GARIS PANDUAN KESELAMATAN ICT DI PDTAG

A. OBJEKTIF

1. Memastikan kelancaran operasi jabatan yang berlandaskan ICT dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT jabatan;

2. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan;

3. Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;

4. Meningkatkan tahap kesedaran keselamatan ICT kepada para kakitangan, pengguna dan pembekal;

5. Memperkemaskan pengurusan risiko;

6. Mencegah penyalahgunaan atau kecurian aset ICT jabatan;

7. Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

B. CIRI-CIRI UTAMA KESELAMATAN

i. **KERAHSIAAN** - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan akses tanpa kebenaran.

ii. **INTEGRITI** - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan.

iii. **TIDAK BOLEH DISANGKAL** - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.

iv. **KESAHIHAN** - Data dan maklumat hendaklah dijamin kesahihannya.

v. **KEBOLEHSEDIAAN** - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

C. KESELAMATAN PERALATAN OLEH PENGGUNA ICT

i. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

ii. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

iii. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;

iv. Pengguna mesti memastikan perisian *antivirus* bagi semua peralatan ICT yang dibekalkan oleh Jabatan seperti komputer peribadi, *notebook, server* termasuk alat komunikasi mudah alih (*Personal Digital Assistant*, *Blackberry, smartphone* dan sebagainya) yang berada di bawah tanggungjawab mereka sentiasa aktif (*activated*) dan dikemas kini di samping turut melakukan imbasan ke atas media storan yang digunakan;

v. Semua peralatan sokongan ICT hendaklah dilindungi daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salahguna;

vi. Aset ICT hendaklah disimpan di tempat yang selamat dan sentiasa di bawah kawalan pegawai yang bertanggungjawab. Arahan Keselamatan Kerajaan hendaklah sentiasa dipatuhi bagi mengelak berlakunya kerosakan atau kehilangan aset;

vii. Peralatan ICT yang hendak dibawa keluar dari premis perlulah mendapat kelulusan Pegawai Aset atau Penyelaras ICT bagi tujuan pemantauan.

D. PENGGUNAAN INTERNET

i. Penggunaan kemudahan internet hendaklah mengikut etika, garis panduan dan prosedur keselamatan penggunaan internet yang ditetapkan.

ii. Pegawai hanya boleh melayari laman web yang dibenarkan sahaja dan dilarang melayari, menyedia, memuat naik (upload), memuat turun (download) dan menyimpan laman web yang mengandungi unsur-unsur lucah, hasutan dan ancaman terhadap keselamatan negara.

iii. Pegawai adalah dilarang menggunakan kemudahan internet untuk tujuan peribadi seperti memuat turun, menyimpan serta menggunakan perisian berbentuk hiburan (permainan elektronik, video, muzik, gambar, chatting atau seumpamanya) yang boleh mengganggu kestabilan talian rangkaian (networking).

iv. Pegawai bertanggungjawab mematuhi sepenuhnya etika, garis panduan dan prosedur keselamatan internet yang ditetapkan.

E. PENGGUNAAN EMEL RASMI

i. Emel adalah merupakan rekod awam. Penggunaan emel tertakluk kepada peraturan yang ditetapkan dan boleh ditarik balik jika pegawai menyalahi peraturan.

ii. Penggunaan kemudahan emel mestilah mengikut etika, garis panduan dan prosedur keselamatan penggunaan emel yang ditetapkan.

iii. Pegawai harus bertindak bijak, profesional dan berhati-hati dalam menggunakan kemudahan emel yang diberi.

iv. Pegawai harus menggunakan identiti/ akaun emel sendiri apabila menggunakan kemudahan emel dan dilarang menggunakan kemudahan emel untuk tujuan peribadi seperti menyebar, menghantar dan melibatkan diri dalam emel yang mengandungi kod perosak, unsur-unsur lucah, hasutan, ancaman dan emel sampah yang dapat mengganggu penggunaan emel milik orang lain.

F. PERANAN DAN TANGGUNGJAWAB PENGGUNA ICT

- Pengguna ICT dan pihak luaran perlu membaca, memahami dan mematuhi Panduan Keselamatan ICT;
- Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;
- Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;
- Melaksanakan prinsip-prinsip Panduan Keselamatan ICT dan menjaga kerahsiaan maklumat jabatan:
- Melaksanakan langkah-langkah perlindungan seperti berikut:

i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
iii. menentukan maklumat sedia untuk digunakan;
iv. menjaga kerahsiaan kata laluan;
v. mematuhi standard, prosedur, langkah dan garis panduan keselamatan ICT yang ditetapkan;
vi. melaksanakan peraturan berkaitan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;
vii. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.