DASAR KESELAMATAN ICT JPP DAN POLITEKNIK

DKICT JPP DAN POLITEKNIK

Pengenalan DKICT

- DKICT mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan telekomunikasi (ICT)

- DKICT juga menerangkan mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT

Objektif DKICT

- Memastikan kelancaran operasi JPP dan Politeknik dan meminimumkan kerosakan atau kemusnahan;

- Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat atau komunikasi; dan

- Mencegah salah guna atau kecurian aset ICT kerajaan.

Pernyataan Dasar

- Keselamatan ICT – keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan.

- 4 Komponen asas Keselamatan ICT iaitu
  - Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
  - Menjamin setiap maklumat adalah tepat dan sempurna;
  - Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
  - Memastikan akses kepada hanya pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Pernyataan Dasar – samb.

Keselamatan Aset ICT ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan. Ia dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosidur dalam pengendalian semua perkara berikut:

a) Perkakasan

b) Perisian

c) Perkhidmatan

d) Data atau Maklumat

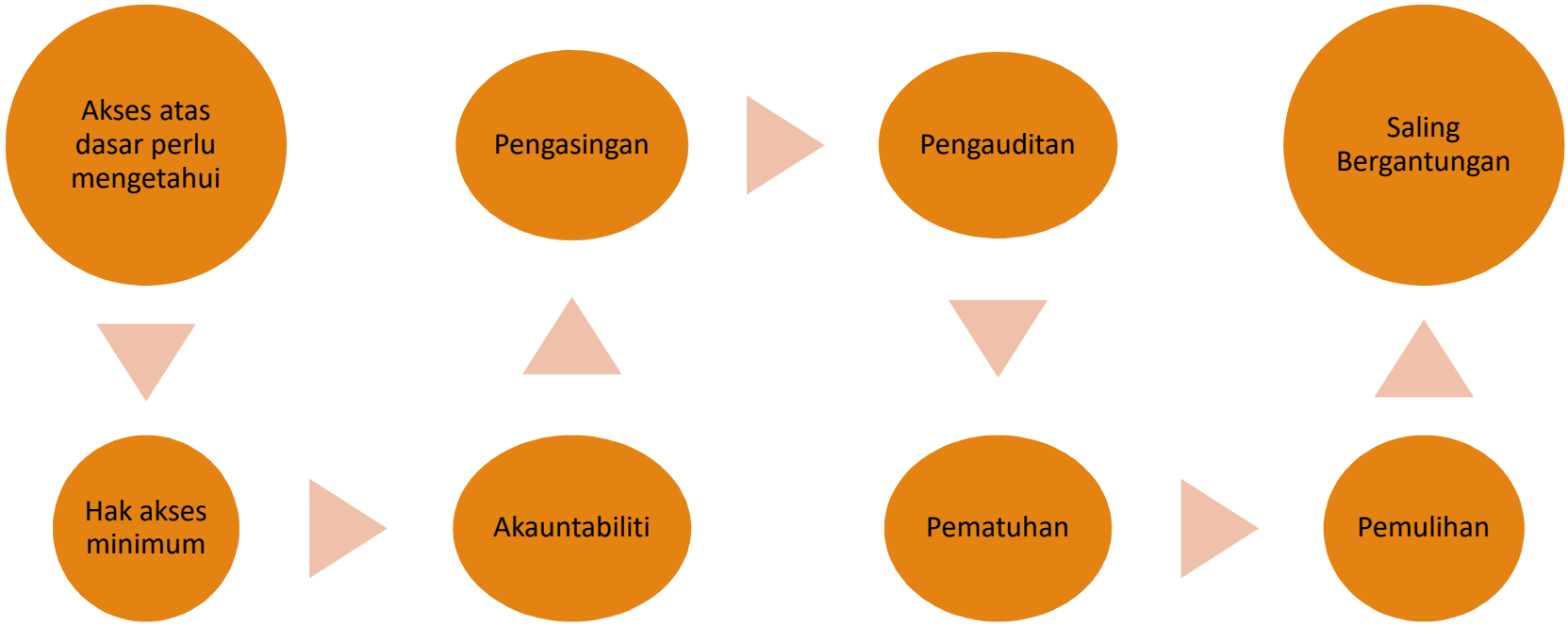
e) Manusia

f) Premis Komputer dan Komunikasi

** semua perkara di atas perlu diberi perlindungan rapi bagi mengelakkan kebocoran rahsia atau kelemahan perlindungan

PRINSIP DKICT

Prinsip-prinsip asas DKICT dan perlu dipatuhi adalah:



Dasar Keselamatan ICT

DKICT mengambilkira objektif kawalan ISO/ICE 27001:2007 Pengurusan Sistem Keselamatan Maklumat yang meliputi bidang-bidang berikut:

- Bidang 1: Pembangunan dan Penyelenggaraan Dasar
- Bidang 2: Organisasi Keselamatan
- Bidang 3: Kawalan Aset dan Pengkelasan Maklumat
- Bidang 4: Keselamatan Sumber Manusia
- Bidang 5: Keselamatan Fizikal dan Persekitaran
- Bidang 6: Pengurusan Operasi dan Komunikasi
- Bidang 7: Kawalan Capaian
- Bidang 8: Pembangunan dan Penyelenggaraan Sistem
- Bidang 9: Pengurusan Pengendalian Insiden Keselamatan
- Bidang 10: Pengurusan Kesinambungan Perkhidmatan
- Bidang 11: Pematuhan

Bidang 1: Pembangunan dan Penyelenggaraan Dasar

Pelaksanaan Dasar	Penyebaran Dasar	Penyelenggaraan Dasar	Pengecualian Dasar
Pengerusi JPICT JPP	Perlu disebarkan kepada semua warga dan pihak yang terlibat	Perlu disemak dan pindaan dari masa ke semasa	Terpakai kepada semua pengguna dan tiada pengecualian
- CIO - **Pengurus ICT** - ICTSO - Pengarah Bahagian	- Emel - Poster - Iklan	- Kenalpasti dan tentukan perubahan - Kemuka cadangan bertulis - Dapatkan kelulusan	

Bidang 2: Organisasi Keselamatan

Infrastruktur Keselamatan Organisasi

Ketua Pengarah

- Pastikan pengguna memahami DKICT
- Pastikan pengguna mematuhi DKICT
- Pastikan keperluan organisasi mencukupi
- Pastikan program keselamatan ICT dilaksanakan
- Memperakui proses tindakan tatatertib ke atas pengguna yang melanggar DKICT

CIO

- Membantu KP dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT
- Menentukan keperluan keselamatan
- Membangun dan menyelaras pelan latihan dan program kesedaran mengenai keselamatan ICT
- Bertanggungjawab ke atas perkara yang berkaitan keselamatan ICT

ICTSO

- Mengurus keseluruhan program keselamatan ICT
- Menguatkuasakan DKICT
- Memberi penerangan dan pendedahan berkenaan dengan DKICT
- Mewujudkan garis panduan, prosidur dan tatacara selaras dengan keperluan DKICT
- Menjalankan pengurusan risiko

Bidang 2: Organisasi Keselamatan

Pengurus ICT

- Membaca, memahami dan mematuhi DKICT
- Mengkaji dan melaksanakan kawalan keselamatan ICT
- Menentukan kawalan akses semua pengguna terhadap asset ICT
- Melaporkan penemuan mengenai pelanggaran DKICT kepada ICTSO
- Menyimpan rekod, bahan bukti dan laporan terkini berkenaan dengan ancaman keselamatan ICT

Pentadbir Sistem

- Mengambil tindakan segera jika berlaku perubahan kakitangan
- Menentukan ketepatan tahap capaian berdasarkan pemilik sistem
- Memantau aktiviti capaian pengguna
- Mengenalpasti aktiviti tidak normal seperti pencerobohan data
- Menyimpan dan menganalisis rekod jejak audit

Pegawai Aset ICT

- Memantau setiap perkakasan ICT yang diagihkan kepada pengguna
- Memastikan aset dilabel dan direkod
- Memastikan aset ICT untuk pinjaman dan simpanan diletakkan di dalam bilik yang mempunyai kawalan
- Memastikan aset ICT yang ingin dilupuskan dilaksana mengikut garis panduan

Bidang 2: Organisasi Keselamatan

Pengguna

- Membaca, memahami dan mematuhi DKICT
- Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya
- Menjalani tapisan keselamatan sekiranya perlu
- Melaksanakan prinsip-prinsip DKICT dan menjaga kerahsiaan maklumat
- Menghadiri program-program kesedaran keselamatan ICT
- Menandatangani surat akuan pematuhan DKIC

JPICT

- Memperaku/Meluluskan dokumen DKICT
- memantau tahap pematuhan keselamatan ICT
- Memperaku garis panduan, prosidur dan tatacara untuk aplikasi khusus dalam JPP dan Politeknik
- Memastikan DKICT JPP selaras dengan dasar ICT kerajaan
- Menerima laporan dan membincangkan hal-hal keselamatan ICT
- Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden

CERT

- Merupakan Pasukan Tindak Balas Insiden Keselamatan ICT
- menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden
- menjalankan siasatan awal insiden yang diterima
- menangani tindak balas insiden keselamatan ICT dan mengambil tindakan pemulihan
- Menyebar maklumat berkaitan pengukuhan keselamatan ICT

Bidang 2: Organisasi Keselamatan

Pihak Ketiga: Pembekal, Pakar Runding dan lain-lain

- Membaca, memahami dan mematuhi DKICT
- Mengenalpasti risiko keselamatan maklumat dan melaksanakan kawalan capaian

- Mengenalpasti keperluan keselamatan sebelum memberi kebenaran kepada pihak ketiga
- Akses kepada aset ICT perlu berlandaskan perjanjian kontrak

- Semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian
- Menandatangani Surat Akuan Pematuhan DKICT

Bidang 3: Kawalan Aset dan Pengkelasan Maklumat

InventoriAset

Memastikan semua aset ICT diberi kawalan dan perlindungan

- Dikenalpasti dan direkod dalam borang harta modal
- Kenalpasti lokasi aset
- Peraturan bagi pengendalian aset ICT dikenalpasti

Pengelasan Maklumat

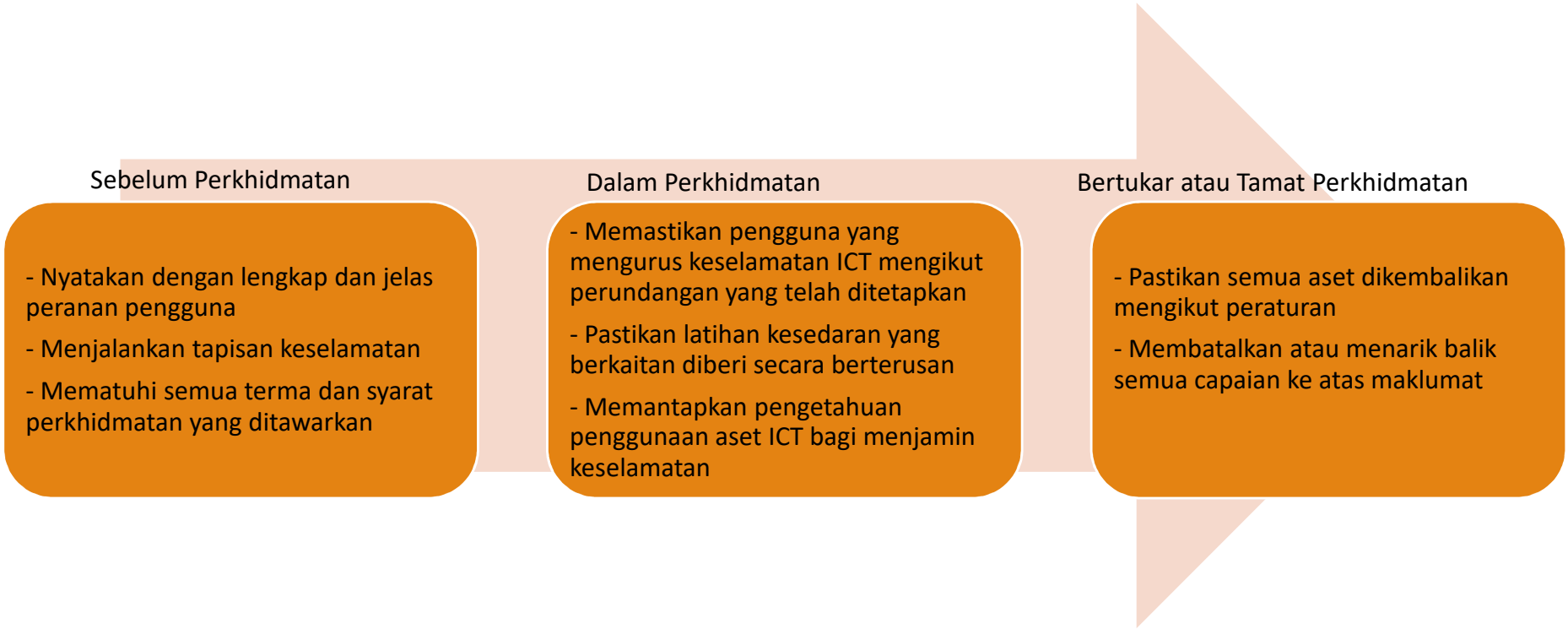
Perlu dikelaskan dan dilabel dengan sewajarnya dan mempunyai peringkat keselamatan seperti yang telah ditetapkan.

Pengendalian Maklumat

Aktiviti pengendalian maklumat perlu mengambilkira langkah keselematan berikut:

- Menghalang pendedahan
- Memeriksa maklumat agar lengkap dan tepat
- Menjaga rahsia kata laluan

Bidang 4: Keselamatan Sumber Manusia



Bidang 5: Keselamatan Fizikal dan Persekitaran

Keselamatan Kawasan: melindungi premis dan maklumat daripada sebarang bentuk pencerobohan

Kawalan Kawasan

- Menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi:
  - Memasang kamera atau alat penggera
  - Mengadakan kaunter kawalan
  - Menyediakan bilik khas untuk pelawat

Kawalan Masuk Fizikal

- Setiap kakitangan perlu memakai kad ID Jabatan sepanjang masa waktu bertugas
- Kad ID Jabatan perlu diserahkan balik jika berhenti atau bersara atau berpindah keluar
- Setiap pelawat perlu mendaftar dan mendapatkan pas pelawat
- Kehilangan pas pelawat mesti dilaporkan segera

Kawasan Larangan

- Kawasan Larangan di JPP adalah bilik KP, TKP, Bilik Server dan lain-lain bilik yang diwartakan sebagai kawasan larangan

Bidang 5: Keselamatan Fizikal dan Persekitaran

Keselamatan Peralatan: melindungi peralatan ICT dari kehilangan, kerosakan dan kecurian

Peralatan ICT

- Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna
- Pengguna bertanggungjawab sepenuhnya ke atas perkakasan ICT masing-masing dan tidak dibenarkan membuat pertukaran tanpa kebenaran
- Pengguna dilarang menambah, menanggal atau menggantikan sebarang perkakasan ICT yang telah ditetapkan
- Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah seliaannya.

Media Storan

- Media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan
- Pergerakan media storan hendaklah direkod
- Mengadakan Salinan pada media storan kedua bagi tujuan keselamatan dan mengelakkan kehilangan data
- Media storan yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat

Media Perisian dan Aplikasi

- Hanya perisian yang diperakui sahaja dibenarkan
- Sistem aplikasi dalaman tidak dibenarkan didemonstasi atau diagih kepada pihak lain kecuali dengan kebenaran
- Lesen perisian perlu disimpan berasingan daripada CD-ROM atau media berkaitan bagi mengelakkan kecurian
- Source code sesuatu sistem hendaklah disimpan dengan baik

Bidang 5: Keselamatan Fizikal dan Persekitaran

Keselamatan Peralatan: melindungi peralatan ICT dari kehilangan, kerosakan dan kecurian - sambungan

Penyelenggaraan

- Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti
  - Diselenggara oleh pihak yang dibenarkan sahaja
  - Hendaklah disemak dan diuji sebelum dan selepas penyelenggaraan
  - Mesti mendapat kebenaran sebelum ia dilaksanakan
  - Aktiviti penyelenggaraan perlu direkodkan

Peminjaman Perkakasan Untuk Kegunaan Luar Pejabat

- Mesti mendapat kelulusan Ketua Jabatan
- Aktiviti peminjaman dan pemulangan direkod dengan baik

Peralatan di Luar Premis

- Dilindungi dan dikawal sepanjang masa penyimpanan dan penempatan peralatan mestilah mengambilkira ciri-ciri keselamatan

Pelupusan

- Hendaklah dilupuskan melalui proses pelupusan semasa
- Dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan

Bidang 5: Keselamatan Fizikal dan Persekitaran

Keselamatan Persekitaran

Kawalan Persekitaran

- Semua cadangan berkaitan dengan premis samada pengubahsuaian, pembelian, penyewaan hendaklah mendapat kelulusan Pegawai Keselamatan Jabatan yang dilantik
- Susun atur pusat data, peralatan ICT perlu dirancang dengan baik
- Bahan mudah terbakar, bahan cecair perlu berjauhan dengan aset ICT

Bekalan Kuasa

- Peralatan sokongan (UPS) boleh digunakan di Bilik Server
- Peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual

Kabel

- Menggunakan kabel yang memenuhi spesifikasi
- Melindungi kabel dan laluan kabel dari kerosakan
- Perlu dilabel dengan jelas

Bidang 5: Keselamatan Fizikal dan Persekitaran

Keselamatan Dokumen

- Setiap dokumen hendaklah difail dan dilabelkan mengikut spesifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar.
- Pergerakan fail dan dokumen hendaklah direkodkan dan mengikut prosidur keselamatan
- Kehilangan dan kerosakan perlu dimaklumkan
- Pelupusan dokumen hendaklah mengikut prosidur keselamatan
- Menggunakan enkripsi ke atas dokumen rahsia rasmi bagi penghantaran secara elektronik

Bidang 6: Pengurusan Operasi dan Komunikasi

Pengurusan Prosidur Operasi: memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat

Pengendalian Prosidur	Kawalan Perubahan	Pengasingan Tugas dan Tanggungjawab
• Semua prosidur hendaklah didokumenkan, disimpan dan dikawal • Mengandungi arahan yang jelas, lengkap • Sentiasa dikemaskini	• Pengubahsuaian perkakasan, sistem, perisian perlu mendapat kelulusan Pegawai Atasan atau pemilik aset ICT • Aktiviti memasang, menyelenggara, menghapus mana-mana komponen ICT hendaklah dibuat oleh pegawai yang diberi kuasa atau berkelayakan • Mestilah direkod dan dikawal	• Perlu diasingkan bagi mengurangkan peluang penyalahgunaan • Perkakasan untuk pembangunan diasingkan dari *production*

Bidang 6: Pengurusan Operasi dan Komunikasi

Perancangan dan Penerimaan Sistem: meminimumkan risiko gangguan atau kegagalan sistem

Sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti

Mengandungi ciri-ciri keselamatan ICT bagi mengurangkan risiko gangguan dan kerugian akibat pengubahsuaian

Sistem aplikasi hendaklah memenuhi kriteria yang telah ditetapkan sebelum diterima atau dipersetujui

Bidang 6: Pengurusan Operasi dan Komunikasi

Pengurusan Pertukaran Maklumat: Memastikan pertukaran maklumat dengan pihak luar terjamin

Pertukaran Maklumat

- Dasar, prosidur dan kawalan pertukaran maklumat yang formal perlu diwujudkan
- Perjanjian perlu diwujudkan antara JPP dan agensi luar
- Media yang mengandungi maklumat perlu dilindungi semasa pemindahan keluar
- Maklumat di dalam emel perlu dilindungi sebaiknya

Mel Elektronik

- Akaun emel jabatan sahaja boleh digunakan. Dilarang berkongsi atau menggunakan akaun emel orang lain
- Memastikan subjek dan kandungan emel adalah berkaitan dengan perbincangan sebelumnya
- Penghantaran emel rasmi hendaklah menggunakan akaun emel rasmi
- Elakkan membuka emel yang diragui
- Mengambil tindakan dan maklum balas dengan cepat
- Penggunaan emel persendirian TIDAK DIGUNAKAN untuk tujuan rasmi
- Pengguna bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing

Bidang 7: Kawalan Capaian

Bidang 8: Pembangunan dan Penyelenggaraan Sistem

Bidang 9: Pengurusan Pengendalian Insiden Keselamatan

Mekanisma Pelaporan Insiden Keselamatan

- Pastikan inciden dikendali dengan cepat dan berkesan
- Perlu dilaporkan kepada ICTSO dan CERT dengan segera
- Cth: kehilangan maklumat, kehilangan fail, sistem kerap kali gagal

Pengurusan Maklumat Insiden Keselamatan ICT

- Memastikan pendekatan yang konsisten dan efektif dalam pengurusan maklumat insiden
- Maklumat perlu disimpan dan dianalisis bagi tujuan tindakan pengukuhan dan pembelajaran
- Bahan bukti perlu disimpan dan diselenggara
- Cth kawalan: simpan jejak audit, *backup* secara berkala, salin bahan bukti

Bidang 10: Pengurusan Kesinambungan Perkhidmatan

Menjamin perkhidmatan yang berterusan

Perlu bangunkan Pelan Kesinambungan Perkhidmatan (Business Continuity Management BCM) – tentukan pendekatan yang menyeluruh diambil	BCM perlu diluluskan oleh JPICT - Kenalpasti semua tanggungjawab dan prosidur kecemasan / pemulihan - Kenalpasti peristiwa yang menyebabkan gangguan terhadap proses - Melaksanakan prosidur kecemasan bagi memastikan pemulihan dapat dibuat secepat mungkin - Dokumentasikan semua prosidur - Mengadakan program latihan - Membuat pendua	BCM perlu mengandungi: - Senarai aktiviti teras yang dianggap kritikal - Senarai kakitangan dan vendor serta nombor untuk dihubungi jika berlaku insiden - Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanan - Alternatif sumber pemprosesan dan lokasi yang lumpuh - Perjanjian dengan pembekal perkhidmatan untuk mendapatkan penyambungan semula perkhidmatan

Bidang 11: Pematuhan

- Semua pengguna hendaklah membaca, memahami dan mematuhi DKICT serta menandatangani Surat Akuan Pematuhan
- Semua aset termasuk maklumat yang disimpan adalah hak milik Kerajaan Malaysia
- Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard
- Keperluan audit dan aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui
- Senarai perundangan dan peraturan seperti di Lampiran 2
- Pelanggaran DKICT boleh dikenakan tindakan tatatertib

Sekian, Terima Kasih