DASAR KESELAMATAN ICT ICU JPM (DKICT)

Definisi Keselamatan

- Suatu keadaan bebas daripada ancaman dan risiko yang tidak boleh diterima

Definisi Aset ICT Kerajaan

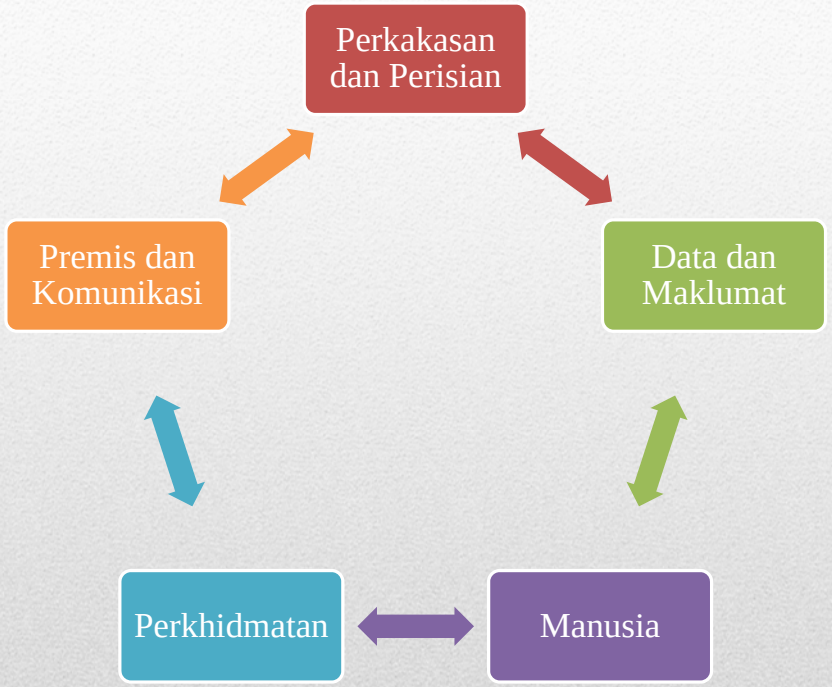
- Manusia, Peralatan, Perisian, Data dan Maklumat, Telekomunikasi, Kemudahan ICT

Petikan dari para 5: Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan

Latar Belakang

- Dokumen rujukan yang mengandungi **peraturan** yang perlu dibaca dan dipatuhi dalam menggunakan aset ICT
- **Hasrat dan hala tuju pengurusan keselamatan** untuk melindungi aset ICT
- Berasaskan kepada persekitaran ICU JPM
- Mendapat kelulusan pengurusan, diterbitkan dan disebarkan kepada semua warga ICU JPM dan pihak ketiga
- Arahan pengurusan berkaitan **tindakan, garis panduan dan prosedur, pernyataan peringkat tertinggi dan keperluan umum** bagi sesuatu agensi

Dasar Keselamatan ICT ICU JPM



Skop DKICT

- Memastikan kelancaran operasi dan kesinambungan perkhidmatan
- Meminimumkan insiden keselamatan ICT
- Meminimumkan kemusnahan dan kerosakan
- Melindungi kepentingan pihak yang bergantung kepada sistem maklumat
- Mencegah salah guna dan kecurian aset ICT Kerajaan.

Objektif DKICT ICU JPM

- Bab 1 – Pembangunan dan Penyelenggaraan Dasar
- Bab 2 – Organisasi Keselamatan
- Bab 3 – Pengurusan Aset
- Bab 4 – Keselamatan Sumber Manusia
- Bab 5 – Keselamatan Fizikal dan Persekitaran
- Bab 6 – Pengurusan Operasi dan Komunikasi
- Bab 7 – Kawalan Capaian
- Bab 8 – Perolehan, Pembangunan dan Penyelenggaraan Sistem
- Bab 9 – Pengurusan Keselamatan Insiden ICT
- Bab 10 – Pengurusan Kesinambungan Perkhidmatan
- Bab 11 - Pematuhan

11 Bab DKICT ICU JPM

- **DKI-0101 – Dasar Keselamatan ICT**
  - Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan ICU JPM dan perundangan yang berkaitan.

Bab 1
Pembangunan dan Penyelenggaraan Dasar

- **DKI- 0201 – Infrastruktur Organisasi Dalaman**
  - Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT ICU JPM .

Bab 2
Organisasi Keselamatan

- **DKI-0201 – Infrastruktur Organisasi Dalaman**
  - Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT ICU JPM .

Bab 2
Organisasi Keselamatan

- **DKI-0202 – Pihak Ketiga**
  - Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).

Bab 2
Organisasi Keselamatan

- **DKI-0301 – Akauntabiliti Aset**
  - Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT ICU JPM .

Bab 3
Pengurusan Aset

- **DKI- 0302 – Pengelasan dan Pengendalian Maklumat**
  - Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

Bab 3
Pengurusan Aset

- **0401 – Keselamatan Sumber Manusia dalam Tugas Harian**
  - Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan ICU JPM , pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga ICU JPM hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

Bab 4
Keselamatan Sumber Manusia

- **DKI-0501 - Keselamatan Kawasan**
  - Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

Bab 5
Keselamatan Fizikal dan Persekitaran

- **DKI- 0502 – Keselamatan Peralatan**
  - Melindungi peralatan ICT ICU JPM dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

Bab 5
Keselamatan Fizikal dan Persekitaran

- **DKI-0503 – Keselamatan Persekitaran**
  - Melindungi aset ICT ICU JPM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

Bab 5
Keselamatan Fizikal dan Persekitaran

- **DKI-0504 - Keselamatan Dokumen**
  - Melindungi maklumat ICU JPM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.

Bab 5
Keselamatan Fizikal dan Persekitaran

- **0601 – Pengurusan Prosedur Operasi**
  - Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

KAWALAN	TANGGUNGJAWAB
060101 PENGENDALIAN PROSEDUR	Semua
060102 KAWALAN PERUBAHAN	Semua
060103 PENGASINGAN TUGAS DAN TANGGUNGJAWAB	Pengurus ICT dan ICTSO

Bidang 6
Pengurusan Operasi dan Komunikasi

- **DKI-0602 – Penyampaian Perkhidmatan Pihak Ketiga**
  - Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.

Bab 6
Pengurusan Operasi dan Komunikasi

- **DKI-0603 – Perancangan dan Penerimaan Sistem**
  - Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

Bab 6
Pengurusan Operasi dan Komunikasi

- **DKI-0604 – Perisian Berbahaya**
  - Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya.

Bab 6
Pengurusan Operasi dan Komunikasi

- **DKI-0605 – Housekeeping**
  - Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

Bab 6
Pengurusan Operasi dan Komunikasi

- **DKI-0606 – Pengurusan Rangkaian**
  - Melindungi maklumat dalam rangkaian dan infrastruktur sokongan

Bab 6
Pengurusan Operasi dan Komunikasi

- **DKI-0607 – Pengurusan Media**
  - Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

Bab 6
Pengurusan Operasi dan Komunikasi

- **DKI-0608 – Pengurusan Penukaran Maklumat**
  - Memastikan keselamatan pertukaran maklumat dan perisian antara ICU JPM dan agensi luar terjamin

Bab 6
Pengurusan Operasi dan Komunikasi

- **DKI-0609 – *e-commerce***
  - Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.

Bab 6
Pengurusan Operasi dan Komunikasi

- **DKI-0610 – Pemantauan**
  - Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

Bab 6
Pengurusan Operasi dan Komunikasi

- **DKI-0701 – Dasar Kawalan Capaian**
  - Mengawal capaian ke atas maklumat.

Bab 7
Kawalan Capaian

- **DKI-0702 – Pengurusan Capaian Pengguna**
  - Mengawal capaian pengguna ke atas aset ICT ICU JPM .

Bab 7
Kawalan Capaian

- **0703 – Kawalan Capaian Rangkaian**
  - Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian
- **0704 – Kawalan Capaian Sistem Pengoperasian**
  - Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

Bab 7
Kawalan Capaian

- **DKI-0705 – Kawalan Capaian Aplikasi dan Maklumat**
  - Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi

- **DKI-0706 – Peralatan Mudah Alih Dan Kerja Jarak Jauh**
  - Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

Bab 7
Kawalan Capaian

- **DKI-0801 – Keselamatan Dalam Membangunkan Sistem dan Aplikasi**
  - Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

Bab 8
Perolehan, Pembangunan dan Penyelenggaraan Sistem

- **DKI-0802 – Kawalan Kriptografi**
  - Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

- **DKI-0803 – Keselamatan Fail Sistem**
  - Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.
- **DKI-0804 – Keselamatan Dalam Proses Pembangunan Dan Sokongan**
  - Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

Bab 8
Perolehan, Pembangunan dan Penyelenggaraan Sistem

- **DKI-0805 – Kawalan Teknikal Keterdedahan**
  - Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya

Bab 8
Perolehan, Pembangunan dan Penyelenggaraan Sistem

- **DKI-0901 – Mekanisme Pelaporan Insiden Keselamatan ICT**
  - Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

- **DKI- 0901 – Pengurusan Maklumat Insiden Keselamatan ICT**
  - Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

Bab 9
Pengurusan Pengendalian Insiden Keselamatan

- **DKI-1001 – Dasar Kesinambungan Perkhidmatan**
  - Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

Bab 10
Dasar Kesinambungan Perkhidmatan

- **DKI-1101 – Pematuhan dan Keperluan Perundangan**
  - Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT ICU JPM .

Bab 11
Pematuhan dan Keperluan Perundangan