Amalan Terbaik Keselamatan ICT Sektor Awam Negeri
(State Public Sector ICT Security Best Practices)

Berikut adalah sebahagian daripada amalan-amalan terbaik yang digalakkan perlu diikuti oleh semua kakitangan kerajaan negeri untuk kebaikan bersama demi untuk mengurangkan risiko ancaman bukan sahaja kepada keselamatan maklumat di tempat masing-masing tetapi kepada semua aset IT kerajaan negeri. Maklumat lanjut boleh didapati di laman web Bahagian Keselamatan, Jabatan Perkhidmatan Komputer Negeri: http://www.jpkn.sabah.gov.my/bk/

1) Lindungi maklumat peribadi anda.
Untuk meminimakan risiko kecurian identiti anda, perkongsian maklumat peribadi anda tidak digalakkan. Gunakan budi bicara sendiri sebelum berkongsi maklumat di laman sosial media seperti Facebook, MySpace, LinkedIn dan Twitter.

2) Lindungi katarahsia anda.
Katarahsia anda perlulah kukuh dan sukar diteka tapi senang diingat. Jangan sesekali berkongsi katarahsia anda dengan orang lain. Kalau pun katarahsia anda perlu ditulis, adalah digalakkan untuk menyimpannya di tempat yang selamat.

3) Lindungi komputer anda setiap masa.
Digalakkan penggunaan katarahsia untuk mengakses komputer anda. Apabila anda meninggalkan komputer anda untuk jangka masa yang pendek, gunakan kemudahan 'mengunci' supaya komputer anda tidak akan digunakan oleh orang lain. Jangan sama sekali tinggalkan *notebook* anda di tempat awam.

4) Selalu buat salinan kepada fail-fail penting.
Buat salinan kepada fail yang dianggap penting di media luaran seperti USB *thumb drive* dan *external harddisk* dan simpan di tempat yang selamat.

5) Jangan buka sebarang fail yang anda sangsi puncanya.
Jangan buka fail sertaan (*e-mail attachments*) terutama yang mempunyai sambungan ".exe" jika anda ragu-ragu atau tidak mengenali pengirimnya.

6) Elakkan dari mengajukan e-mel berupa spam dan e-mel rantaian (*chain e-mails*).
Anda dinasihati supaya tidak mengajukan sebarang emel yang menunjukkan ciri-ciri spam atau rantaian e-mel yang antara lainnya berbunyi "Please forward this e-mail to 10 of your friends". E-mel seperti ini tidak mendatangkan faedah dan yang pastinya, akan memudaratkan operasi rangkaian SabahNet.

7) Elakkan dari menginstal perisian yang anda ragu-ragu puncanya.
Hanya muat turun dan instal perisian dari punca yang dipercayai dengan reputasi yang baik. Perisian cetak rompak (*pirated software*) adalah dilarang sama sekali untuk diinstal dalam aset IT kerajaan kerana perisian seperti ini adalah sukar dikemaskini atau pengemaskinian yang perlu selalunya tidak berjaya. Ini akan membuka ruang kepada ancaman keselamatan seperti mudah dijangkiti virus dan senang digodam.

8) Segala perisian dan sistem operasi perlulah dikemaskini selalu.
Sistem operasi komputer anda perlu dikonfigurasikan supaya pengemaskinian dapat dilakukan secara otomatik apabila tiba masanya. Pengemaskinian ini adalah bertujuan untuk memperbaiki kelemahan-kelemahan sekuriti yang timbul dalam sistem operasi tersebut. Begitu juga perisian-perisian yang lain, perlu dikemaskini selalu.

9) Gunakan perisian antivirus dan *firewall* yang bertauliah.
Perisian antivirus digunakan untuk meminimakan serangan wabak virus dan *firewall* pula perlu untuk mengurangkan risiko serangan penggodaman. Oleh kerana ancaman selalu berubah, adalah disyorkan perisian antivirus dan *firewall* dikemaskinikan selalu.

10) Laporkan sebarang pencorobohan data dan kehilangan komputer dengan kadar segera.
Sebarang pencorobohan ke atas laman web jabatan perlu dilaporkan kepada team@sgcert.org (Sabah Government Computer Emergency Response Team) untuk tindakan lanjut. Kehilangan komputer, *notebook* dan media storan mudah alih yang mengandungi data sensitif perlu dilaporkan kepada pihak polis untuk penyiasatan lanjut.

Disediakan oleh:

Bahagian Keselamatan,
Jabatan Perkhidmatan Komputer Negeri,
Tingkat 2, Blok B, Wisma Kewangan,
88999 Kota Kinabalu, Sabah.