
	LAPORAN ONSITE ASSESSMENT INDEKS KAMI	 INDEKS KEAMANAN INFORMASI
Instansi/Perusahaan: PEMERINTAH PROVINSI DKI JAKARTA	Pimpinan Unit Kerja : Atika Nur Rahmania, S.IP, M.Si 19720406 199803 2 006	
Unit Kerja: DINAS KOMUNIKASI, INFORMATIKA, DAN STATISTIK	Narasumber Instansi : 1. R. Boedi Setiawan, S.H, 197009171998031006 2. Reyhan Adinata, 198510132010011020	
Alamat: Jl. Medan Merdeka Selatan no 8-9 Blok H Lantai 13, Jakarta Pusat 10110	3. Andrie Yuswanto, 19781231 201101 1 014 4. Tony Yudianto, 19820227201001102 5. Rycan Fahmi, 198101032011011013 6. Tanti Widyaningrum, 198504012010012038 7. Lamria Simatupang, 198601272011012009 8. Andy Susanto, 198107282011011005 9. M. Taufik Hidayat, 197610192007011009 10. Iman Pribadi, 197706062006041024 11. Venny Yulianty, 198507192014032002 12. Arif Buchari Marpaung, 198801132015041002 13. Novaldo Caesar, 199111162022031005 14. Rina Yuliani Fadila	
Email: diskominfotik@jakarta.go.id	Asesor : 1. Marcelina Tri N. W., S.Sos., M.Si (han) 19750717 199412 2 001	
Tel/ Fax: (021) 3822357	2. Irma Nurfitri Handayani, S.ST. 19850303 200501 2 002 3. Aprita Danang P., S.ST., M.Kom. 19870412 200701 1 002 4. Carissa Mega Yulianingrum, S.Tr.TP 19930720 201611 2 001	

A. Ruang Lingkup:

1. Instansi / Unit Kerja:

Dinas Komunikasi, Informatika, dan Statistik Provinsi DKI Jakarta.

2. Fungsi Kerja:

Sebagaimana Peraturan Gubernur Provinsi DKI Jakarta Nomor 144 Tahun 2019 tentang Organisasi dan Tata Kerja, Dinas Komunikasi, Informatika, dan Statistik, Dinas Kominfo dan Statistik mempunyai tugas melaksanakan urusan pemerintahan di bidang komunikasi dan informatika, statistik, dan persandian. Untuk menyelenggarakan tugas sebagaimana dimaksud pada ayat (1), Dinas Kominfo dan Statistik menyelenggarakan fungsi:

- penyusunan rencana strategis dan rencana kerja dan anggaran Dinas Kominfo dan Statistik;
- pelaksanaan rencana strategis dan dokumen pelaksanaan anggaran Dinas Kominfo dan Statistik;
- pelaksanaan penyiapan perumusan dan pelaksanaan kebijakan di bidang komunikasi dan informatika, statistik, dan persandian;
- penyusunan norma, standar, prosedur dan kriteria di bidang komunikasi dan informatika, statistik, dan persandian;
- pemberian bimbingan teknis dan supervisi, serta pamaritauan, evaluasi, dan pelaporan di bidang komunikasi dan informatika, statistik, dan persandian; dan
- pelaksanaan fungsi lain di dalam peraturan Gubernur Provinsi DKI Jakarta Nomor 144 Tahun 2019.

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor Pusat	Jl. Medan Merdeka Selatan no 8-9 Blok H Lantai 13, Jakarta Pusat 10110
2	<i>Data Center</i>	Jl. Medan Merdeka Selatan no 8-9 Blok G Lantai 3, Jakarta Pusat 10110
3	<i>Disaster Recovery Center (DRC)</i>	Telkom, Bandung

B. Nama /Jenis Layanan Publik:

Operasional Perangkat Keamanan Jaringan (Bidang Siber dan Sandi, Dinas Komunikasi, Informatika dan Statistik, Pemerintah Provinsi DKI Jakarta).

C. Aset TI yang kritikal:

1. Informasi:
 - a. NIP;
 - b. NIK;
 - c. Berkas-berkas bersifat terbatas, rahasia, dan rahasia yang dimasukkan ke dalam sistem.
2. Aplikasi:

aplikasi TPP (<https://etpp.jakarta.go.id>)
3. Server :

server di data center dan pendukungnya.
4. Infrastruktur Jaringan/Network:

Internet dan Intranet

D. DATA CENTER (DC):

- ☒ ADA, dalam ruangan khusus (Ruang server dikelola internal)
- ☐ ADA, jadi satu dengan ruang kerja
- ☐ TIDAK ADA

E. DISASTER RECOVERY CENTER (DRC):

- ☐ ADA ☐ Dikelola Internal ☒ Dikelola Vendor :
- ☐ TIDAK ADA

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

No	Nama Dokumen	Ya	Tdk	Keterangan (D: Draf, R:Rilis, T:Tersosialisasikan)
	Kebijakan, Sasaran, Rencana, Standar			
1	Kebijakan Keamanan Informasi	Ya		Rilis Internal
2	Organisasi, Peran dan Tanggungjawab Keamanan Informasi	Ya		R
3	Panduan Klasifikasi Informasi	Ya		R
4	Kebijakan Manajemen Risiko TIK	Ya		R
5	Kerangka Kerja Manajemen Kelangsungan Usaha (Business Continuity Management)	Ya		R
6	Kebijakan Penggunaan Sumberdaya TIK	Ya		R
	Prosedur/ Pedoman:			
1	Pengendalian Dokumen	Ya		R
2	Pengendalian Rekaman/Catatan	Ya		R
3	Audit Internal SMKI	Ya		R
4	Tindakan Perbaikan & Pencegahan	Ya		R
5	Pelabelan, Pengamanan, Pertukaran & Disposal Informasi	Ya		R
6	Pengelolaan Removable Media & Disposal Media	Ya		R
7	Pemantauan (Monitoring) Penggunaan Fasilitas TIK	Ya		R
8	User Access Management	Ya		R
9	Teleworking	Ya		R
10	Pengendalian instalasi software & HAKI	Ya		R

11	Pengelolaan Perubahan (Change Management) TIK	Ya		R
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi	Ya		R

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

Dokumen yang diperiksa:

1. Peraturan Gubernur DKI Jakarta Nomor 144 Tahun 2019 tentang Organisasi dan Tata Kerja Dinas Komunikasi dan Informatika Provinsi DKI Jakarta.
2. Peraturan Gubernur DKI. Jakarta Nomor 5 Tahun 2022 tentang klasifikasi Informasi yang dikecualikan.
3. Keputusan Gubernur no 1599 Tahun 2021 tentang Jadwal Retensi Arsip.
4. Peraturan Sekretaris Daerah Nomor 31 SE Tahun 2019 tentang Kebijakan Perlindungan Data Pribadi Dalam Sistem Elektronik Di Lingkungan Pemerintah Provinsi Daerah Khusus Ibukota Jakarta.
5. Dokumen Kebijakan Manual Keamanan Informasi Nomor DKIS.SMKI.MKI.01.
6. Surat Keputusan Tim Keamanan Informasi Nomor DKIS.SMKI.MKI.LAM.05.
7. Surat Keputusan Tim Business Continuity Plan DKIS.SMKI.MKI.LAM.06.
8. Keputusan Kepala Dinas Kominfotik No 31 Tahun 2021 tentang Bussines Continuity Plan (BCP).
9. Dokumen DPA No 105/DPA/2022 Penyelenggaraan Siber dan Sandi Pemerintah Provinsi DKI Jakarta.
10. Dokumen Rencana Strategis Dinas Komunikasi dan Informatika Provinsi DKI Jakarta Tahun 2023-2026.
11. Dokumen Non-disclosure Agreement (NDA) dengan pihak ketiga.
12. Perkin Dinas Komunikasi dan Informatika Pemerintah Provinsi DKI Jakarta Tahun 2022.
13. Prosedur Pengendalian Informasi Terdokumentasi Nomor DKIS.SMKI.SOP.01
14. Prosedur Internal Audit Nomor DKIS.SMKI.SOP.03.
15. Prosedur Tinjauan Manajemen Nomor DKIS.SMKI.SOP.04.
16. Prosedur Kepatuhan Peraturan Nomor DKIS.SMKI.SOP.05.
17. Prosedur Manajemen Resiko Nomor DKIS.SMKI.SOP.06.
18. Prosedur Komunikasi Nomor DKIS.SMKI.SOP.07.
19. Prosedur Monitoring Operasional Jaringan Nomor DKIS.SMKI.SOP.09.
20. Prosedur Seleksi Dan Penerimaan Pegawai Nomor DKIS.SMKI.SOP.10.

21. Prosedur Pengendalian Akses Fisik Nomor DKIS.SMKI.SOP.14.
22. Prosedur Pengendalian Akses Non Fisik Nomor DKIS.SMKI.SOP.15.
23. Prosedur Backup Dan Restore Nomor DKIS.SMKI.SOP.17.
24. Prosedur Pengelolaan Aset Nomor DKIS.SMKI.SOP.18.
25. Prosedur Pemeliharaan Dan Perbaikan Nomor DKIS.SMKI.SOP.19.
26. Prosedur Manajemen Kapasitas Nomor DKIS.SMKI.SOP.20.
27. Prosedur Manajemen Perubahan Nomor DKIS.SMKI.SOP.21.
28. Prosedur Manajemen Insiden Nomor DKIS.SMKI.SOP.22.
29. Prosedur Manajemen Keberlangsungan Nomor DKIS.SMKI.SOP.23.
30. Prosedur Hak Akses Jarak Jauh Vendor Nomor DKIS.SMKI.SOP.26.
31. Prosedur No 60 Tahun 2020 tentang SOP Bidang Sistem Informasi Manajemen: Bagian SOP Perancangan Sistem Informasi.
32. Formulir Risk Assessment Diskominfo DKI Jakarta Tahun 2021.
33. Laporan Penyelenggaraan Persandian Tahun 2020.
34. Laporan Pentest 2021.
35. Update Data SDM BSS Februari 2022.
36. Laporan Audit Keamanan Informasi Internal.
37. Laporan Simulasi Fortinet Tanggal 12 Agustus 2021.
38. Dokumen Usulan Perubahan Dokumen ISO 2021.
39. KAK Pengadaan Perangkat Keamanan Jaringan.
40. Nota Dinas ND/18.1.BSS/VI/2022 tanggal 23 Juni 2022 tentang Laporan Monitoring Opearional Perangkat Keamanan Jaringan.
41. Laporan Analisis Kebutuhan Hardware/Software tahun 2022.
42. Dokumen No. 34/BSS/XII/2021 tanggal 31 Desember 2021 Laporan Persentase Perangkat Daerah Provinsi Menggunakan Layanan Kaminfo.
43. Laporan Insiden Siber ke BSSN Tahun 2022.
44. Laporan Ransomware Sudin Utara.

Bukti-bukti (rekaman/arsip) penerapan SMKI:

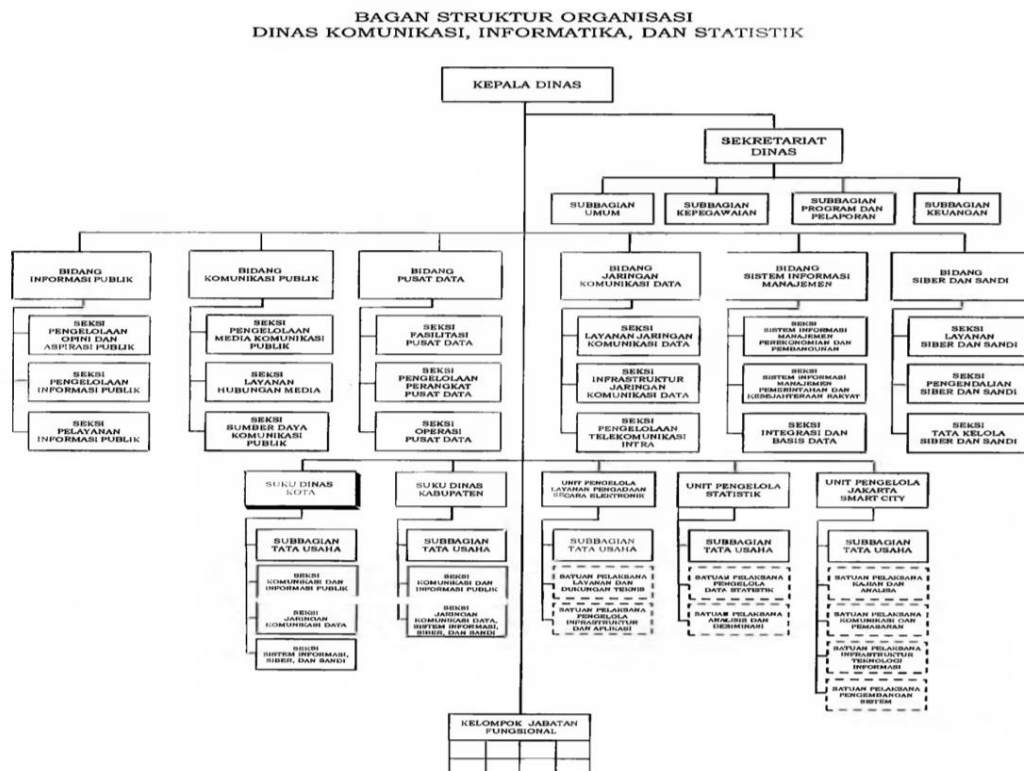
1. Daftar Peraturan Keamanan Informasi DKIS.SMKI.FM.05.03 tanggal 26 Agustus 2019.
2. Matriks Kompetensi Personil Diskominfo Provinsi DKI Jakarta Tahun 2021;
3. Formulir Status Temuan Audit Internal
4. Tangkapan Layar Aplikasi e-TPP.
5. Rencana dan Jadwal Rapat Tinjauan Manajemen.

6. Notulen Tinjauan Manajemen
7. Statement Of Applicability (SOA)
8. Tabel Komunikasi Internal
9. Tabel Komunikasi Eksternal
10. Jadwal Komunikasi Internal
11. Formulir Status Temuan Audit Internal.
12. Notulen Rapat Tinjauan Manajemen Tahun 2021.
13. Evaluasi Kebijakan Kontrol Keamanan Informasi.
14. Formulir Aset Register Peralatan.

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

I. KONDISI UMUM:

1. Diskominfo Provinsi DKI Jakarta dibentuk berdasarkan Peraturan Gubernur Provinsi DKI Jakarta Nomor 144 Tahun 2019 tentang Organisasi dan Tata Kerja, Dinas Komunikasi, Informatika, dan Statistik. Adapun struktur Diskominfo dan Statistik Provinsi DKI Jakarta adalah sebagai berikut:



Gambar 1. Struktur Organisasi Diskominfo dan Statistik Provinsi DKI Jakarta

2. SDM ASN Diskominfo dan Statistik Provinsi DKI Jakarta berjumlah 261 orang.

Berdasarkan verifikasi terhadap hasil Self Assessment isian file Indeks KAMI diperoleh hasil sebagai berikut:

Penilaian Mandiri Indeks KAMI dilakukan di tahun 2022 dengan ruang lingkup Diskominfo Provinsi DKI Jakarta, dilakukan verifikasi oleh Tim BSSN dengan kategori Sistem Elektronik **STRATEGIS** dan hasil evaluasi akhir **BAIK** dengan total nilai **631**.

Pada Tahun 2022 ini merupakan penilaian kedua bagi Diskominfo Provinsi DKI Jakarta, sebelumnya dilakukan penilaian Indeks KAMI Tahun 2018 oleh Tim BSSN. Verifikasi oleh Tim BSSN dalam penilaian mandiri Indeks KAMI setelah melakukan pengecekan keseluruhan kelengkapan kebijakan dan/atau prosedur dan penerapan dokumen kebijakan dan/atau prosedur pada area Kategori, Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, dan Teknologi.

Tim penilaian tahun 2022 berfokus kepada satu Sistem Elektronik yang dikelola oleh Diskominfo Provinsi DKI Jakarta dengan kategori strategis yaitu: Sistem Elektronik TPP.

Total Score Verifikasi Penilaian Indeks KAMI Tahun 2018: 285

Total Score Setelah Verifikasi: 285 (ref. file Indeks KAMI pasca Verifikasi)

Hasil Evaluasi Akhir:

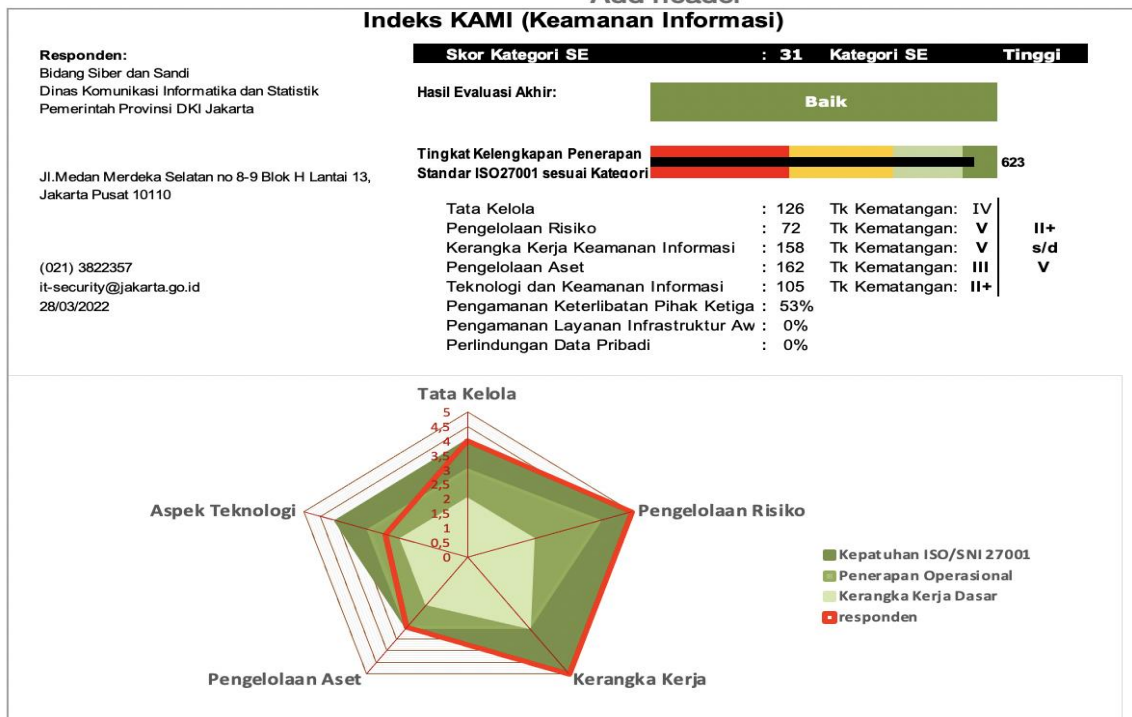
Tidak Layak

Tingkat Kelengkapan Penerapan Standar ISO27001 sesuai

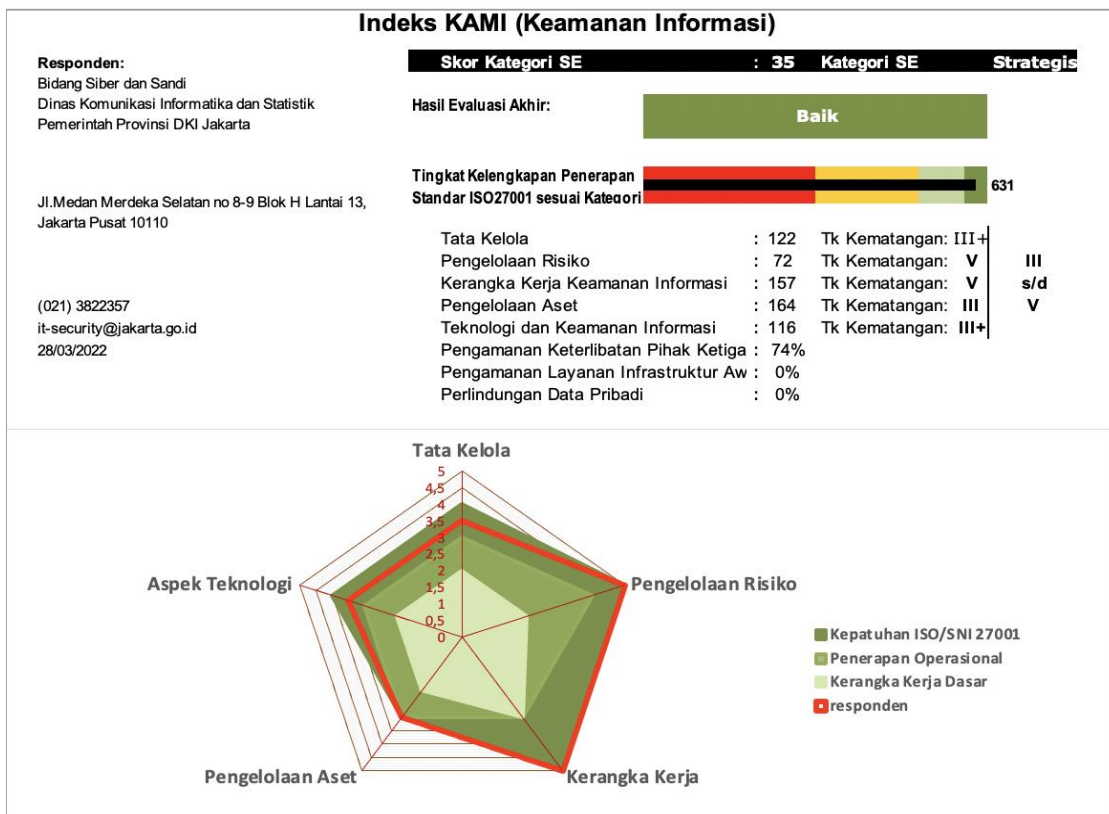
285

Skor Kategori SE	: 32	Kategori SE		Tinggi
Tata Kelola	: 69	Tk Kematangan:	II	
Pengelolaan Risiko	: 10	Tk Kematangan:	I	I
Kerangka Kerja Keamanan Informas	: 46	Tk Kematangan:	I+	s/d
Pengelolaan Aset	: 78	Tk Kematangan:	II	II
Teknologi dan Keamanan Informasi	: 82	Tk Kematangan:	II	

Total Score Self Assessment Penilaian Indeks KAMI Tahun 2022 Sebelum Verifikasi: 623



Total Score Verifikasi Penilaian Indeks KAMI Tahun 2022 Setelah Verifikasi: 631



II. ASPEK TATA KELOLA:

A. Kekuatan/Kematangan

1. Pimpinan dari Diskominfo Provinsi DKI Jakarta sudah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen diantaranya sudah ada penetapan kebijakan-kebijakan terkait SMKI.
2. Diskominfo Provinsi DKI Jakarta sudah menetapkan fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab dalam mengelola dan mengimplementasikan program keamanan informasi dan memastikan kepatuhannya.
3. Pejabat/petugas pelaksana pengamanan informasi sudah ditunjuk di dalam organisasi yang mempunyai wewenang untuk mengimplementasikan program keamanan informasi yang akan dilaksanakan.
4. Alokasi sumber daya terkait pelaksanaan program keamanan informasi sudah direncanakan dan disediakan dalam rangka memastikan pengelolaan keamanan informasi telah memadai dan dipastikan kepatuhannya.
5. Diskominfo Provinsi DKI Jakarta sudah mendefinisikan persyaratan/standar kompetensi dan keahlian khususnya terkait pelaksana pengelolaan keamanan informasi.
6. Semua pelaksana pengamanan informasi yang terlibat di Diskominfo Provinsi DKI Jakarta sudah memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku khususnya terkait aspek kontrol teknis dan operasional keamanan informasi.
7. Manajemen Diskominfo Provinsi DKI Jakarta dan fungsi pengelola keamanan informasi sudah merencanakan dan menerapkan program sosialisasi dan peningkatan pemahaman terhadap keamanan informasi melalui media sosial dan dievaluasi hasil penerapannya untuk memastikan kepatuhannya bagi semua pihak yang terkait.
8. Diskominfo Provinsi DKI Jakarta sudah menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi dengan merencanakan secara berkala minimal setiap tahun dalam rangka memastikan kebutuhan penerapan kontrol keamanan informasi telah terpenuhi.
9. Beberapa persyaratan keamanan informasi yang terdapat dalam standard yang berlaku sudah terintegrasi kedalam proses kerja yang ada namun sebagian lainnya masih bersifat aktivitas kontrol tambahan yang dilakukan.
10. Diskominfo Provinsi DKI Jakarta sudah mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku.
11. Tanggung jawab pengelolaan keamanan informasi yang didelegasikan kepada fungsi pengelola keamanan informasi sudah mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, dan untuk mengidentifikasi persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada.

12. Koordinasi antara fungsi pengelola keamanan informasi dengan satker 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 masih belum konsisten dan terlaksana secara memadai.
13. Tanggung jawab terhadap pengelolaan langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans) sebagian dirancang dalam dokumentasi yang ada. Hal ini termasuk pengalokasian kebutuhan sumber daya dan proses yang diperlukan dalam rangka menjamin kelangsungan bisnis ketika terjadi kondisi darurat yang telah ditetapkan oleh manajemen.
14. Fungsi pengelola keamanan informasi sudah melaporkan kepada manajemen mengenai sebagian dari kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi secara rutin.
15. Setiap permasalahan keamanan informasi yang terjadi di Diskominfo Provinsi DKI Jakarta sudah menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis dalam melakukan tindakan perbaikan yang diperlukan untuk meningkatkan efektifitas pelaksanaan kontrol keamanan informasi.
16. Diskominfo Provinsi DKI Jakarta sudah menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya.
17. Metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi sudah didefinisikan yang mencakup mekanisme, waktu pengukuran, pelaksanaannya, dan harus diukur dan dievaluasi pemantauannya secara berkala serta dilakukan eskalasi pelaporan kepada manajemen untuk memastikan efektifitas dari proses pengelolaan program dan kontrol keamanan informasi yang diterapkan.
18. Diskominfo Provinsi DKI Jakarta sudah mendefinisikan dan menerapkan program penilaian kinerja terkait penerapan proses keamanan informasi bagi individu (pejabat & petugas) pelaksanaannya sebagai bagian dari proses evaluasi tingkat pemahaman individu tersebut terhadap pengelolaan keamanan informasi di organisasi.
19. Target dan sasaran pengelolaan keamanan informasi sudah didefinisikan dan diformulasikan, serta dilakukan evaluasi dan mengkaji hasil pencapaiannya secara rutin. Laporan hasil evaluasi terhadap target dan sasaran tersebut telah dilaporkan statusnya kepada pimpinan organisasi.
20. Manajemen Diskominfo Provinsi DKI Jakarta mendelegasikan pihak terkait / unit kerja / fungsi pengelola keamanan informasi pada internal Diskominfo Provinsi DKI Jakarta untuk mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi serta dipastikan untuk dipatuhi dengan menganalisa tingkat kepatuhannya.

B. Kelemahan/Kekurangan

1. Peran fungsi pelaksana pengamanan informasi sudah dipetakan terkait pengelolaan program keamanan informasi namun belum dilaksanakan secara menyeluruh melibatkan Bidang-Bidang lain dalam lingkup Diskominfo Provinsi

- DKI Jakarta, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan.
2. Manajemen Diskominfo Provinsi DKI Jakarta belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

III. ASPEK RISIKO:

A. Kekuatan/Kematangan

1. Program kerja pengelolaan risiko keamanan informasi sudah terdokumentasi dan diterapkan secara memadai dalam proses penilaian dan evaluasi risiko.
2. Manajemen Diskominfo Provinsi DKI Jakarta sudah menentukan penanggung jawab proses manajemen risiko yang berwenang dalam eskalasi terhadap pelaporan hasil analisa risiko keamanan informasi sampai ke tingkat pimpinan organisasi
3. Kerangka kerja pengelolaan risiko keamanan informasi sudah terdokumentasi dalam dokumen metodologi manajemen risiko sehingga dapat digunakan secara resmi.
4. Kerangka kerja pengelolaan risiko sudah mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian di Diskominfo Provinsi DKI Jakarta.
5. Ambang batas tingkat risiko yang dapat diterima sudah ditetapkan oleh manajemen Diskominfo Provinsi DKI Jakarta dalam rangka melakukan evaluasi terhadap tingkatan risiko yang dianalisa.
6. Dalam proses pengelolaan manajemen risiko, Diskominfo Provinsi DKI Jakarta sudah terdapat pendefinisian mengenai kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
7. Ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi.
8. Pada proses analisa risiko sudah ditetapkan mengenai dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sesuai dengan definisi yang ada.
9. Proses pengkajian ulang profil risiko dan pengkajian ulang kerangka kerja pengelolaan risiko untuk memastikan/meningkatkan efektivitasnya sudah menjadi sebuah perhatian khusus. Profil risiko berikut bentuk mitigasinya sudah secara berkala dikaji ulang dalam rangka memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut.
10. Status penyelesaian langkah mitigasi risiko sudah dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya.
11. Profil risiko berikut bentuk mitigasinya sudah secara berkala dikaji ulang dalam rangka memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru.

12. Langkah-langkah mitigasi dan penanggulangan risiko yang ada sudah disusun sesuai dengan kebutuhan rencana yang jelas.
13. Langkah mitigasi risiko sesuai target penyelesaiannya diprioritaskan serta penanggungjawabnya ditentukan, mekanisme untuk memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK sudah diterapkan.
14. Kerangka kerja pengelolaan risiko sudah secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya.
15. Pengelolaan risiko sudah menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan.
16. Sudah terdapat proses evaluasi yang obyektif/terukur terhadap penyelesaian langkah mitigasi yang telah diterapkan untuk memastikan konsistensi dan efektifitasnya.

B. Kelemahan/Kekurangan

-

IV. ASPEK KERANGKA KERJA:

A. Kekuatan/Kematangan

1. Sudah adanya proses untuk mengidentifikasi kondisi yang membahayakan keamanan kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan didokumentasikan dengan jelas, termasuk peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya.
2. Kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya.
3. Mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya sudah diatur dan didokumentasikan secara formal.
4. Sudah adanya proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga.
5. Kebijakan dan prosedur keamanan informasi yang sudah ditetapkan sudah merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang telah ditetapkan.
6. Sudah adanya proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkan sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan.
7. Kontrak dengan pihak ketiga sudah mencakup aspek-aspek kontrol keamanan informasi seperti proses pelaporan insiden, keharusan menjaga kerahasiaan, penggunaan perangkat lunak yang berlisensi (HAKI), dan tata tertib penggunaan dan pengamanan aset maupun layanan TIK.

8. Konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan pada seluruh pegawai dan pihak ketiga.
9. Diskominfo Provinsi DKI Jakarta sudah menetapkan dan menerapkan kebijakan dan prosedur operasional terkait implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, hingga pelaporannya.
10. Aspek keamanan informasi sudah diidentifikasi untuk beberapa aktivitas proyek selama proses manajemen proyek dan sudah tertuang dalam dokumentasi.
11. Evaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul sudah dilakukan.
12. Proses pengembangan sistem yang aman (Secure SDLC) sudah menerapkan prinsip atau metode sesuai standar platform teknologi yang digunakan.
13. Ketika terdapat penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, Diskominfo Provinsi DKI Jakarta sudah terdapat proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya.
14. Uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal.
15. Hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dievaluasi. Langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal)) sudah ditetapkan secara jelas dalam suatu dokumentasi yang resmi.
16. Kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mencakup persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya sudah disusun dan didokumentasikan.
17. Perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mencakup mengenai komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk.
18. Seluruh kebijakan dan prosedur keamanan informasi sudah dievaluasi kelayakannya secara berkala.
19. Strategi penerapan keamanan informasi sudah dirumuskan dan ditetapkan sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi.
20. Strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko sudah ditetapkan secara resmi.
21. Strategi penerapan keamanan informasi sudah direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi.
22. Diskominfo Provinsi DKI Jakarta sudah menetapkan 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).

23. Audit internal sudah mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi.
24. Hasil audit internal secara rutin dikaji/dievaluasi terkait langkah pembenahan dan pencegahan yang diperlukan, ataupun inisiatif peningkatan kinerja keamanan informasi.
25. Hasil audit internal sudah dilaporkan kepada pimpinan organisasi dan sudah ditetapkan langkah-langkah perbaikan atau program peningkatan kinerja keamanan informasi.
26. Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, sudah terdapat proses dalam melakukan analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya.
27. Diskominfo Provinsi DKI Jakarta sudah 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 pembenahan yang diperlukan, telah diterapkan secara efektif.
28. Rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) sudah direalisasikan secara konsisten.

B. Kelemahan/Kekurangan

1. Belum adanya tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini.

V. ASPEK PENGELOLAAN ASET:

A. Kekuatan/Kematangan

1. Daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi sudah didokumentasikan secara lengkap, akurat dan terpelihara (termasuk kepemilikan aset).
2. Definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku sudah didefinisikan.
3. Proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Diskominfo Provinsi DKI Jakarta dan keperluan pengamanannya sudah didefinisikan dan ditetapkan secara resmi.
4. Definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut sudah didokumentasikan.
5. Sudah adanya proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi).
6. Sudah tersedianya proses pengelolaan konfigurasi yang diterapkan secara konsisten.
7. Sudah ditetapkannya proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.

8. Sudah adanya definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Diskominfo Provinsi DKI Jakarta.
9. Sudah adanya tata tertib penggunaan komputer, email, internet dan intranet.
10. Sudah ditetapkan tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI.
11. Telah ada aturan terkait instalasi piranti lunak di aset TI milik Diskominfo Provinsi DKI Jakarta.
12. Telah diatur mengenai penggunaan data pribadi yang mensyaratkan pemberian izin tertulis oleh pemilik data pribadi.
13. Telah ada proses mengenai pengelolaan identitas elektronik dan proses otentikasi (*username & password*) termasuk kebijakan terhadap pelanggarannya.
14. Sudah ditetapkan persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
15. Telah ada ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data.
16. Sudah ada ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya
17. Sudah tersedianya proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi.
18. Sudah ada prosedur untuk proses *back-up* dan uji coba pengembalian data (*restore*) secara berkala.
19. Sudah adanya ketentuan mengenai pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya.
20. Sudah berjalannya proses pengecekan latar belakang SDM.
21. Sudah dilakukan mekanisme terkait pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib sudah tertuang dalam dokumentasi.
22. Telah ada prosedur penghancuran data/aset yang sudah tidak diperlukan.
23. Sudah tersedianya prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya (*user access rights*) berikut langkah pembenahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku.
24. Sudah ada ketentuan dan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/*outsourc*e yang habis masa kerjanya
25. Daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya sudah didokumentasikan.
26. Sudah terdokumentasinya daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
27. Pengamanan fasilitas fisik (lokasi kerja) sudah diterapkan sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang.
28. Sudah ada proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik sudah jelas mekanismenya.
29. Infrastruktur komputasi telah terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya.

30. Infrastruktur komputasi yang terpasang sebagian telah terlindungi dari gangguan pasokan listrik atau dampak dari petir.
31. Sudah ditetapkan proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris).
32. Konstruksi ruang penyimpanan perangkat pengolah informasi penting sebagian sudah menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai.
33. Sudah adanya proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting.
34. Sudah ada mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
35. Sudah didefinisikan dan ditetapkan 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).
36. Sudah adanya proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Diskominfo DKI Jakarta.

B. Kelemahan/Kekurangan

1. Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan belum ditetapkan dan didokumentasikan.
2. Belum ditetapkan peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor).

VI. ASPEK TEKNOLOGI:

A. Kekuatan/Kematangan

1. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan.
2. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll).
3. Konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi sudah didokumentasikan dan dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan.
4. Analisa kepatuhan penerapan konfigurasi standar yang ada sudah dianalisa secara berkala.

5. Jaringan, sistem dan aplikasi yang digunakan secara rutin sudah dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi.
6. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada.
7. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada.
8. Setiap perubahan dalam sistem informasi sudah direkam pada suatu log pada sistem.
9. Upaya akses oleh yang tidak berhak sudah terekam di dalam log.
10. Semua log sudah dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik).
11. Diskominfo Provinsi DKI Jakarta sudah menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada.
12. Diskominfo Provinsi DKI Jakarta sudah mempunyai standar dalam menggunakan enkripsi.
13. Pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya sudah diterapkan.
14. Akses yang digunakan untuk mengelola sistem (administrasi sistem) sudah menggunakan bentuk pengamanan khusus yang berlapis.
15. Pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi sudah diterapkan.
16. Sudah ada proses untuk menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan.
17. Sistem operasi untuk setiap perangkat desktop dan server sudah dimutakhirkan dengan versi terkini.
18. Setiap desktop dan server telah dilindungi dari penyerangan virus (malware).
19. Sudah tersimpannya rekaman dan hasil analisa (jejak audit - audit trail) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis.
20. Sudah adanya proses pelaporan penyerangan virus/malware yang gagal/sukses yang ditindaklanjuti dan diselesaikan.
21. Keseluruhan jaringan, sistem dan aplikasi sudah tersinkronisasi waktu yang akurat, sesuai dengan standar yang ada.
22. Aplikasi yang ada telah memiliki dokumentasi mengenai spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba.
23. Lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun telah diterapkan.
24. Diskominfo Provinsi DKI Jakarta telah melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin.

B. Kelemahan/Kekurangan

1. Sebagian sistem dan aplikasi belum secara otomatis menerapkan manajemen dalam penggantian password secara otomatis pada sistem, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama.
2. Sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, namun belum melakukan logout setelah kegagalan login, dan penarikan akses.

VII. REKOMENDASI

1. Peran fungsi pelaksana pengamanan informasi sudah dipetakan terkait pengelolaan program keamanan informasi namun belum dilaksanakan secara menyeluruh melibatkan Bidang-Bidang lain dalam lingkup Diskominfo Provinsi DKI Jakarta, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan.
2. Manajemen Diskominfo Provinsi DKI Jakarta belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).
3. Belum adanya tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekuensi dari kondisi ini.
4. Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan belum ditetapkan dan didokumentasikan.
5. Belum ditetapkannya peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor).
6. Sebagian sistem dan aplikasi belum secara otomatis menerapkan manajemen dalam penggantian password secara otomatis pada sistem, termasuk menon-aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama.
7. Sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, namun belum melakukan logout setelah kegagalan login, dan penarikan akses.

VIII. PENUTUP

Demikian Laporan *Onsite Assessment* Indeks KAMI Diskominfo Provinsi DKI Jakarta T.A. 2022 ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan informasi Diskominfo Provinsi DKI Jakarta.

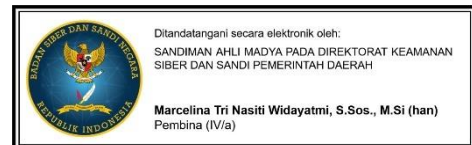
Laporan *Onsite Assessment* Indeks KAMI Diskominfo Provinsi DKI Jakarta T.A. 2022 ini disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi DKI Jakarta; dan
3. Sekretaris Daerah Provinsi DKI Jakarta.

Jakarta, 27 Juli 2022

Kepala Bidang Siber dan Sandi

Sandiman Madya pada
Direktorat Keamanan Siber dan Sandi
Pemerintah Daerah



R. Boedi Setiawan, S.H.
197009171998031006

Marcelina Tri N. W., S.Sos., M.Si (han)
19750717 199412 2 001

Mengetahui,
Kepala Diskominfo dan Statistik
Provinsi DKI Jakarta

Atika Nur Rahmania, S.IP, M.Si.
19720406 199803 2 006