POLITEKNIK KESEHATAN SURAKARTA JL. LETJEND SUTOYO, MOJOSONGO, SURAKARTA	NOMOR	DP.03.04/1.1/7487.1/2019
	TANGGAL PEMBUATAN	8 Oktober 2019
	TANGGAL REVISI	
	TANGGAL EFEKTIF	
	DISAHKAN OLEH	Direktur Satino, SKM., MScN NIP. 196101021989031001

PROSEDUR SISTEM MANAJEMEN KEAMANAN (SECURITY AWARENESS) SISTEM INFORMASI

PROSEDUR SISTEM MANAJEMEN KEAMANAN INFORMASI

1. Pendahuluan

Informasi merupakan aset yang sangat penting bagi Instansi penyelenggara layanan publik, dan karenanya perlu dilindungi dari ancaman yang dapat mengganggu kelangsungan bisnisnya.

Penggunaan fasilitas TI selain memudahkan proses pekerjaan juga mengandung risiko bila tidak digunakan dan dikelola dengan tepat

Penggunaan TI harus dikelola sedemikian rupa sehingga memberi manfaat sebesar - besarnya dengan kemungkinan risiko yang rendah.

Kebijakan ini didokumentasikan sebagai panduan untuk melindungi informasi dari ancaman keamanan informasi yang meliputi kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability) dan mengurangi dampak dari terjadinya insiden keamanan

2. Tujuan

Melindungi aset informasi Instansi penyelenggara layanan publik dari segala bentuk ancaman, baik eksternal maupun internal, sengaja atau tidak.

3. Ruang lingkup

Kebijakan ini berlaku untuk seluruh aset informasi yang digunakan Instansi penyelenggara layanan publik yang meliputi:

3.1. Organisasi dan Lokasi

Seluruh unit kerja di Instansi penyelenggara layanan publik dan lokasi kerja yang digunakan untuk mengelola dan menyediakan layanan internal dan eksternal instansi penyelenggara layanan publik

3.2 Aset

Aset yang dicakup meliputi:

- Data dan Informasi
  Termasuk data dan informasi meliputi: dokumen pengadaan dan kontrak, data pelanggan, data gaji, data pegawai, sistem dokumentasi manajemen, dokumen teknis & konfigurasi jaringan, hasil penetration test, materi pelatihan, prosedur operasional, *business continuity plan*, dan hasil audit
- Software
  Yang termasuk dalam aset perangkat lunak atau software antara lain : software aplikasi, operating system, development tool, dan software tool (antivirus, audit tool)
- Hardware
  Yang termasuk dalam aset perangkat keras atau hardware misalnya :Server, PC, Laptop, media penyimpan data
- Perangkat Jaringan Komunikasi
  Yang termasuk dalam aset perangkat jaringan komunikasi antara lain Router, Modem, Switch, Kabel, Firewall
- Fasilitas Pendukung
  Yang termasuk dalam aset fasilitas pendukung antara lain Ruang Server / Ruang Data Center, Ruang Kerja, Ruang Disaster Recovery Center (DRC), UPS, Genset, A/C, CCTV, Fire Extinguisher, Access Door Electronic, dan sebagainya;
- Sumber Daya Manusia
  Yang termasuk dalam aset sumber daya manusia misalnya pegawai tetap, calon pegawai tetap, pegawai kontrak, mitra, vendor dan pihak ketiga lainnya yang menyediakan layanan, jasa, serta produk yang menunjang bisnis Instansi penyelenggara layanan publik.

4. Kebijakan

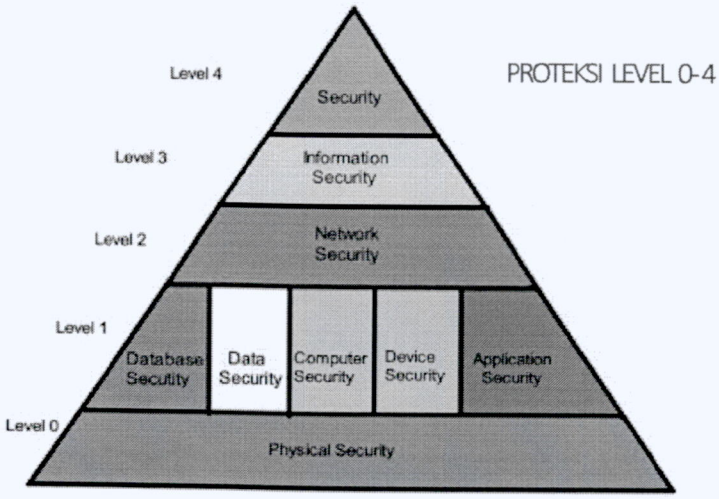
- Seluruh informasi yang disimpan dalam media simpan, ditulis, dicetak, dan dikomunikasikan langsung atau melalui teknologi komunikasi harus dilindungi terhadap kemungkinan kerusakan, kesalahan penggunaan secara sengaja atau tidak, dicegah dari akses oleh user yang tidak berwenang dan dari ancaman terhadap kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability).
- Kebijakan keamanan informasi harus dikomunikasikan ke seluruh pegawai dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.
- Instansi penyelenggara layanan publik meningkatkan kepedulian (*awareness*), pengetahuan dan keterampilan tentang keamanan informasi bagi pegawai. Sosialisasi juga perlu diberikan kepada vendor, konsultan, mitra, dan pihak ketiga lainnya sepanjang diperlukan.
- Seluruh kelemahan keamanan informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan TI harus segera dilaporkan ke penanggung jawab TI terkait.
- Seluruh pimpinan di semua tingkatan bertanggungjawab menjamin kebijakan ini diterapkan di seluruh unit kerja di bawah pengawasannya.
- Seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan aset informasi serta mematuhi kebijakan dan prosedur keamanan informasi yang telah ditetapkan
- Setiap pelanggaran terhadap kebijakan ini yang relevan dapat dikenai sanksi atau tindakan disiplin sesuai peraturan yang berlaku.
- Kebijakan yang lebih teknis merujuk prinsip-prinsip yang ditetapkan dalam kebijakan ini.
- Setiap pengecualian terhadap kebijakan ini dan kebijakan turunnya harus mendapat persetujuan minimum dari pejabat yang berwenang

5. PROTEKSI

Skema Klasifikasi Informasi

RAHASIA	Aset informasi yang sangat peka dan berisiko tinggi yang pembocoran atau penyalahgunaan akses terhadapnya bisa mengganggu kelancaran usaha instansi/lembaga secara temporer atau mengganggu citra dan reputasi perusahaan. Contoh: data wajib pajak, rencana mutasi, IP address, password komputer, laporan audit, data gaji dan penilaian kinerja karyawan, dan data kesehatan pribadi yang secara legal harus dilindungi instansi/lembaga.
INTERNAL	Informasi yang telah terdistribusi secara luas di lingkungan internal instansi/lembaga yang penyebarannya secara internal tidak lagi memerlukan izin dari pemilik informasi dan risiko penyebarannya secara tak berwenang tidak menimbulkan kerugian signifikan. Contoh: kebijakan instansi/lembaga, panduan kerja, prosedur kerja, instruksi kerja, memo / publikasi internal, bahan / materi training, informasi yang disediakan dalam intranet, dan data operasional TI lainnya.
PUBLIK	Informasi yang secara sengaja disediakan instansi/lembaga untuk dapat diketahui publik. Contoh: brosur marketing, situs publik dan siaran pers.

1. Tingkatan Level



- **Keamanan level 0**
  - Keamanan fisik, merupakan keamanan tahap awal dari komputer security. Jika keamanan fisik tidak terjaga dengan baik, maka data-data bahkan hardware komputer sendiri tidak dapat diamankan
- **Keamanan level 1**
  - keamanan database
  - keamanan data
  - keamanan dari PC itu sendiri
  - keamanan device
  - keamanan application

- **Keamanan level 2**
  - Keamanan jaringan
  - Komputer yang terhubung dengan jaringan sangat rawan dalam masalah keamanan, oleh karena itu keamanan level 2 harus dirancang supaya tidak terjadi kebocoran jaringan, akses ilegal yang dapat merusak keamanan data tersebut.
- **Keamanan level 3**
  - Keamanan informasi
  - Keamanan informasi kadang tidak dipedulikan oleh administrator, seperti memberikan *password* ke teman, atau menuliskannya dikertas.
- **Keamanan level 4**
  - merupakan keamanan secara keseluruhan dari komputer
  - Jika level 1-3 sudah dapat dikerjakan dengan baik maka otomatis keamanan untuk level 4 sudah tercapai