# *PANDUAN KESELAMATAN ICT*

## TUJUAN

Tujuan Panduan ini adalah untuk memaklumkan peraturan-peraturan yang perlu dipatuhi untuk menjaga keselamatan aset Teknologi Maklumat dan Komunikasi (ICT). Dengan adanya peraturan ini adalah diharapkan tahap keselamatan dapat ditingkatkan.

## PERNYATAAN DASAR KESELAMATAN

2. Keselamatan ICT merangkumi perlindungan keatas semua bentuk maklumat elektronik bertujuan untuk menjamin kerahsiaan, integriti, kesahihan dan kebolehsediaan kepada semua pengguna yang dibenarkan.

3. Maklumat adalah merupakan hasil terakhir sesuatu sistem pengkomputeran dan dengan itu ianya amat penting dan bernilai bagi sesebuah organisasi. Kehilangan atau kemusnahan data/maklumat yang disimpan di dalam komputer sering berlaku disebabkan oleh kejadian-kejadian seperti kebakaran, pengkhianatan, kecuaian dan kecurian. Bagi mengatasi masalah ini, kawalan ke atas capaian data/ maklumat dan keselamatan fizikal perlu diperketatkan. Disamping itu data/ maklumat yang penting perlu dibuat salinan yang secukupnya dan disimpan dibangunan berasingan. Data/ maklumat yang dicuri melalui talian komunikasi data dapat dicegah dengan teknik yang lebih rumit misalnya dengan menggunakan kaedah penyulitan (encryption).

**SKOP**

4. Keselamatan ICT merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasuk, diwujud, dimusnah, disimpan, dihasil, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan keselamatan kedalam semua komponen komputer atau rangkaian.

**RUJUKAN**

5. Dokumen-dokumen berikut adalah berkaitan atau dirujuk dalam panduan ini:

- Arahan Keselamatan Kerajaan;
- Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan;
- Pekeliling dan Surat Pekeliling yang berkaitan;
- LAN Administrator's Guidelines for NetWare; dan
- Pekeliling Am Bil. 3 Tahun 2000

Sebarang pertanyaan hendaklah dialamatkan ke **Meja Bantuan 03-88881717**.

**TERMINOLOGI**

6. Teminologi berikut akan digunakan dalam Panduan ini bagi menjelaskan mengenai keselamatan.

| | |
|---|---|
| ***Keselamatan*** | *Daripada perspektif ICT, keselamatan merujuk kepada perlindungan sumber ICT daripada dicerobohi oleh mereka yang tidak dibenarkan atau kesilapan yang disengajakan..* |
| ***Server*** | *Server merujuk kepada komputer yang berkeupayaan tinggi yang berfungsi sebagai pelayan perkhidmatan dalam sesuatu rangkaian..* |
| ***Perisian Sistem*** | *Perisian Sistem merujuk kepada sistem pengoperasian seperti Windows 95/98 bagi komputer mikro dan NetWare/ Windows NT pada Server.* |
| ***Perisian Aplikasi*** | *Perisian aplikasi merujuk kepada pakej yang selalu digunakan seperti spreadsheet dan word processing, juga aplikasi yang dibangunkan bagi tujuan tertentu..* |
| ***Virus*** | *Virus adalah subersif program komputer yang boleh mengakibatkan fail komputer mengalami kerosakan atau terhapus dan mungkin menukar tingkahlaku operasi komputer.* |

| | |
|---|---|
| ***Rahsia Besar*** | *Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia..* |
| ***Rahsia*** | *Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.* |
| ***Sulit*** | *Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.* |
| ***Terhad*** | *Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakan juga diberi satu tahap perlindungan keselamatan..* |

| | |
|---|---|
| ***Kerahsiaan*** | *Maklumat/data tidak boleh didedahkan sewenang-wenangnya atau dibiarkan dicapai tanpa kebenaran..* |
| ***Integriti*** | *Maklumat/data hendaklah tepat, lengkap dan hanya boleh diubah dengan cara yang dibenarkan..* |
| ***Kebolehsediaan*** | *Maklumat/data dan sistem maklumat hendaklah boleh diakses dan digunakan bila dan apabila diperlukan mengikut fungsi..* |

**OBJEKTIF DASAR KESELAMATAN ICT**

7. Objektif Keselamatan ICT termasuklah:

(a) Memastikan kelancaran operasi Kerajaan berterusan, meminimumkan kerosakan atau kemusnahan melalui usaha pencegahan atau usaha mengurangkan kesan kejadian yang tidak diingini;

(b) Melindung kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada akibat kegagalan atau usaha melemahkan kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;

(c) Mencegah salahguna atau kecurian sumber dan aset ICT kerajaan.

**TUGAS DAN TANGGUNGJAWAB**

8. Tanggungjawab perlindungan ICT dikategorikan kepada tiga (3) peranan seperti berikut:

**(a) Pemilik**

Maklumat yang diproses oleh sistem komputer mestilah mempunyai pemilik yang sah. Pemilik mungkin memberikuasa pemilikan kepada individu lain. Pemilik maklumat mempunyai kuasa dan tanggungjawab untuk:

(i) Menentukan nilai maklumat dan klasifikasinya;
(ii) Memberi akses kepada pengguna yang layak selaras dengan tugas pengguna;
(iii) Menentukan kawalan dan menetapkan keperluan kawalan kepada penjaga dan pengguna maklumat; dan
(iv) Menyediakan keterangan terperinci mengenai keperluan "*back-up*" dan arkib serta memaklumkan keperluan-keperluan ini kepada penjaga.

**(b) Penjaga**

Bahagian Teknologi Maklumat (BTM) diberikuasa dan bertanggungjawab dalam mentadbir, menyimpan dan mengawal data/maklumat seperti:

(i) Menyediakan keselamatan fizikal;
(ii) Menyediakan prosedur keselamatan;
(iii) Mentadbir capaian kepada maklumat; dan
(iv) Menilai keberkesanan kawalan.

**(c) Pengguna**

Pengguna adalah mana-mana individu yang telah diberi kuasa untuk membaca atau memasukkan atau mengemaskini maklumat. Pengguna sesuatu maklumat mempunyai tanggungjawab dalam perkara-perkara berikut:

(i) Menggunakan maklumat hanya seperti yang ditetapkan oleh pemilik sahaja;
(ii) Mematuhi dengan semua kawalan yang ditetapkan oleh pemilik dan penjaga; dan
(iii) Tidak mendedahkan maklumat dalam apa jua bentuk kepada sesiapa tanpa kebenaran yang NYATA daripada pemilik.

**PENGKELASAN DATA/ MAKLUMAT DAN PENGLABELAN**

9. Klasifikasi maklumat hendaklah mematuhi "Arahan Keselamatan" perenggan 53, mukasurat 15 dimana maklumat dikategorikan kepada **Rahsia Besar, Rahsia, Sulit dan Terhad**. Perkara-perkara berikut hendaklah dipatuhi dalam mengendalikan bahan/data/maklumat berbentuk elektronik:

(a) Akses terhadap data/maklumat hanya akan diberikan bagi tujuan spesifik dan dihadkan kepada pengguna tertentu dan hanya akan diberikan atas dasar "Perlu Mengetahui" sahaja mengikut klasifikasi maklumat. Ini bergantung kepada tapisan keselamatan pengguna;

(b) Penglabelan semua media menyimpan maklumat mengikut klasifikasi dan warna misalnya merah bagi Rahsia/Rahsia Besar, hijau bagi peringkat Sulit dan putih bagi Terhad;

(c) Pastikan maklumat yang hendak dikirim menggunakan disket atau media elektronik hanya data/maklumat yang betul; dan

(d) Penyimpanan bahan/data/maklumat berbentuk elektronik hendaklah mengikut peraturan Arahan Keselamatan.

10. Data/bahan/maklumat rasmi yang sensitif atau bersifat terperingkat perlu dilindungi dari pendedahan, dimanipulasi atau diubah semasa dalam penghantaran. Penggunaan kod penyulitan atau tandatangan digital mesti dipertimbangkan bagi melindungi data yang dikirim secara elektronik.

11. Dasar kawalan akses ke atas aplikasi/ sistem hendaklah menurut klasifikasi maklumat samada Rahsia Besar, Rahsia, Sulit atau Terhad.

**KAWALAN SISTEM KOMPUTER**

12. Apabila pengguna diberi kebenaran untuk menggunakan sistem atau rangkaian, adalah perlu untuk menghadkan kebenaran tersebut ke tahap set yang paling minima bersamaan dengan keperluan melaksanakan tugas yang efektif. Pada kebiasaannya had akses minimum bermakna tidak boleh akses. Seterusnya akses untuk membaca atau melihat sahaja, mewujud, kemaskini, mengubah atau memadam boleh diberikan tetapi hendaklah berpandukan peruntukan dasar dan dengan kelulusan tertentu. Pelaksanaan akses kawalan adalah berbeza bergantung kepada sistem ICT tetapi pada amnya melibatkan kebenaran membaca, menulis dan memadam.

**(a) Pencaman Pengguna (User-Id)**

Semua pengguna sistem komputer akan disediakan dengan kod pencaman bagi membolehkannya membuat capaian.

(i) Setiap pengguna akan diberikan kod pencaman pengguna yang tidak boleh dikongsi; dan

(ii) Pengguna mestilah menyediakan pengesahan (authentication) (i.e kata laluan) yang hanya diketahui oleh pengguna berkenaan.

**(b) Kawalan Kata Laluan (Password)**

Kata laluan perlu dikawal untuk mengelakkan daripada diketahui oleh orang yang tidak diberi kuasa menggunakannya:

(i) Kata laluan tidak boleh dicatat di atas kertas;

(ii) Kata laluan mestilah mempunyai kombinasi sekurang-kurangnya enam aksara;

(iii) Kata laluan perlu ditukar sekurang-kurangnya setiap enam bulan;

(iv) Kata laluan yang disimpan dalam komputer akan dikod (encrypted);

(v) Kata laluan dimasukkan pada medan tanpa boleh lihat; dan

(vi) Had percubaan dari segi masa atau bilangan percubaan akan ditetapkan untuk memasukkan kata laluan dan pencaman pengguna. Sekiranya kemasukan tidak berjaya dalam had tersebut, percubaan seterusnya tidak akan dibenarkan.

**(c) Kawalan perisian**

Keselamatan perisian boleh dipertingkatkan dengan cara-cara berikut:

(i) Membuat beberapa salinan bagi setiap perisian dan salinan ini kemudiannya disimpan di bangunan lain yang lebih selamat;
(ii) Melindungi perisian sistem daripada pindaan yang tidak dibenarkan;
(iii) Mengawal capaian kepada sistem komputer melalui pengunaan kata laluan (password) dan pencaman pengguna (user-ID); dan
(iv) Melindungi perisian sistem daripada virus, "trojan horses" dan bom jangka.

**PERLINDUNGAN VIRUS DAN PENCEGAHAN**

13. Untuk memastikan perkhidmatan komputer dan rangkaian yang disediakan tidak terganggu, semua sistem dilengkapkan dengan perisian "virus-screening". Perisian ini hendaklah digunakan untuk mengimbas semua perisian pihak ketiga atau dari lain-lain agensi atau sumber; pengimbasan hendaklah dilakukan sebelum perisian dilaksanakan. **Sila rujuk lampiran A - Prosedur Mengelak Jangkitan Virus.**

**KOMPUTER MIKRO / KOMPUTER PERIBADI**

14. Pemprosesan, penyimpanan dan penggunaan data pada komputer mikro hendaklah dilindungi. Perlindungan sumber yang berasaskan komputer mikro hendaklah berasaskan tahap sensitiviti dan nilai kepada organisasi. **Rujuk Lampiran B - Panduan Penggunaan Komputer Mikro.**

**SALINAN PERISIAN DAN HAKCIPTA**

15. Pengguna tidak dibenarkan sama sekali menyalinkan perisian daripada sistem sama ada untuk kegunaan rasmi atau persendirian kerana ia menyalahi **Akta Hakcipta (Pindaan 1990).**

**KAWALAN FIZIKAL DAN AKSES**

16. Kawalan Fizikal meliputi perkara-perkara seperti bilik server, instalasi komputer dan bekalan elektrik. Pemilihan tapak komputer yang selamat adalah penting bagi mengurangkan kesan bencana seperti banjir, kebakaran, gempabumi dan capaian yang tidak dibenarkan.

**(a) Perlindungan Daripada Kebakaran**

Kawalan bagi mengurangkan risiko kebakaran peralatan ICT dan mengurangkan kerosakan jika berlaku kebakaran:

(i) Merokok adalah dilarang di dalam bilik server dan di kawasan yang menyimpan bahan mudah terbakar;
(ii) Bilik Server hendaklah dilengkapkan dengan alat pemadam api;
(iii) Bahan mudah bakar seperti kertas tidak boleh disimpan di bilik server;
(iv) Bekas sampah hendaklah diletakkan diluar bilik server; dan
(v) Suis kepada semua alat-alat komputer perlu ditutup apabila tidak digunakan.

**(b) Perlindungan Daripada Air**

Kawalan mesti diadakan bagi mengurangkan risiko kerosakan disebabkan air dalam bilik server:

(i) Kakitangan di bilik server hendaklah memastikan tidak berlaku limpahan air dari alat hawa dingin.

**(d) Kawalan Persekitaran**

Kawalan mestilah diambil untuk melindungi peralatan komputer daripada bahaya persekitaran:

(i) Sistem elektrik hendaklah dilindungi daripada masalah yang boleh mengakibatkan kerosakan kepada peralatan;
(ii) Suhu dan kelembapan dibilik Server hendaklah diawasi dan dikawal; dan
(iii) Kakitangan di bilik server hendaklah dilatih untuk mengawasi kawalan persekitaran peralatan, bagaimana untuk bertindak sekiranya berlaku kecemasan.

**(d) Kawalan Akses**

Untuk memasuki kawasan bilik server hendaklah terlebih dahulu mendapat kebenaran daripada Pengarah BTM:

(i) Pintu masuk hendaklah sentiasa dikunci dan diawasi;
(ii) Pelawat-pelawat di kawasan ini hendaklah diiring sepanjang masa; dan
(iii) Memasuki ke bilik server dihadkan kepada kakitangan yang bertanggungjawab sahaja.

**PENUTUP**

17. Tanggungjawab keseluruhan dan kawalan semua sumber ICT diletakkan dibawah Bahagian Teknologi Maklumat. Ini amat perlu disebabkan sifat sistem yang saling bergantung dan berhubung antara satu sama lain. Dibawah hirarki keseluruhan tanggungjawab dan kewajipan ICT, cawangan-cawangan di peringkat negeri juga mempunyai tanggungjawab tambahan disamping tanggungjawab setempat. Keselamatan ICT bergantung penuh kepada pengurusan ICT yang mana pengawalannya hendaklah dilakukan secara pusat manakala pelaksanaannya diagih-agihkan.

**Lampiran A**

## PROSEDUR MENGELAK JANGKITAN VIRUS

### A.1 Jangkitan virus boleh berlaku sekiranya

a) Menggunakan komputer yang telah dijangkiti virus;
b) Menggunakan disket yang telah dijangkiti virus; dan
c) Menyalin kandungan disket yang telah dijangkiti virus.

### A.2 Pencegahan jangkitan virus

Beberapa langkah pencegahan dan pengawalan mungkin dapat mengawal perkembangan virus daripada merebak. Antara langkah-langkah untuk mengawal ialah:

a) *"Write protect"* pada disket yang digunakan supaya penyalinan tidak dapat digunakan;
b) Jangan menyalin sebarang perisian;
c) Sentiasa gunakan *"Scan"* untuk mengesan kehadiran virus;
d) Sentiasa *"boot system"* dari cakera padat;
e) Asingkan fail program dari fail data dalam disket berlainan;
f) Pengasingan penggunaan komputer.

### A.3 Jika jangkitan telah dikesan

a) *"Back-up"*kan kesemua data;
b) *"Off"*kan sistem;
c) *"Boot"*kan semula dengan menggunakan disket DOS di *"write-protected"* yang bersih dari sebarang virus;

d) Gunakan program anti virus (dari disket) untuk membuang virus pada cakera padat atau disket yang dijangkiti tadi; dan

e) *"Boot"*kan semula jika menggunakan cakera padat.

## A.4 Tanda-tanda disket telah diserang virus

a) Penggunaan storan bertambah dengan cepat;

b) Program tidak dapat digunakan/dijalankan;

c) Berlaku *"disc error";*

d) Kegagalan *"boot"* sistem;

e) Pengurangan keupayaan sistem.

## A.5 Di mana virus menyerang

a) Ke dalam fail
*.EXE
*.COM
*.SYS
*.OVR;

b) Ke dalam *"Memory";*

*c)* Ke ruang *"File Allocation Table (FAT)";*

d) Ke dalam fail data
*.DBF
*.WK?.
*.DOC

## A.6 Cara mengesan virus

Gunakan "*VIRUS SCAN*".

## A.7 Jenis-jenis virus, kesan serangan dan kaedah menghapuskannya

Semua maklumat ini boleh di dapati di fail *"readme"* dan fail *"doc"* yang disertakan bersama program anti virus.

## PANDUAN PENGGUNAAN KOMPUTER MIKRO

### B.1 Am

a) Pengguna komputer mikro adalah bertanggungjawab terhadap penjagaan dan keselamatan peralatan yang disediakan;
b) Peralatan yang dipasang tidak boleh diubahalih daripada tempat asal tanpa kebenaran;
c) Pastikan suis punca elektrik dihidupkan terlebih dahulu sebelum menggunakan komputer mikro dan pencetak;
d) Suis komputer mikro dan punca elektrik hendaklah ditutup sekiranya tidak digunakan;
e) Kawasan persekitaran yang menempatkan peralatan hendaklah sentiasa dalam keadaan bersih;
f) Makanan dan minuman tidak dibenarkan dibawa masuk ke bilik berkenaan;
g) Pengguna adalah dilarang merokok semasa menggunakan peralatan;
h) Pengguna hendaklah menggunakan peralatan untuk tujuan rasmi sahaja; dan
i) Sebarang kerosakan peralatan dan masalah perisian hendaklah dilaporkan kepada BTM.

### B.2 PENGGUNAAN

a) Pengguna hendaklah menggunakan komputer mikro dengan cara yang betul;
b) Pengguna dinasihatkan supaya sentiasa *"scan"* disket yang digunakan;
c) Pengguna tidak dibenarkan memformat cakera padat;

d) Pengguna tidak boleh memasukkan sebarang perisian ke dalam cakera padat;

e) Pengguna tidak dibenarkan menyimpan fail/data ke dalam cakera padat melainkan dengan kebenaran;

f) Pengguna dikehendaki menggunakan disket untuk menyimpan fail masing-masing;

g) Disket-disket yang digunakan hendaklah dilebelkan mengikut peringkat keselamatan dan menjadi tanggungjawab mereka untuk menjaganya;

h) Disket-disket yang mengandungi maklumat/data penting hendaklah dibuat salinan dan disimpan di tempat berasingan;

i) Pengguna boleh membuat rujukan mengenai perisian/peralatan melalui manual-manual yang disediakan; dan

j) Apabila mencetak, gunakan kertas pencetak tanpa pembaziran.