



LAPORAN ONSITE ASSESMENT INDEKS KAMI



Instansi/Perusahaan:
Pemerintah Kota Malang

Narasumber Instansi/Perusahaan:

1. Johannes Agus Baju Widjaja, S.Sos., M.Si.
2. Didik Supriyadi
3. Rhomaisa Rosyadi, S.ST.

Unit Kerja:
Dinas Komunikasi dan Informatika Kota Malang

Alamat:
Perkantoran Terpadu Gedung A Lt.4
Jalan Mayjen Sungkono Malang

Tel:
(0341)751550

Email:
kominfo@malangkota.go.id

Pimpinan Unit Kerja:
Muhammad Nur Widiyanto, S.Sos.

A. Ruang Lingkup: Pengelolaan Data Center pada Dinas Komunikasi dan Informatika Kota Malang

1. Instansi / Unit Kerja:
Dinas Komunikasi dan Informatika Kota Malang
2. Fungsi Kerja:
Pengelolaan surat pemerintah Kota Malang meliputi pembuatan, pengiriman, penerimaan, disposisi dan arsip surat.
3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor	Perkantoran Terpadu Gedung A Lt.4 Jalan Mayjen Sungkono Malang
2	Data Center	Jalan Tugu No.1, Malang
3	Disaster Recovery Center	Belum ada

B. Nama /Jenis Layanan Publik:

Layanan yang masuk ruang lingkup adalah Sistem Layanan Infrastruktur (Data Center, Aplikasi, Jaringan, Server) Sistem Informasi dan Sistem Komunikasi yang dikelola oleh Bidang Statistik dan Persandian, Dinas Komunikasi dan Informatika Kota Malang

C. Aset TI yang kritis:

1. Informasi:
 - Data Pribadi
2. Aplikasi:
 - Suradi (Surat Digital)
3. Server:

4. Infrastruktur Jaringan/Network:

- Internet

D. DATA CENTER (DC):

ADA, berada pada tempat khusus. Data Center Diskominfo Pemkot Malang memiliki fasilitas dan peralatan sebagai berikut :

- Ruang Data Center memiliki satu pintu masuk dan tidak memiliki pintu darurat.
- Perimitri untuk akses masuk sudah menggunakan akses *fingerprint*
- CCTV untuk monitoring perangkat pengelolaan informasi pada Data Center berjalan dengan baik dan recorder CCTV disimpan dalam periode jangka waktu tertentu. Salah satu perangkat CCTV terpasang di luar ruangan Data Center dengan tujuan adalah untuk memberikan informasi aktivitas keluar masuk personil.
- Sarana pendukung untuk kondisi kebakaran di dalam Data Center sudah di akomodir dengan menggunakan APAR sebanyak 1 (satu) unit.

E. DISASTER RECOVERY CENTER (DRC):

Belum memiliki konsep Disaster Recovery Center

Status Ketersediaan Dokumen (Kebijakan/Prosedur)

Table 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

No	Nama Kebijakan	Cakupan Dokumen	Ada/Tidak
1	Kebijakan Keamanan Informasi	Menyatakan komitmen manajemen/pimpinan instansi/lembaga menyangkut pengamanan informasi yang didokumentasikan dan disahkan secara formal. Kebijakan keamanan informasi dapat mencakup antara lain: <ul style="list-style-type: none">• Definisi, sasaran dan ruang lingkup keamanan informasi• Persetujuan terhadap kebijakan dan program keamanan informasi• Kerangka kerja penetapan sasaran kontrol dan kontrol• Struktur dan metodologi manajemen risiko• Organisasi dan tanggungjawab keamanan informasi	Tidak
2	Organisasi, peran dan tanggungjawab keamanan informasi	Uraian tentang organisasi yang ditetapkan untuk mengelola dan mengkoordinasikan aspek keamanan informasi dari suatu instansi/lembaga serta uraian peran dan tanggungjawabnya. Organisasi pengelola keamanan informasi tidak harus berbentuk unit kerja terpisah	Ada

3	Panduan Klasifikasi Informasi	Berisi tentang petunjuk cara melakukan klasifikasi informasi yang ada di instansi/lembaga dan disusun dengan memperhatikan nilai penting dan kritikalitas informasi bagi penyelenggaraan pelayanan publik, baik yang dihasilkan secara internal maupun diterima dari pihak eksternal. Klasifikasi informasi dilakukan dengan mengukur dampak gangguan operasional, jumlah kerugian uang, penurunan reputasi dan legal manakala terdapat ancaman menyangkut kerahasiaan (<i>confidentiality</i>), keutuhan (<i>integrity</i>) dan ketersediaan (<i>availability</i>) informasi.	Tidak
4	Kebijakan Manajemen Risiko TIK	Berisi metodologi / ketentuan untuk mengkaji risiko mulai dari identifikasi aset, kelemahan, ancaman dan dampak kehilangan aspek kerahasiaan, keutuhan dan ketersediaan informasi termasuk jenis mitigasi risiko dan tingkat penerimaan risiko yang disetujui oleh pimpinan.	Ada
5	Kerangka Kerja Manajemen Kelangsungan Usaha (<i>Business Continuity Management</i>)	Berisi komitmen menjaga kelangsungan pelayanan publik dan proses penetapan keadaan bencana serta penyediaan infrastruktur TIK pengganti saat infrastruktur utama tidak dapat beroperasi agar pelayanan publik tetap dapat berlangsung bila terjadi keadaan bencana/k darurat. Dokumen ini juga memuat tim yang bertanggungjawab (ketua dan anggota tim), lokasi kerja cadangan, skenario bencana dan rencana pemulihan ke kondisi normal setelah bencana dapat diatasi/berakhir.	Tidak
6	Kebijakan Penggunaan Sumber daya TIK	Berisi aturan penggunaan komputer (desktop/laptop/modem atau email dan internet).	Tidak
No	Nama Prosedur/ Pedoman	Cakupan Dokumen	Ada/Tidak
1	Pengendalian Dokumen	Berisi proses penyusunan dokumen, wewenang persetujuan penerbitan, identifikasi perubahan, distribusi, penyimpanan, penarikan dan pemusnahan jika tidak digunakan, daftar dan pengendalian dokumen eksternal yang menjadi rujukan	Ada
2	Pengendalian Rekaman	Berisi pengelolaan rekaman yang meliputi: identifikasi rekaman penting, kepemilikan, pengamanan, masa retensi, dan pemusnahan jika tidak digunakan lagi	Ada

3	Audit Internal SMKI	Proses audit internal: rencana, ruang lingkup, pelaksanaan, pelaporan dan tindak lanjut hasil audit serta persyaratan kompetensi auditor	Tidak
4	Tindakan Perbaikan & Pencegahan	Berisi tatacara perbaikan/pencegahan terhadap masalah/gangguan/insiden baik teknis maupun non teknis yang terjadi dalam pengembangan, operasional maupun pemeliharaan TI	Tidak
5	Pelabelan, Pengamanan, Pertukaran & Disposasi Informasi	Aturan pelabelan, penyimpanan, distribusi, pertukaran, pemusnahan informasi/daya "rahasia" baik softcopy maupun hardcopy, baik milik instansi maupun informasi pelanggan/mitra yang dipercayakan kepada Instansi	Ada
6	Pengelolaan Removable Media & Disposasi Media	Aturan penggunaan, penyimpanan, pemindahan, pengamanan media simpan informasi (tape/hard disk/Flashdisk/CD) dan penghapusan informasi ataupun penghancuran media	Tidak
7	Pemantauan (Monitoring) Penggunaan Fasilitas TIK	Berisi proses monitoring penggunaan CPU, storage, email, internet, fasilitas TIK lainnya dan pelaporan serta tindak lanjut hasil monitoring	Ada
8	<i>User Access Management</i>	Berisi proses dan tatacara pendaftaran, penghapusan dan review hak akses user, termasuk administrator, terhadap sumber daya informasi (aplikasi, sistem operasi, database, internet, email dan internet)	Ada
9	<i>Teleworking</i>	Pengendalian dan pengamanan penggunaan hak akses secara remote (misal melalui modem atau jaringan). Siapa yang berhak menggunakan dan cara mengontrol agar penggunaannya aman.	Ada
10	Pengendalian instalasi software & Hak Kekayaan Intelektual	Berisi daftar software standar yang diijinkan di Instansi, permintaan pemasangan dan pelaksana pemasangan termasuk penghapusan software yang tidak diijinkan	Ada
11	Pengelolaan Perubahan (<i>Change Management</i>) TIK	Proses permintaan dan persetujuan perubahan aplikasi/infrastruktur TIK, serta pengkinian konfigurasi/database/versi dari aset TIK yang mengalami perubahan.	Ada
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi	Proses pelaporan & penanganan gangguan/insiden baik menyangkut ketersediaan layanan atau gangguan karena penyusupan/pengubahan informasi secara tidak berwenang. Termasuk analisis penyebab dan eskalasi jika diperlukan tindak lanjut ke aspek legal.	Ada

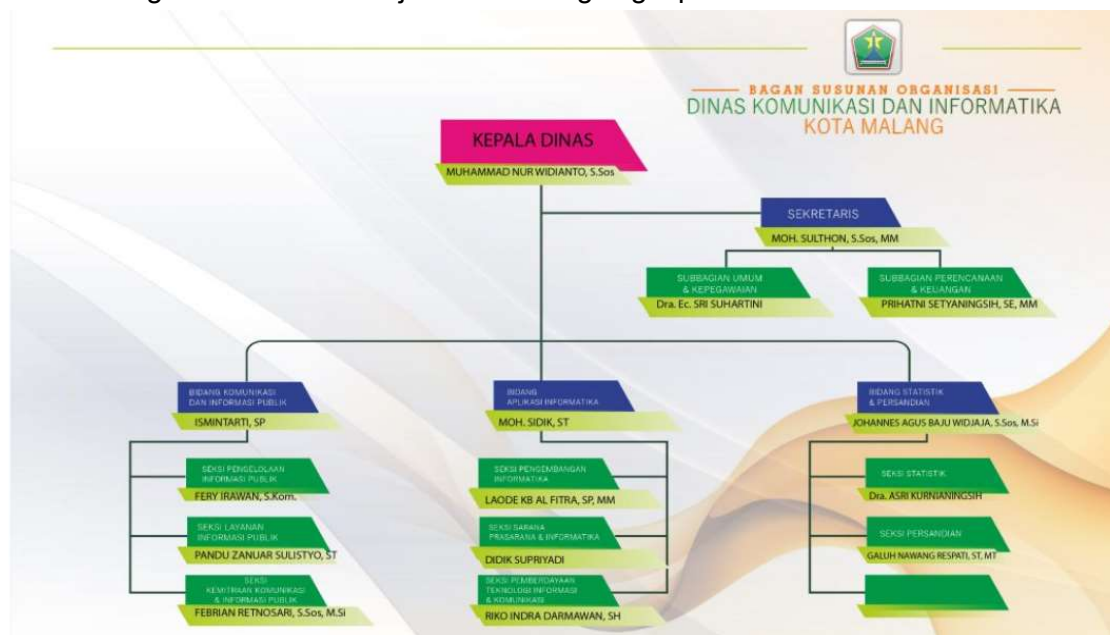
Dokumen-dokumen yang diperiksa:

1. Peraturan Daerah Kota Malang Nomor 1 Tahun 2019 Tentang Rencana Pembangunan Jangka Menengah Daerah Kota Malang Tahun 2018-2023
2. Peraturan Walikota Malang Nomor 72 Tahun 2019 Tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi dan Informatika
3. Lampiran Daftar Informasi yang dikecualikan

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

I. KONDISI UMUM:

1. Struktur organisasi satuan kerja dalam ruang lingkup



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

Total Score Sebelum Verifikasi: 117

Indeks KAMI (Keamanan Informasi)

Responden:

DINAS KOMUNIKASI DAN INFORMATIKA KOTA MALANG

Skor Kategori SE

: 29 Kategori SE Tinggi

Hasil Evaluasi Akhir:

Tidak Layak

Tingkat Kelengkapan Penerapan

Standar ISO27001 sesuai



PERKANTORAN TERPADU LT. 4 JALAN MAYJEN SINGKOND ARJOWINANGUN KOTA MALANG

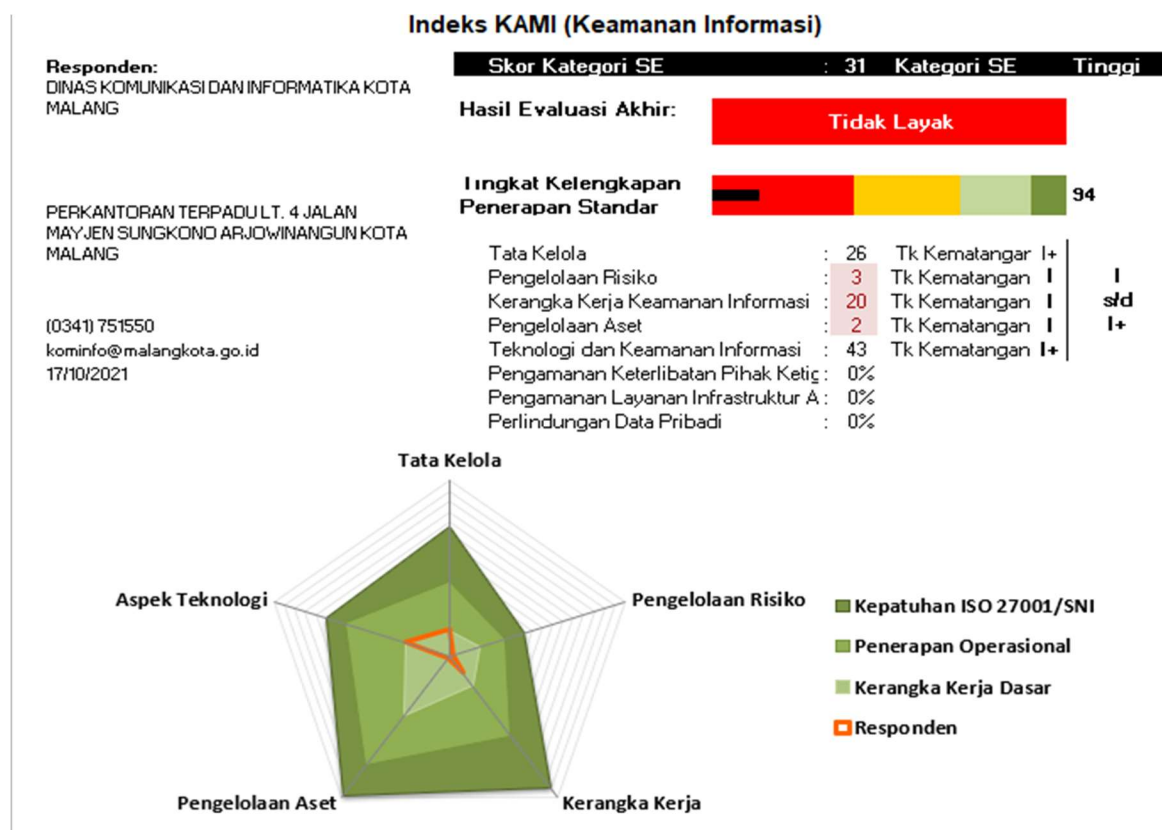
(0341) 751550

kominfo@malangkota.go.id

17/10/2021

Tata Kelola	: 32	Tk Kematangan: I+	
Pengelolaan Risiko	: 22	Tk Kematangan: I	I
Kerangka Kerja Keamanan Informasi	: 30	Tk Kematangan: I	s/d
Pengelolaan Aset	: 0	Tk Kematangan: I	I+
Teknologi dan Keamanan Informasi	: 33	Tk Kematangan: I+	
Pengamanan Keterlibatan Pihak Ketiga	: 0%		
Pengamanan Layanan Infrastruktur Aw	: 0%		
Perlindungan Data Pribadi	: 0%		

Total Score Setelah Verifikasi: 94



II. ASPEK TATA KELOLA:

A. Kekuatan/Kematangan

1. Pimpinan dari Diskominfo Pemkot Malang secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi, hal ini ditandai dengan adanya kebijakan yang telah dibuat sebagai dasar teknis pelaksanaan kegiatan penerapan keamanan informasi pada lingkup tugasnya.
2. Diskominfo Pemkot Malang memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi.
3. Diskominfo Pemkot Malang sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi.
4. Diskominfo Pemkot Malang sudah menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi.

B. Kelemahan/Kekurangan

1. Belum adanya integrasi keperluan/persyaratan keamanan informasi dalam proses kerja.
2. Belum ada identifikasi data pribadi yang digunakan dalam proses kerja dan belum menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku.
3. Tanggung jawab pengelolaan keamanan informasi yang didelegasikan kepada fungsi pengelola keamanan informasi belum 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.
4. Pengelola keamanan informasi belum secara proaktif berkoordinasi dengan satker terkait ataupun pihak eksternal yang berkepentingan untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak

5. Tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) belum didefinisikan dan dialokasikan.
6. Penanggungjawab pengelolaan keamanan informasi belum melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi secara rutin dan resmi.
7. Pimpinan satuan kerja di Diskominfo Kota Malang belum menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya.
8. Diskominfo Kota Malang belum mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanaannya, pemantauannya dan eskalasi pelaporannya.
9. Belum ada program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksanaannya.
10. Diskominfo Kota Malang belum menerapkan 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.
11. Diskominfo Kota Malang belum mendelegasikan pihak terkait / unit kerja / fungsi pengelola keamanan informasi pada internal Badan Pendapatan Daerah Kota Malang untuk mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi serta dipastikan untuk dipatuhi dengan menganalisa tingkat kepatuhannya
12. Diskominfo Kota Malang belum mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

III. ASPEK RISIKO:

A. Kekuatan/Kematangan

1. Diskominfo Kota Malang sudah mengidentifikasi ancaman dan kelemahan yang terkait dengan aset informasi.
2. Diskominfo Kota Malang telah menetapkan dampak kerugian terkait hilangnya/terganggunya fungsi aset utama.

B. Kelemahan/Kekurangan

1. Diskominfo Kota Malang belum mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
2. Belum ada penetapan penanggungjawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan
3. Belum ada kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
4. Kerangka kerja pengelolaan risiko belum mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian di Diskominfo Kota Malang
5. Belum ada penetapan ambang batas tingkat risiko yang dapat diterima dalam rangka melakukan evaluasi terhadap tingkatan risiko yang dianalisa.
6. Diskominfo Kota Malang belum mendefinisikan mengenai kepemilikan dan pihak pengelola (*custodian*) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
7. Belum dilakukan analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada.
8. Langkah-langkah mitigasi dan penanggulangan risiko belum disusun.
9. Kerangka kerja pengelolaan risiko belum secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya.
10. Diskominfo Kota Malang belum melakukan penilaian risiko sebagai bagian dari implementasi program yang dapat mengintegrasikan seluruh bagian dari bisnis proses organisasi dan menjadi bagian dari kriteria penilaian obyektif kinerja efektivitas pengamanan.

11. Pemantauan secara berkala terhadap status penyelesaian langkah mitigasi risiko belum dilakukan.

IV. ASPEK KERANGKA KERJA:

A. Kekuatan/Kematangan

1. Diskominfo Kota Malang telah menyusun kebijakan terkait keamanan informasi, namun masih belum di sahkan.
2. Diskominfo Kota Malang telah melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan sebagian aset informasi yang ada.

B. Kelemahan/Kekurangan

1. Diskominfo Kota Malang belum memiliki mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
2. Belum terdapat proses (mencakup pelaksana, mekanisme, jadwal, materi dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga.
3. Kebijakan dan prosedur keamanan informasi yang ada belum merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi.
4. Belum terdapat proses untuk mengidentifikasi kondisi yang membahayakan keamanan informasi dan menetapkan sebagai insiden keamanan informasi.
5. Aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK belum tercantum dalam kontrak dengan pihak ketiga.
6. Konsekuensi dari pelanggaran kebijakan keamanan informasi belum didefinisikan.
7. Diskominfo Kota Malang belum menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya.
8. Belum terdapat proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul.
9. Belum memiliki kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*).
10. Belum memiliki kerangka kerja perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*).
11. Seluruh kebijakan dan prosedur keamanan informasi belum dievaluasi kelayakannya secara berkala.
12. Strategi penerapan keamanan informasi belum dirumuskan dan ditetapkan sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi.
13. Strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko belum ditetapkan secara resmi.
14. Strategi penerapan keamanan informasi belum direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi.

V. ASPEK PENGELOLAAN ASET:

A. Kekuatan/Kematangan

-

B. Kelemahan/Kekurangan

1. Belum adanya daftar inventaris aset informasi secara keseluruhan/lengkap sesuai *scope* secara akurat dan terpelihara dengan informasi tambahan pemilik aset yang akan bertanggung jawab dalam pemeliharaannya.

2. Belum ada pendefinisian klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku.
3. Belum terdapat proses evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi dan keperluan pengamanannya.
4. Belum ada proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten
5. Belum ada proses yang mengatur mengenai perilsan suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
6. Diskominfo Kota Malang belum mendefinisikan tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi.
7. Belum ada tata tertib mengenai penggunaan komputer, email, internet dan intranet serta pengamanan dan penggunaan aset instansi terkait HAKI.
8. Belum ada peraturan terkait instalasi piranti lunak di aset TI milik instansi.
9. Belum ada peraturan mengenai penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data.
10. Pengelolaan identitas elektronik dan proses otentikasi termasuk kebijakan terhadap pelanggaran belum ada.
11. Belum ada ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada, syarat penghancuran data dan ketetapan terkait pertukaran data dengan pihak eksternal beserta pengamanannya.
12. Belum ada prosedur backup dan uji coba pengembalian data (*restore*)
13. Belum terdapat proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak berwajib.
14. Prosedur penghancuran data/aset yang sudah tidak diperlukan belum ada.
15. Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya berikut langkah pembenahan apabila terjadi ketidaksesuaian terhadap kebijakan yang berlaku belum ada.
16. Prosedur yang mengatur terkait user yang mutasi/keluar atau tenaga kontrak/*outsourse* yang habis masa kerjanya belum ditetapkan dan belum didokumentasikan.
17. Daftar data/informasi yang harus di backup dan laporan analisa kepatuhan terhadap prosedur *backup*-nya belum ditetapkan dan didokumentasikan
18. 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.
19. Peraturan pengamanan perangkat komputasi milik instansi yang digunakan di luar lokasi kerja resmi (kantor) belum ada.
20. Belum adanya mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
21. Belum didefinisikan dan ditetapkannya 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).

VI. ASPEK TEKNOLOGI:

A. Kekuatan/Kematangan

1. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan. Pengamanan yang diterapkan pada sistem yaitu dengan implementasi *firewall* dan SSL.
2. Jaringan komunikasi sudah disegmentasi sesuai dengan pembagian instansi/perusahaan.
3. Diskominfo Kota Malang telah melakukan monitoring untuk memastikan ketersediaan kapasitas yang cukup pada keseluruhan infrastruktur jaringan, sistem dan aplikasi.
4. Pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi sudah diterapkan.

5. Diskominfo Kota Malang telah menerapkan pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan.

B. Kelemahan/Kekurangan

1. Konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi belum di dokumentasikan dan dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan.
2. Analisa kepatuhan terhadap penerapan konfigurasi standar belum dilakukan.
3. Belum dilakukannya pemindaian secara rutin terhadap jaringan, sistem dan aplikasi.
4. Analisa secara berkala terhadap log untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik) belum dilakukan.
5. Belum memiliki standar dalam penggunaan enkripsi.
6. Pengamanan untuk mengelola kunci enkripsi yang digunakan termasuk siklus penggunaannya belum diterapkan.
7. Sistem dan aplikasi belum dibuat untuk secara otomatis melakukan penggantian password, menon-aktifkan password, pengaturan kompleksitas/panjangnya dan penggunaan password lama.
8. Tidak ada pengamanan khusus yang berlapis terhadap akses yang digunakan untuk mengelola sistem (administrasi sistem).
9. Antivirus/antimalware yang digunakan belum dimutakhirkan secara rutin dan sistematis.
10. Mekanisme sinkronisasi waktu sesuai standar yang ada untuk keseluruhan jaringan, sistem dan aplikasi belum diterapkan.
11. Lingkungan pengembangan dan uji coba belum diamankan sesuai dengan standar platform teknologi yang ada.
12. Belum melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin.

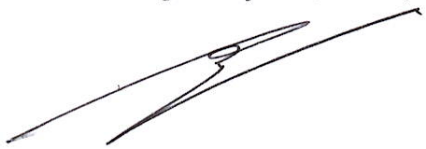

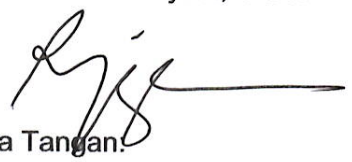
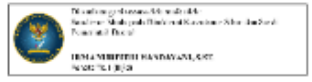
VIII. REKOMENDASI

1. Diskominfo Kota Malang perlu menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait.
2. Diskominfo Kota Malang perlu menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi.
3. Diskominfo Kota Malang perlu mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada.
4. Pengelola keamanan informasi perlu 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 pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak.
5. Identifikasi data pribadi yang digunakan dalam proses kerja perlu disusun dan diterapkan pengamanan sesuai dengan peraturan perundangan yang berlaku.
6. Tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) perlu didefinisikan dan dialokasikan.
7. Mekanisme penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi perlu disusun secara resmi dan dilakukan secara rutin.
8. Pimpinan satuan kerja di Diskominfo Kota Malang perlu menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya.
9. Diskominfo Kota Malang perlu mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksanaannya, pemantauannya dan eskalasi pelaporannya.
10. Program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksanaannya perlu disusun.

11. Diskominfo Kota Malang perlu menerapkan 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.
12. Diskominfo Kota Malang perlu mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya
13. Diskominfo Kota Malang perlu mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).
14. Diskominfo Kota Malang perlu menyusun program kerja pengelolaan risiko keamanan informasi dan secara resmi digunakan.
15. Perlu menetapkan penanggungjawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan
16. Kerangka kerja pengelolaan risiko keamanan informasi yang perlu didokumentasi dan secara resmi digunakan. Kerangka kerja pengelolaan risiko perlu mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian di Diskominfo Kota Malang.
17. Perlu menetapkan ambang batas tingkat risiko yang dapat diterima dalam rangka melakukan evaluasi terhadap tingkatan risiko yang dianalisa.
18. Diskominfo Kota Malang perlu mendefinisikan mengenai kepemilikan dan pihak pengelola (*custodian*) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
19. Perlu dilakukan analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada.
20. Langkah-langkah mitigasi dan penanggulangan risiko perlu disusun.
21. Kerangka kerja pengelolaan risiko perlu secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya.
22. Diskominfo Kota Malang perlu melakukan penilaian risiko sebagai bagian dari implementasi program yang dapat mengintegrasikan seluruh bagian dari bisnis proses organisasi dan menjadi bagian dari kriteria penilaian obyektif kinerja efektivitas pengamanan.
23. Perlu dilakukan pemantauan secara berkala terhadap status penyelesaian langkah mitigasi risiko.
24. Diskominfo Kota Malang perlu menyusun mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
25. Kebijakan dan prosedur keamanan informasi disusun dengan merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi.
26. Perlu dilakukan identifikasi kondisi yang membahayakan keamanan informasi dan menetapkan sebagai insiden keamanan informasi.
27. Dalam kontrak dengan pihak ketiga, perlu mencantumkan aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK.
28. Konsekuensi dari pelanggaran kebijakan keamanan informasi perlu didefinisikan.
29. Diskominfo Kota Malang perlu menyusun dan menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya.
30. Perlu dilakukan evaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan proses untuk menanggulangi permasalahan yang muncul.
31. Perlu menyusun kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) dan kerangka kerja perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*).
32. Perlu dilakukan dievaluasi kelayakannya secara berkala untuk seluruh kebijakan dan prosedur keamanan informasi.

33. Strategi penerapan keamanan informasi perlu dirumuskan dan ditetapkan sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi.
34. Strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko perlu ditetapkan secara resmi.
35. Strategi penerapan keamanan informasi perlu direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi.
36. Perlu menyusun daftar inventaris aset informasi secara keseluruhan/lengkap sesuai *scope* secara akurat dan terpelihara dengan informasi tambahan pemilik aset yang akan bertanggung jawab dalam pemeliharannya.
37. Klasifikasi aset informasi perlu didefinisikan sesuai dengan peraturan perundangan yang berlaku.
38. Perlu dilakukan evaluasi dan klasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi dan keperluan pengamanannya.
39. Proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) perlu diterapkan secara konsisten.
40. Perlu menyusun prosedur mengenai perilisan suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
41. Diskominfo Kota Malang perlu mendefinisikan tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi.
42. Perlu menyusun tata tertib mengenai penggunaan komputer, email, internet dan intranet serta pengamanan dan penggunaan aset instansi terkait HAKI dan peraturan terkait instalasi piranti lunak di aset TI milik instansi.
43. Peraturan mengenai penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data perlu disusun.
44. Pengelolaan identitas elektronik dan proses otentikasi termasuk kebijakan terhadap pelanggarannya perlu disusun.
45. Perlu penetapan terkait waktu penyimpanan untuk klasifikasi data yang ada, syarat penghancuran data dan ketentuan terkait pertukaran data dengan pihak eksternal beserta pengamanannya.
46. Perlu menyusun prosedur backup dan uji coba pengembalian data (*restore*).
47. Perlu menyusun prosedur pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak berwajib.
48. Prosedur penghancuran data/aset yang sudah tidak diperlukan perlu disusun.
49. Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya berikut langkah pembenahan apabila terjadi ketidaksesuaian terhadap kebijakan yang berlaku perlu disusun.
50. Prosedur yang mengatur terkait user yang mutasi/keluar atau tenaga kontrak/*outsourcing* yang habis masa kerjanya perlu ditetapkan dan perlu didokumentasikan.
51. Daftar data/informasi yang harus di backup dan laporan analisa kepatuhan terhadap prosedur *backup*-nya perlu ditetapkan dan didokumentasikan.
52. 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 perlu ditetapkan dan didokumentasikan.
53. Peraturan pengamanan perangkat komputasi milik instansi yang digunakan di luar lokasi kerja resmi (kantor) perlu disusun.
54. Perlu menetapkan mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
55. 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 telepon genggam di dalam ruang server, menggunakan kamera dll) perlu didefinisikan dan didokumentasikan.
56. Konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi perlu di dokumentasikan dan dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan.

57. Perlu dilakukan analisa kepatuhan terhadap penerapan konfigurasi standar.
58. Pemindaian secara rutin terhadap jaringan, sistem dan aplikasi perlu diterapkan.
59. Analisa secara berkala terhadap log untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik) perlu diterapkan.
60. Standar dalam penggunaan enkripsi dan mekanisme pengamanan untuk mengelola kunci enkripsi perlu didefinisikan dan didokumentasikan secara resmi.
61. Perlu diterapkan otomatisasi penggantian password, penon-aktifan password, pengaturan kompleksitas/panjangnya dan penggunaan password lama pada sistem dan aplikasi.
62. Perlu diterapkan pengamanan khusus yang berlapis terhadap akses yang digunakan untuk mengelola sistem (administrasi sistem).
63. Antivirus/antimalware yang digunakan perlu dimutakhirkan secara rutin dan sistematis.
64. Mekanisme sinkronisasi waktu sesuai standar yang ada untuk keseluruhan jaringan, sistem dan aplikasi perlu diterapkan.
65. Lingkungan pengembangan dan uji coba perlu diamankan sesuai dengan standar platform teknologi yang ada.

<p>Malang, 2 Desember 2021</p> <p>Dinas Komunikasi dan Informatika Kota Malang</p> <p>1. Johannes Agus Baju W.,S.Sos.,M.Si.</p>  <p>Tanda Tangan:</p> <p>2. Didik Supriyadi</p>  <p>Tanda Tangan:</p> <p>3. Rhomaisa Rosyadi, S.ST.</p>  <p>Tanda Tangan:</p>	<p>Assessor Indeks KAMI:</p> <p>1.Assessor : Irma Nurfitri Handayani, S.ST</p>  <p>Tanda Tangan:</p> <p>2. Assesor : Melita Irmasari, S.ST., M.M</p> <p>Tanda Tangan:</p> <p>3.. Assesor : Ni Putu Ayu Lhaksmi.,S.Tr.TP.</p> <p>Tanda Tangan</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------