Ruang Lingkup:</u></p> <p>1. Instansi / Unit Kerja:        a. Bidang Teknologi Informasi dan Komunikasi        b. Bidang e-Government        c. Bidang Persandian dan Keamanan Informasi</p> <p>2. Fungsi Kerja:        Dinas Komunikasi dan Informatika Provinsi Jawa Tengah dibentuk berdasarkan Peraturan Daerah Provinsi Jawa Tengah Nomor 9 Tahun 2016 tentang Pembentukan Dan Susunan Perangkat Daerah Provinsi Jawa Tengah dan Peraturan Gubernur Jawa Tengah Nomor 70 Tahun 2016 tentang Organisasi dan Tata Kerja Dinas Komunikasi dan Informatika Provinsi Jawa Tengah. Adapun tugas dari Dinas Komunikasi dan Informatika Provinsi Jawa Tengah membantu Gubernur melaksanakan urusan pemerintahan bidang komunikasi dan informatika, bidang persandian, dan bidang statistik yang menjadi kewenangan Daerah dan tugas pembantuan yang ditugaskan kepada Daerah.</p> <p>Ruang lingkup kegiatan Verifikasi Indeks KAMI pada Dinas Kominfo Provinsi Jawa Tengah mencakup dua fungsi pengelolaan berikut :</p> <p>a. Data Center Dinas Kominfo Prov Jateng, dan        b. Pengelolaan Aplikasi Utama milik Dinas Kominfo Prov Jateng</p> <p>3. Lokasi:</p> <table border="1"> <thead> <tr> <th>No</th> <th>Nama Lokasi</th> <th></th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Kantor Pusat</td> <td>Jl. Menteri Supeno 1 / 2 Semarang, Jawa Tengah 50243</td> </tr> <tr> <td>2</td> <td>Data Center</td> <td>Jl. Menteri Supeno Semarang, Jawa Tengah 50243</td> </tr> <tr> <td>3</td> <td>Disaster Recovery</td> <td>Batam</td> </tr> </tbody> </table>			No	Nama Lokasi		1	Kantor Pusat	Jl. Menteri Supeno 1 / 2 Semarang, Jawa Tengah 50243	2	Data Center	Jl. Menteri Supeno Semarang, Jawa Tengah 50243	3	Disaster Recovery	Batam
No	Nama Lokasi													
1	Kantor Pusat	Jl. Menteri Supeno 1 / 2 Semarang, Jawa Tengah 50243												
2	Data Center	Jl. Menteri Supeno Semarang, Jawa Tengah 50243												
3	Disaster Recovery	Batam												

B. Nama /Jenis Layanan Publik:

1. Portal Resmi Provinsi Jawa Tengah : jatengprov.go.id
2. **eMonev** (Monitoring dan Evaluasi Pemerintah Daerah Provinsi Jawa Tengah) : <http://emonev.jatengprov.go.id>
3. **Lapor Gub.** adalah Portal Laporan Pengaduan Online Seputar Pemerintah Provinsi Jawa Tengah : <https://laporgub.jatengprov.go.id>
4. **GRMS Jateng** adalah Portal Government Resource Management System : <https://grms.jatengprov.go.id>

C. Aset TI yang kritikal:

1. Informasi:

Data / Informasi yang terdapat pada aplikasi yang dibuat dan dikelola oleh Dinas Kominfo Pemprov Jateng yang merupakan informasi bagi pihak pimpinan dalam mendukung proses pengambilan keputusan adalah salah satu informasi utama yang perlu dijaga kerahasiaan, integritas data dan ketersediaan data nya.

Data/Informasi tersebut terdapat pada :

- a. Informasi pada aplikasi di Website GRMS Jateng
- b. Informasi pada aplikasi eMonev
- c. Informasi pada aplikasi Lapor Gub

2. Server:

Seluruh aplikasi utama yang dibuat dan dikelola oleh Dinas Kominfo Pemprov Jateng ditempatkan pada Server yang berada pada ruangan Data Center.

Adapun aplikasi utama tersebut adalah sbb:

- a. **Portal Resmi Provinsi Jawa Tengah**
- b. **eMonev**
- c. **Lapor Gub**
- d. **GRMS Jateng**

3. Infrastruktur Jaringan / Network

Jaringan yang digunakan untuk menghubungkan Server dengan semua pengguna yang ada di seluruh SKPD adalah jaringan Fiber Optic.

D. DATA CENTER (DC):

(*Beri keterangan apakah ruang Data Center terpisah dengan perimeter/pembatas, memiliki pengamanan fisik dan sarana pendukung, dsb)*

- **ADA, dalam ruangan khusus**  ADA, jadi satu dengan ruang kerja

E. DISASTER RECOVERY CENTER (DRC):

(*Jika ada, jelaskan kondisi DRC: colocation di pihak ketiga atau di instansi lain termasuk pengelolaan keamanan DRC)*

- **ADA** →  **Dikelola Internal**      ■ **Dikelola Pihak Ketiga**  
 **TIDAK ADA**

<b>Status Ketersediaan Dokumen Kerangka Kerja Sistem Manajemen Keamanan Informasi (SMKI)</b>				
No	Nama Dokumen	Ya	Tdk	Keterangan (D: Draf, R:Rilis, T:Tersosialisasikan)
	<b>Kebijakan, Sasaran, Rencana, Standar</b>			
1	Kebijakan Keamanan Informasi (ref. kebijakan yg disyaratkan ISO 27001)	Ya		Pergub Jateng No. 45 Thn 2013 Tentang Penyelenggaraan TIK Pemprov Jateng
2	Syarat & Ketentuan Penggunaan Sumber Daya TI (Email, Internet, Aplikasi)	Ya		<b>Draft</b> Kebijakan dan Prosedur Instalasi Perangkat Lunak
3	Sasaran TI / Keamanan Informasi	Ya		<b>Draft</b> Sasaran dan Rencana Kerja SMKI
4	Organisasi TI / Keamanan Informasi (IT Steering Committee, Fungsi Keamanan TI)		Tdk	
5	Metodologi Manajemen Risiko TI	Ya		<b>Draft</b> Kebijakan dan Prosedur Manajemen Risiko
6	Business Continuity Plan	Ya		<b>Draft</b> Kebijakan dan Prosedur Keberlanjutan Bisnis dan Keamanan Informasi
7	Klasifikasi Informasi	Ya		Ref. UU no 14 /2008 - Keterbukaan Informasi Publik. Klasifikasi informasi ada 2: Informasi PUBLIK dan "YANG DIKECUALIKAN"
8	Standar software dekstop	Ya		<b>Draft</b> Kebijakan dan Prosedur Instalasi Perangkat Lunak
9	Metode Pengukuran Efektivitas Kontrol	Ya		<b>Draft</b> Kebijakan dan Prosedur Pengukuran
10	Non Disclosure Agreement (NDA)		Tdk	
	<b>Prosedur- Prosedur:</b>			
1	Pengendalian Dokumen	Ya		<b>Draft</b> Kebijakan dan Prosedur Pengendalian Dokumentasi

2	Pengendalian Rekaman/Catatan	Ya		<b>Draft</b> Kebijakan dan Prosedur Pengendalian Dokumentasi
3	Tindakan Perbaikan & Pencegahan		Tdk	
4	Audit Internal	Ya		<b>Draft</b> Kebijakan dan Prosedur Audit Internal
5	Penanganan (Handling) Informasi: pelabelan, penyimpanan, pertukaran, penghancuran		Tdk	
6	Pengelolaan Media Removable & Disposal		Tdk	
7	Pengelolaan Perubahan Sistem TI (Change Control Sistem TI)	Ya		<b>Draft</b> Kebijakan dan Prosedur Manajemen Perubahan Fasilitas Data Center
8	Pengelolaan Hak Akses (User Access Management)	Ya		<b>Draft</b> Kebijakan dan Prosedur Pengendalian Akses
9	Teleworking (Akses Remote)		Tdk	
10	Pengelolaan & Pelaporan Gangguan / Insiden Keamanan Informasi	Ya		<b>Draft</b> Kebijakan dan Prosedur Pengelolaan Insiden
11	Pemantauan (Monitoring) Sumber Daya TI: a. Monitoring Kapasitas b. Log Penggunaan User		Tdk	
12	Instalasi & Pengendalian Software	Ya		<b>Draft</b> Kebijakan dan Prosedur Instalasi Perangkat Lunak
13	Back-up & restore (prosedur/jadwal)		Tdk	

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

**Dokumen yang diperiksa:**

1. Pergub Jateng No. 45 Thn 2013 Tentang Penyelenggaraan TIK Pemprov Jateng
2. Pergub Jateng No. 70 Thn 2016 Tentang Organisasi dan Tata Kerja Dinas Komunikasi dan Informatika Provinsi Jawa Tengah
3. Pergub Jateng No. 89 Thn 2016 Tentang Sistem Manajemen Informasi Terintegrasi Pemprov Jateng
4. KepGub Jateng No. 550/36 Thn 2017 Tentang Pembentukan Tim Pengarah dan Tim Pelaksana Government Resources Management System (GRMS) Dalam Penyelenggaraan Pemerintahan Provinsi Jawa Tengah
5. Master Plan TI Pemerintah Provinsi Jawa Tengah 2018-2023

File-file Kebijakan dan Prosedur berikut, diperlihatkan kepada Tim Asesor dalam bentuk tampilan di layar presentasi. Seluruh file berikut ini dibuat pada tahun 2013 dan pada saat diperlihatkan masih dalam bentuk draft, belum disahkan oleh pejabat yang berwenang :

6. Kebijakan dan Prosedur Co-Location Server
7. Kebijakan dan Prosedur Klasifikasi dan Penanganan Informasi
8. Kebijakan dan Prosedur Pengamanan dan Pengelolaan Aset
9. Konteks dan Ruanglingkup SMKI
10. Kebijakan dan Prosedur Instalasi Perangkat Lunak
11. Kebijakan dan Prosedur Pengendalian Akses
12. Sasaran dan Rencana Kerja SMKI
13. Kebijakan dan Prosedur Pengelolaan Insiden
14. Kebijakan dan Prosedur Pengendalian Dokumentasi
15. Kebijakan dan Prosedur Kepatuhan Keamanan Informasi
16. Kebijakan dan Prosedur Peningkatan Pemahaman (Awerness) dan Komunikasi
17. Kebijakan dan Prosedur Keberlanjutan Bisnis dan Keamanan Informasi
18. Kebijakan dan Prosedur Pengukuran
19. Kebijakan dan Prosedur Audit Internal
20. Kebijakan dan Prosedur Manajemen Perubahan Fasilitas Data Center
21. Kebijakan dan Prosedur Keamanan Jaringan
22. Kebijakan dan Prosedur Tinjauan Manajemen
23. Kebijakan dan Prosedur Manajemen Kapasitas
24. Kebijakan dan Prosedur Penanganan Ketidaksesuaian dan Peningkatan
25. Kebijakan dan Prosedur Manajemen Risiko
26. Kebijakan dan Prosedur Pengelolaan Data Center
27. Kebijakan dan Prosedur Pengamanan Pihak Ketiga
28. Kebijakan dan Prosedur Keamanan Sumber Daya Manusia

**Bukti-bukti (rekaman/arsip) penerapan SMKI:**

Pada saat dilakukan Onsite Visit ke Data Center Dinas Kominfo Pemprov Jateng rekaman yang diperlihatkan adalah sbb:

1. Buku Tamu di Data Center
2. Buku aktivitas pemeliharaan Genset

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

**I. KONDISI UMUM:**

1. Struktur organisasi satuan kerja dalam ruang lingkup :
  - a. Dinas Komunikasi dan Informatika
  - b. Bidang Teknologi Informasi dan Komunikasi
    - » Seksi Infrastruktur dan Teknologi
    - » Seksi Data dan Integrasi Sistem Informasi
    - » Seksi Internet dan Intranet
  - c. Bidang E-Government
    - » Seksi Pengembangan Aplikasi
    - » Seksi Pengembangan Ekosistem E-Government
    - » Seksi Tata Kelola Government
  - d. Bidang Persandian dan Keamanan Informasi
    - » Seksi Tata Kelola Persandian
    - » Seksi Pengamanan Persandian dan Informasi
    - » Seksi Sistem Komunikasi Intra Pemerintah
2. SDM pengelola terdiri dari:
  - Total SDM di Bidang TIK sebanyak 25 orang
  - Total SDM di Bidang E-Government sebanyak 18 orang
  - Total SDM di Bidang Persandian dan Keamanan Informasi sebanyak 20 orang
3. Berdasarkan verifikasi terhadap hasil Self Assessment isian file Indeks KAMI diperoleh hasil sebagai berikut:

**Total Score Sebelum Verifikasi:** Pada tanggal 27 September 2017 sudah dilakukan verifikasi dengan ruang lingkup SPSE, dengan score indeks KAMI **sebesar 264.** (ref Laporan Pemeringkatan Indeks Keamanan Informasi Tahun 2017 dari Direktorat Keamanan Informasi Dirjen Aplikasi Informatika)

**Total Score Setelah Verifikasi: 274 (ref. file Indeks KAMI pasca Verifikasi)**

**Indeks KAMI (Keamanan Informasi)**



**II.KEKUATAN/KEMATANGAN:**

1. Aspek Ketersediaan Kerangka Kerja :
  1. Pimpinan Instansi sudah secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP)
  2. Sudah memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi
  3. Penanggungjawab pelaksanaan pengamanan informasi sudah diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi
  4. Sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi
2. Aspek Penerapan :
  1. Sudah ada daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlihara ? (termasuk kepemilikan aset )
  2. Sudah dilakukan proses pengecekan latar belakang SDM
  3. Sudah ada proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik
  4. Infrastruktur komputasi sudah terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya
  5. Infrastruktur komputasi yang terpasang sudah terlindungi dari gangguan pasokan listrik atau dampak dari petir
  6. Proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)
  7. Konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan sudah dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban)
  8. Sudah ada peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)

9. Sudah ada proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda
10. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan
11. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)
12. Infrastruktur jaringan, sistem dan aplikasi sudah dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada
13. Infrastruktur jaringan, sistem dan aplikasi sudah dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada
14. Setiap perubahan dalam sistem informasi sudah secara otomatis terekam di dalam log
15. Upaya akses oleh yang tidak berhak sudah secara otomatis terekam di dalam log
16. Sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses
17. Sudah menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi
18. Sudah menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi
19. Sudah terdapat laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan
20. Sudah menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yg dibangun

### **III. KELEMAHAN/KEKURANGAN:**

1. Aspek Kerangka Kerja
  1. Pelaksana pengamanan informasi sudah sebagian mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi
  2. Pelaksana pengamanan informasi sebagian telah memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku
  3. Penerapan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait sudah sebagian dilakukan
  4. Penerapan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi sudah sebagian dilakukan
  5. Integrasi keperluan/persyaratan keamanan informasi dalam proses kerja yang ada sudah sebagian dilakukan
  6. Identifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundungan yang berlaku sudah sebagian dilakukan
  7. Tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasi persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada sudah sebagian dilakukan
  8. Pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan

<p>pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak sudah sebagian dilakukan</p> <p>9. Penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi sudah sebagian dilakukan</p> <p>10. Kondisi dan permasalahan keamanan informasi sudah sebagian dilakukan menjadi konsideran atau bagian dari proses pengambilan keputusan strategis</p> <p>11. Pimpinan satuan kerja di Instansi anda sudah menerapkan sebagian program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya</p> <p>12. Metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya sudah didefinisikan sebagian</p> <p>13. Penerapan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat &amp; petugas) pelaksananya sudah sebagian dilakukan</p> <p>14. Pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan masih dalam perancanaan</p> <p>15. Tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) masih dalam perancanaan untuk didefinisikan dan dialokasikan</p> <p>16. Penerapan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi masih dalam perencanaan</p> <p>17. Identifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya masih dalam perencanaan</p> <p>18. Program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan masih dalam perencanaan</p> <p>19. Penetapan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan masih dalam perencanaan</p> <p>20. Kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan masih dalam perencanaan</p> <p>21. Penetapan ambang batas tingkat risiko yang dapat diterima masih dalam perencanaan</p> <p>22. Inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada masih dalam perencanaan (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)</p> <p>23. Kerangka kerja pengelolaan risiko ini belum mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian</p> <p>24. Belum mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?</p> <p>25. Ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama belum teridentifikasi</p> <p>26. Dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama belum ditetapkan sesuai dengan definisi yang ada</p>
--

- 27. Belum menyusun langkah mitigasi dan penanggulangan risiko yang ada
- 28. Langkah mitigasi risiko belum disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK
- 29. Status penyelesaian langkah mitigasi risiko belum dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya, serta dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya
- 30. Profil risiko berikut bentuk mitigasinya belum secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru
- 31. Kerangka kerja pengelolaan risiko belum secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya
- 32. Pengelolaan risiko belum menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan
- 33. Kebijakan keamanan informasi sudah sebagian ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya tetapi belum terdokumentasi
- 34. Sudah sebagian proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan
- 35. Aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga sudah diterapkan sebagian
- 36. Penerapan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggungjawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya sudah dilakukan sebagian
- 37. Penerapan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan sudah dilakukan sebagian
- 38. Kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya sudah dilakukan sebagian
- 39. 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 masih dalam perencanaan
- 40. Mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya masih dalam perencanaan
- 41. Strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda masih dalam perencanaan
- 42. Belum ada proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga
- 43. Keseluruhan kebijakan dan prosedur keamanan informasi yang ada, belum merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi
- 44. Konsekwensi dari pelanggaran kebijakan keamanan informasi belum didefinisikan, dikomunikasikan dan ditegakkan

45. Belum tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini
46. Belum membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup
47. Belum menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul
48. Perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) belum mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim
49. Uji-coba perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) belum dilakukan sesuai jadwal
50. Kebijakan dan prosedur keamanan informasi belum dievaluasi kelayakannya secara berkala
51. Belum mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi
52. Belum mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko
53. Belum memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)
54. Belum secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pemberian yang diperlukan, telah diterapkan secara efektif
55. Belum mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten

## 2. Aspek Penerapan

1. Definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku sudah diterapkan sebagian
2. Proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset dan keperluan pengamanannya sudah dilakukan sebagian
3. Sudah diterapkan sebagian definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut
4. Proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) sudah diterapkan sebagian
5. Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil sudah diterapkan sebagian
6. Tata tertib penggunaan komputer, email, internet dan intranet sudah diterapkan sebagian
7. Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI sudah diterapkan sebagian
8. Peraturan terkait instalasi piranti lunak di aset TI milik instansi sudah diterapkan sebagian
9. Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi sudah diterapkan sebagian
10. Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya sudah diterapkan sebagian

11. Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi sudah diterapkan sebagian
12. Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya sudah diterapkan sebagian
13. Daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya sudah diterapkan sebagian
14. Ketersediaan daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya sudah dilakukan sebagian
15. Sudah diterapkan sebagian pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang
16. Proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting sudah diterapkan sebagian
17. Proses pengelolaan konfigurasi yang diterapkan secara konsisten masih dalam perencanaan
18. Proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi masih dalam perencanaan
19. Pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya masih dalam perencanaan
20. Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi masih dalam perencanaan
21. Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data masih dalam perencanaan
22. Prosedur back-up dan ujicoba pengembalian data (restore) secara berkala masih dalam perencanaan
23. Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib masih dalam perencanaan
24. Prosedur penghancuran data/aset yang sudah tidak diperlukan masih dalam perencanaan
25. Peraturan pengamanan perangkat komputasi apabila digunakan di luar lokasi kerja resmi (kantor) masih dalam perencanaan
26. Konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan sudah diterapkan sebagian
27. Analisa kepatuhan penerapan konfigurasi standar yang ada sudah dilakukan sebagian
28. Jaringan, sistem dan aplikasi yang digunakan sudah sebagian dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi
29. Analisa log sudah sebagian dilakukan secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)
30. Penerapan enkripsi sudah sebagian dilakukan untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada
31. Sudah menerapkan sebagian pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya
32. Sistem operasi untuk setiap perangkat desktop dan server sudah sebagian dimutakhirkan dengan versi terkini
33. Keseluruhan jaringan, sistem dan aplikasi sudah sebagian menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada

- 34. Aplikasi yang ada sudah sebagian memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba
- 35. Akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis sudah dilakukan sebagian
- 36. Desktop dan server sudah sebagian dilindungi dari penyerangan virus (malware)
- 37. Sistem dan aplikasi belum secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama
- 38. Belum ada rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis
- 39. Pihak independen belum dilibatkan untuk mengkaji kehandalan keamanan informasi secara rutin

#### **IV. REKOMENDASI:**

Secara umum pelaksanaan Pengelolaan Keamanan Informasi di Dinas Kominfo Prov Jateng sudah berjalan baik, terutama pada aspek Tata Kelola dan aspek Teknologi.

Masih diperlukan adanya peningkatan pada aspek Kerangka Kerja agar nilai pada aspek ini dapat berada di atas ambang batas nilai yang dipersyaratkan oleh Indeks KAMI.

Demikian juga pada aspek Pengelolaan Risiko Keamanan Informasi, masih sangat diperlukan adanya pembuatan Kerangka Kerja Pengelolaan Risiko Keamanan Informasi dan Kajian Risiko Keamanan Informasi.

Beberapa dokumen prosedur sudah dibuat sejak tahun 2013, namun belum dilakukan pengesahan oleh pejabat yang berwenang. Hal tersebut disebabkan tidak ada personel atau fungsi yang ditunjuk secara khusus untuk menangani kegiatan SMKI ini secara berkesinambungan, terutama pada saat terjadinya reorganisasi sebagaimana tertuang pada Perhub 70 Tahun 2016.

Dari hasil assessment yang kami lakukan, kami merekomendasikan beberapa hal sebagai berikut :

1. Sebaiknya dibuat penugasan khusus kepada beberapa orang personel di Dinas Kominfo Prov Jateng yang mewakili bidang-bidang terkait dalam penerapan SMKI, yang dikordinasikan oleh Kepala Bidang Persandian dan Keamanan Informasi, untuk mengawal dan melakukan implementasi SMKI secara tahap demi tahap di lingkungan Dinas Kominfo Prov Jateng. Penugasan kepada beberapa personel ini dilakukan untuk memastikan adanya kesinambungan informasi dan aktifitas dalam penerapan SMKI. Dengan adanya penugasan ini juga diharapkan dapat membantu pimpinan dalam merangkai semua aktifitas yang diperlukan dalam penerapan SMKI menjadi sebuah gambaran utuh, sehingga keterhubungan antar fungsi di Bagian dan Seksi dapat dipetakan secara jelas.
2. Segera melakukan pengesahan atas dokumen-dokumen Kebijakan dan Prosedur yang masih dalam bentuk draft, dengan ditandatangani oleh pejabat yang berwenang.
3. Memenuhi aktivitas yang belum atau baru dilaksanakan sebagian di Aspek Kerangka Kerja, antara lain:
  1. Penerapan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi.

2. Identifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya.
3. Membuat program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
4. Penetapan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan.
5. Membuat kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
6. Penetapan ambang batas tingkat risiko yang dapat diterima.
7. Inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada. (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)
8. Membuat kerangka kerja pengelolaan risiko yang mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugiannya.
9. Mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
10. Melakukan identifikasi ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama.
11. Menetapkan dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama.
12. Menyusun langkah mitigasi dan penanggulangan risiko yang ada
13. Menyusun langkah mitigasi risiko sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK
14. Pemantauan secara berkala status penyelesaian langkah mitigasi risiko, untuk memastikan penyelesaian atau kemajuan kerjanya, serta dievaluasi melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya
15. Pengkajian secara berkala profil risiko berikut bentuk mitigasinya untuk memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru
16. Pengkajian secara berkala Kerangka kerja pengelolaan risiko untuk memastikan/meningkatkan efektifitasnya
17. Memasukkan pengelolaan risiko sebagai bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan
18. Mendokumentasikan kebijakan keamanan informasi secara formal, mempublikasikan kepada semua staf/karyawan termasuk pihak terkait dan membuat mudah diakses oleh pihak yang membutuhkannya.
19. Penerapan secara konsisten kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggungjawab untuk memonitor adanya rilis security patch baru, dan memastikan pemasangannya.
20. Melakukan penerapan proses pengembangan sistem yang aman (Secure SDLC) dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan pada setiap aktifitas pengembangan aplikasi.
21. Membuat mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.

22. Membuat proses sosialisasi yang mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya, untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga.
23. Keseluruhan kebijakan dan prosedur keamanan informasi yang ada, harus merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi
24. Membuat prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini
25. Membuat kajian atas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup
26. Dalam pembuatan prosedur pemulihan bencana terhadap layanan TIK (disaster recovery plan) agar mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim
27. Melakukan evaluasi kelayakan secara berkala atas Kebijakan dan prosedur keamanan informasi.
28. Membuat strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko
29. Melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)
30. Agar secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pemberian yang diperlukan, telah diterapkan secara efektif
4. Melakukan aktivitas yang belum dilaksanakan atau baru dilaksanakan sebagian di Aspek Penerapan, antara lain:
1. Membuat proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
  2. Menerapkan pengelolaan identitas elektronik dan proses otentikasi (username & password) termasuk kebijakan terhadap pelanggarannya
  3. Menerapkan persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
  4. Menetapkan waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data
  5. Menetapkan Prosedur back-up dan ujicoba pengembalian data (restore) secara berkala
  6. Menetapkan Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib
  7. Menetapkan Prosedur penghancuran data/aset yang sudah tidak diperlukan masih
  8. Menetapkan Peraturan pengamanan perangkat komputasi apabila digunakan di luar lokasi kerja resmi (kantor)
  9. Menerapkan sistem dan aplikasi yang secara otomatis mendukung dan menerapkan penggantian password secara otomatis, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama
  10. Melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin

<p>Jakarta, 1 November 2018 Narasumber : Dinas Kominfo Prov Jateng : 1. Eny Soelastri, SH.  2. Eka Suprapti, ST,MM.  3. Toto Sumarmo, S.Sos, M.Kom </p>	<p>Assessor Indeks KAMI: 1. Assessor Utama: <b>Egia Kerta Anggara</b>  2. Assessor Pendamping: Rakean Bagus M.R  3. Assessor Pendamping: <b>Eduar Fardji</b> </p>
--	--