



POLISI DASAR KESELAMATAN ICT PEJABAT DAERAH DAN TANAH PERAK TENGAH, SERI ISKANDAR



1. **Gunakan Kata Laluan**

- ❖ Gunakan kata laluan yang kreatif (gabungan huruf , nombor dan simbol).
- ❖ Elakkan daripada mendedah kata laluan kepada orang lain.
- ❖ Sentiasa menukar kata laluan secara berkala dan elak dari menggunakan kata laluan yang sama atau berulang.
- ❖ Sulitkan (*encrypt*) penghantaran dokumen rasmi kerajaan dengan kata laluan.
- ❖ Elakkan menghantar dokumen rasmi kerajaan bersama-sama dengan kata laluan.

2. **Kemaskini perisian keselamatan**

- ❖ Lengkapkan komputer dan gajet dengan perisian keselamatan (seperti *anti – virus* atau *anti – spyware*) terkini.
- ❖ Elakkan daripada menggunakan perisian keselamatan yang telah tamat tempoh.
- ❖ Gunakan perisian tulen.

3. Simpan dan lindungi maklumat

- ❖ Elakkan daripada memuat naik dokumen rasmi kerajaan dalam *public cloud*.
- ❖ Sentiasa imbas peranti storan sebelum menggunakannya.
- ❖ Sentiasa sediakan salinan pendua (*backup*) maklumat digital secara berkala.
- ❖ Elakkan meninggalkan komputer atau gajet tanpa sebarang pengawasan.
- ❖ Putuskan sambungan internet atau *wi-fi* sekiranya tidak menggunakannya lagi.
- ❖ Pastikan meja kerja dikemas dan semua maklumat rasmi (termasuk yang berada di dalam media storan) disimpan di tempat yang selamat dan berkunci.

5. Beretika ketika menggunakan Internet dan emel rasmi kerajaan

- ❖ Pastikan alamat emel dan kata laluan rasmi tidak digunakan dalam akaun peribadi media sosial.
- ❖ Elakkan daripada berkongsi maklumat peribadi dan maklumat berkaitan tugas rasmi di internet dan media social.
- ❖ Elakkan memuat turun sebarang aplikasi yang tidak diketahui tahap keselamatannya.

6. **Waspada jenayah siber**

- ❖ Jangan benarkan individu lain menggunakan identiti dan kata laluan akaun emel dan media.
- ❖ Elakkan daripada melayari laman web dan blog yang berunsur lucah, fitnah , hasutan, skim cepat kaya dan ideology keganasan.
- ❖ Elakkan dari menyebarkan kandungan berunsur lucah, fitnah , hasutan, skim cepat kaya dan ideologi keganasan.

7. **Fikir dulu sebelum klik**

- ❖ Jangan klik pada emel, pautan atau lampiran yang mencurigakan (termasuk orang yang tidak dikenali). Padamkan emel tersebut.

8. **Laporkan**

- ❖ Laporkan dengan segera kehilangan sebarang aset ICT Kerajaan (seperti peranti storan, komputer riba, komputer).
- ❖ Laporan emel atau pautan yang mencurigakan atau dari orang yang tidak dikenali kepada Unit Teknologi Maklumat.
- ❖ Laporan kepada pihak berkuasa sekiranya berlaku sebarang insiden jenayah siber seperti penipuan internet.

9. **Ambil Tahu**

- ❖ Peka dengan tren ancaman siber terkini.
- ❖ Peka, fahami dan waspada mengenai kesan-kesan negatif akibat penyalahgunaan internet.

10. **Patuhi**

- ❖ Ketahui dan patuhi polisi, arahan, peraturan, garis panduan dan pekeliling berkaitan keselamatan siber yang dikeluarkan oleh agensi/organisasi anda dan kerajaan.