APA ITU DKICT ?

Dasar Keselamatan ICT (DKICT) ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) di KPWKM dan Agensi

OBJEKTIF

01

- Diwujudkan untuk menjamin kesinambungan urusan Jabatan dengan meminimumkan kesan insiden keselamatan ICT

02

- Untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Jabatan

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

Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan.

Mencegah salah guna atau kecurian aset ICT Kerajaan.

Memperkemaskan pengurusan keselamatan ICT KPWKM.

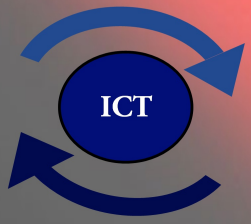
Memastikan kelancaran operasi Jabatan dan meminimumkan kerosakan atau kemusnahan.

OBJEKTIF DKICT

Sumber : Dasar Keselamatan ICT KPWKM V.3.6

KOMPONEN ASAS KESELAMATAN

1. Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan dari capaian tanpa kuasa yang sah.
2. Menjamin setiap maklumat adalah tepat dan sempurna.
3. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna.
4. Memastikan akses kepada hanya pengguna-pengguna yang sah atau menerima maklumat dari sumber yang sah.



Sumber : Dasar Keselamatan ICT KPWKM V.3.6

PENGURUSAN E-MEL
@kpwkm.gov.my

- Elakkan membuka e-mel daripada penghantar yang tidak diketahui atau diragui.
- Laksanakan *housekeeping* e-mel secara berkala.
- Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan segera.
- Kenal pasti dan sahkan identiti pengguna sebelum meneruskan transaksi maklumat.
- Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang.
- Setiap e-mel rasmi yang dihantar atau diterima hendaklah diuruskan mengikut tatacara yang betul.

MyGovuC 2.0

Pastikan anda sentiasa membuka "Emel Rasmi"
SETIAP HARI

Sumber : Dasar Keselamatan ICT KPWKM V.3.6

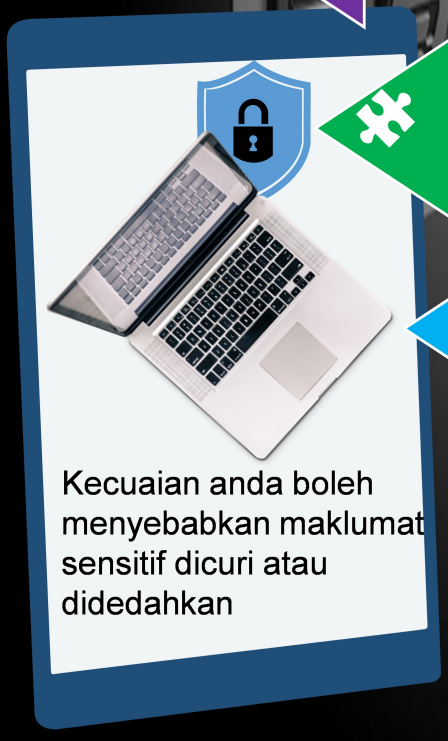
PENGURUSAN KATA LALUAN

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur

INFO KESELAMATAN ICT

Dalam apa jua keadaan dan sebab kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun

Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara (huruf), angka (nombor) dan aksara khusus (simbol)



Kecuaian anda boleh menyebabkan maklumat sensitif dicuri atau didedahkan

Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi

Kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun

Mengelakkan penggunaan semula kata laluan yang baru digunakan

Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama

Sumber : Dasar Keselamatan ICT KPWKM V.3.6

CLEAR DESK & CLEAR SCREEN

Bermaksud tidak meninggalkan bahan-bahan sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.

Kecuaian anda boleh menyebabkan maklumat sensitif dicuri atau didedahkan!

Peranti storan mudah alih yang digunakan untuk menyimpan maklumat sulit ditinggalkan di atas meja (contoh : *Pendrive* USB)

Fail-fail berlabel sulit atau rahsia dibiarkan tanpa pengawasan

Dokumen yang mengandungi maklumat sensitif tidak dirincih sebelum dibuang ke dalam tong sampah

Tidak log keluar sistem aplikasi serta membiarkan skrin monitor terpasang tanpa dikunci dengan "*screen saver*"

Nota-nota kecil yang mengandungi maklumat sulit dipamerkan (contoh : kata laluan)

Sumber : Dasar Keselamatan ICT KPWKM V.3.6