BUKU PANDUAN PENGURUSAN KESELAMATAN ICT

Bahagian Teknologi Pendidikan
Kementerian Pelajaran Malaysia

BTP

ISBN : 978-983-3244-77-5

EDISI PERTAMA: Julai 2007

MENDIDIK JIWA DAN MINDA

SEKOLAH BESTARI MALAYSIA

Diterbitkan oleh
Sektor Perkhidmatan ICT
Bahagian Teknologi Pendidikan
Kementerian Pelajaran Malaysia
Pesiaran Bukit Kiara
50604 Kuala Lumpur
Tel : 603-2098 7788
Faks : 603-2092 3763

KANDUNGAN

LATAR BELAKANG

Buku Panduan Pengurusan Keselamatan ICT ialah buku panduan baru, yang dikemaskini dan diadaptasi daripada Dokumen Dasar dan Prosedur Pengurusan Keselamatan Sekolah Bestari Versi 1.0 yang diterbitkan di bawah Projek Rintis Sekolah Bestari pada tahun 2000. Dokumen asal buat pertama kali disemak semula pada tahun 2001.

Pengguna edisi pertama dan edisi kedua buku panduan ini akan mendapati bahawa teks telah disemak semula sepenuhnya; sebahagian besar semakan merupakan pengasingan kandungan kepada dua dokumen baru, satu untuk Penyelaras ICT Sekolah dan satu lagi untuk pengguna lain.

Buku Panduan Pengurusan Keselamatan ICT ini berasaskan maklumat pengurusan keselamatan ICT yang terkandung dalam Buku Panduan Pengurusan Keselamatan Teknologi Maklumat & Komunikasi Sektor Awam Malaysia yang diterbitkan oleh MAMPU.

KETUA PENGARAH PELAJARAN MALAYSIA
KEMENTERIAN PELAJARAN MALAYSIA

Pendahuluan

Saya ingin mengucapkan tahniah kepada Jawatankuasa Buku Panduan, yang diselaraskan oleh Bahagian Teknologi Pendidikan, atas usaha dan dedikasi dalam menyiapkan buku panduan ini. Komitmen jawatankuasa ini dalam menyediakan buku panduan ini amat disanjungi.

Buku panduan ini bertujuan memberi garis panduan yang lengkap dan ringkas lagi padat tentang Pengurusan Keselamatan ICT. Saya berharap agar garis panduan dan prosedur yang disenarai memberi manfaat kepada pengguna.

Seterusnya saya ingin merakamkan penghargaan kepada semua guru yang memberi sumbangan yang tidak ternilai dalam menjayakan penerbitan buku panduan ini, yang merupakan sumbangan yang sangat penting kepada persekitaran ICT sekolah.

(DATO' DR. HJ. AHAMAD BIN SIPON)
Ketua Pengarah Pelajaran
Kementerian Pelajaran Malaysia

BAHAGIAN TEKNOLOGI PENDIDIKAN
KEMENTERIAN PELAJARAN MALAYSIA

Prakata

Buku panduan ini memberikan gambaran ringkas tentang Pengurusan Keselamatan ICT untuk semua sekolah di Malaysia.

Buku panduan ini boleh diguna sebagai sumber rujukan oleh semua sekolah dalam melaksanakan pengurusan keselamatan ICT yang berkesan. Walaupun tidak ada jaminan bahawa keselamatan mutlak dapat dicapai dalam persekitaran kerja elektronik peringkat global, namun penggunaan buku panduan ini seharusnya dapat mengurangkan risiko yang dihadapi oleh sistem berasaskan ICT.

Saya ingin mengucapkan tahniah kepada ahli jawatankuasa dan semua pihak yang terlibat dalam menghasilkan buku panduan ini.

(DATO' HJ. YUSOFF BIN HARUN)
Pengarah
Bahagian Teknologi Pendidikan
Kementerian Pelajaran Malaysia

PENGENALAN

Buku panduan ini diadaptasi daripada Buku Panduan Pengurusan Maklumat & Keselamatan Teknologi Komunikasi Sektor Awam Malaysia yang diterbitkan oleh MAMPU, serta Dokumen Dasar dan Prosedur Pengurusan Keselamatan Sekolah Bestari Versi 1.0 yang diterbitkan oleh Pasukan Projek Rintis Sekolah Bestari Kementerian Pelajaran Malaysia.

Buku panduan ini disusun mengikut topik untuk membantu pengguna mengamalkan pengurusan keselamatan secara sistematik dan berkesan. Kandungan dalam setiap topik disusun mengikut urutan agar langkah yang disenaraikan mudah diikuti dan memberi panduan yang menyeluruh kepada pengurusan keselamatan ICT.

Setiap tajuk bermula dengan pengenalan dan tujuan, diikuti dengan garis panduan yang memberi gambaran keseluruhan pengurusan keselamatan ICT. Pengguna seharusnya dapat mempraktikkan amalan keselamatan ICT dengan berkesan apabila menggunakan garis panduan yang terdapat dalam buku ini.

Buku Panduan Pengurusan Keselamatan ICT diharap dapat membantu meningkatkan pengetahuan pembaca dan seterusnya mewujudkan kesedaran tentang pengurusan keselamatan ICT.

Glosari disertakan agar kandungan buku ini dapat difahami dengan lebih baik.

1 Penggunaan Internet dan E-Mel

1.1 Pengenalan

Kemajuan dalam bidang teknologi maklumat dan komunikasi (ICT) membolehkan maklumat dihantar dan diterima dengan cepat. Kemudahan ini menyebabkan penggunaan internet dan e-mel semakin meningkat. Komunikasi elektronik kini digunakan secara meluas sebagai media alternatif untuk berkongsi maklumat. Walau bagaimanapun penggunaan perkhidmatan internet dan e-mel yang tidak terkawal mungkin mendedahkan kita kepada pelbagai ancaman keselamatan. Oleh itu, perlindungan keselamatan mestilah diwujudkan untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat.

1.2 Tujuan

Topik ini bertujuan menggariskan penggunaan perkhidmatan internet dan e-mel yang berkesan di sekolah. Semua peraturan ini hendaklah diwujudkan untuk melindungi warga sekolah. Penyalahgunaan e-mel dan internet mungkin mendedahkan sekolah kepada risiko keselamatan, seperti serangan virus, perubahan dalam sistem dan perkhidmatan rangkaian serta isu-isu perundangan.

1.3 Tanggungjawab

Warga sekolah yang boleh mengakses sistem ICT sekolah dikehendaki mematuhi peraturan dan garis panduan yang terdapat dalam topik ini.

1.4 Penggunaan Internet

1) Sistem komunikasi elektronik atau kemudahan ICT sekolah pada amnya digunakan untuk memudah dan menambah baik pentadbiran dan operasi sekolah. Pengguna seharusnya menyedari bahawa data dan sistem yang digunakan oleh mereka merupakan hak Kerajaan Malaysia.

2) Aktiviti melayari laman web hendaklah dihadkan kepada perkara yang berkaitan dengan urusan kerja atau tujuan lain yang dibenarkan oleh Pengetua/Guru Besar sekolah.

3) Pengguna perlu mengesahkan integriti dan ketepatan bahan yang dimuat turun. Semua bahan ini mestilah diimbas agar bebas daripada *malicious code*.

4) Bahan yang dimuat turun daripada internet (contohnya perisian) hendaklah dikenal pasti sumbernya untuk mengelakkan pelanggaran hak cipta. Pengguna hendaklah menyatakan sumber bagi semua bahan internet yang digunakan.

5) Maklumat yang hendak dimuat naik ke internet hendaklah dipantau oleh Penyelaras ICT sekolah dan dibenarkan oleh Pengetua/ Guru Besar sekolah.

6) Hanya pengguna yang mendapat kebenaran sahaja boleh melibatkan diri dan menggunakan kemudahan perbincangan awam dalam

talian seperti *newsgroups* dan *bulletin board*. Pengguna yang terlibat mestilah mendapat kebenaran Pengetua/Guru Besar tertakluk kepada dasar dan tatacara yang telah ditetapkan. Setiap pengguna yang menyertai forum seperti ini mestilah bertindak dengan bijaksana, jelas dan berupaya mengekalkan konsistensi dan keutuhan maklumat berkenaan kerana setiap maklumat yang dikongsi melambangkan imej sekolah, Kementerian Pelajaran Malaysia dan Kerajaan Malaysia.

7) Pengguna adalah **dilarang** daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan Internet seperti:

a) Melanggar hak mana-mana individu atau syarikat yang dilindungi oleh hak cipta, rahsia perniagaan, paten atau harta intelek, atau peraturan bagi undang-undang yang berkaitan, termasuk, tetapi tidak terhad kepada, pemasangan atau pengedaran perisian cetak rompak untuk kegunaan sekolah.

b) Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen.

c) Memuat naik, memuat turun, menghantar dan menyimpan kad elektronik *(e-card)*, video, lagu dan kepilan fail melebihi saiz dua (2) megabait yang boleh mengakibatkan kelembapan perkhidmatan dan operasi sistem rangkaian komputer.

d) Menyedia, memuat naik, memuat turun dan menyimpan ucapan, imej atau bahan lain yang boleh:

   i) dianggap sebagai gangguan seks, etnik dan perkauman;

   ii) menimbulkan keadaan huru-hara seperti menyebarkan khabar angin, memfitnah atau menghasut; dan

   iii) mencemar reputasi sekolah, Kementerian Pelajaran Malaysia atau Kerajaan Malaysia.

e) Menyertai aktiviti yang tidak berkaitan dengan kerja (komersial, politik atau yang lain) yang boleh menjejaskan produktiviti staf dan menyalahgunakan sumber maklumat seperti:

   i) menggunakan kemudahan *chatting* melalui internet; dan

   ii) memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan dalam talian seperti permainan elektronik, video dan lagu.

f) Melakukan kegiatan jenayah seperti menyebarkan bahan yang membabitkan perjudian, senjata dan kegiatan pengganas.

g) Menyalahgunakan kemudahan perbincangan awam dalam talian seperti *newsgroups* dan *bulletin board*.

8) Pengguna tidak dibenarkan menyertai aktiviti dalam talian seperti *hacking, sniffing,* mencuri maklumat atau memberikan maklumat palsu.

1.5 E-Mel

1) E-mel membolehkan pengguna berkomunikasi antara satu sama lain dalam bentuk mesej elektronik. Penggunaan e-mel kini semakin meluas untuk membolehkan komunikasi dua hala yang lebih berkesan.

2) Semua warga sekolah perlu diberi akaun e-mel untuk kegunaan rasmi. Sebagai contoh alamat e-mel ialah nama@moe.edu.my.

3) Penggunaan perkhidmatan e-mel tertakluk kepada peraturan yang ditetapkan dan Penyelaras ICT Sekolah mempunyai hak untuk membatalkan penggunaan tersebut jika pengguna tidak mematuhi peraturan.

4) E-mel ialah salah satu daripada saluran komunikasi rasmi di sekolah. Oleh itu, e-mel harus dikarang dengan berhati-hati. Sebagai contoh, penggunaan huruf besar untuk kandungan e-mel tidak digalakkan dan dianggap tidak beretika. Pengguna dinasihati menulis e-mel dengan menggunakan bahasa yang betul, ringkas dan sopan. Pengguna juga

perlu memastikan bahawa subjek dan kandungan e-mel adalah berkaitan.

5) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul. Penghantar boleh menggunakan kemudahan 'salinan kepada' *(cc)* sekiranya e-mel tersebut perlu dimaklumkan kepada penerima yang lain. Bagaimanapun, penggunaan '*blind cc' (bcc)* u□dak digalakkan.

6) Pengguna tidak dibenarkan menghantar fail kepilan menggunakan e-mel yang melebihi dua (2) megabait. Perisian pemampatan yang sesuai seperti *WinZip* hendaklah digunakan untuk mengurangkan saiz fail kepilan.

7) Pengguna sepatutnya mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui.

8) Pengguna sepatutnya mengimbas semua fail kepilan sebelum membukanya.

9) E-mel pada lazimnya tidak melalui proses penyulitan *(encryption)*. Pengguna dilarang menghantar maklumat terperingkat *(classified information)* melainkan maklumat itu telah melalui proses penyulitan *(encryption)*. Rujuk **Bab 5 - Pengklafikasian dan Pengendalian Maklumat** untuk mendapatkan maklumat terperinci.

10) Setiap pengguna perlu mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan komunikasi dan transaksi maklumat melalui e-mel. Hal ini bertujuan melindungi maklumat Kerajaan daripada sebarang bentuk penyalahgunaan.

11) Setiap e-mel rasmi yang dihantar atau diterima hendaklah diarkib mengikut tatacara pengurusan sistem fail elektronik. Pengguna adalah digalakkan mengarkibkan e-mel pada sumber storan kedua seperti disket bagi tujuan keselamatan.

12) E-mel yang tidak penting atau tidak mempunyai nilai arkib serta tidak diperlukan lagi bolehlah dihapuskan.

13) Pengguna dilarang daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan e-mel rasmi Kerajaan seperti:

    a) menggunakan akaun milik orang lain, berkongsi akaun atau memberi akaun kepada orang lain;

    b) menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah;

    c) menggunakan e-mel untuk tujuan komersial atau politik;

d) menghantar dan memiliki bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian dan jenayah;

e) menghantar dan melibatkan diri dalam e-mel yang berunsur hasutan, e-mel 'sampah', e-mel 'bom', e-mel *spam*, fitnah, ciplak atau aktiviti-aktiviti lain yang ditegah oleh undang-undang Kerajaan Malaysia; dan

f) menyebarkan *malicious code* seperti virus, *worm*, *trojan horse* dan *trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain.

2 Pemilihan Kata Laluan

2.1 Pengenalan

Kata laluan ialah salah satu cara mengesahkan hak pengguna untuk mengakses sistem komputer. Oleh yang demikian, pengguna hendaklah tahu akan tanggungjawab mereka dalam mengekalkan kawalan capaian yang berkesan khususnya berkaitan dengan penggunaan kata laluan. Memandangkan seseorang pengguna itu perlu mengingat beberapa kata laluan, maka kata laluan yang dipilih itu mestilah mudah diingat dan menepati amalan baik keselamatan kata laluan. Topik ini menggariskan beberapa amalan baik keselamatan kata laluan yang seharusnya dipatuhi oleh semua pengguna di sekolah.

2.2 Tujuan

Topik ini bertujuan memastikan pengguna berdaftar di sekolah mematuhi amalan terbaik dalam mengguna dan memilih kata laluan bagi semua sistem aplikasi dan sistem rangkaian yang diakses oleh mereka.

2.3 Tanggungjawab

Warga sekolah yang dibenarkan mengakses sistem ICT sekolah hendaklah mematuhi garis panduan yang ditetapkan dalam topik ini.

2.4 Kompromi Kata Laluan

Kata laluan boleh dikompromi oleh pihak-pihak lain melalui pelbagai cara. Antaranya termasuklah:

1) Kata laluan yang dikongsi dengan kawan atau rakan sekerja.

2) Kata laluan yang ditulis terdedah kepada orang lain.

3) Kata laluan boleh diteka, sama ada oleh pengguna lain atau perisian diagnosis keselamatan.

4) Server yang menyimpan kata laluan boleh dicerobohi dan kata laluan berkenaan boleh diakses oleh penceroboh.

5) Kata laluan yang dihantar boleh dicerobohi dan dirakam oleh penceroboh.

6) Pengguna diperdaya untuk memberikan kata laluan mereka kepada penceroboh.

2.5 Peraturan Am Kata Laluan

1) Kata laluan hendaklah dirahsiakan dan tidak boleh dikongsi dengan orang lain. Jangan dedahkan kata laluan anda kepada orang lain.

2) Kata laluan hendaklah dihafal dan jangan sekali-kali disalin di mana-mana media.

3) Jangan tinggalkan komputer yang sedang digunakan tanpa pengawasan melainkan komputer tersebut dilindungi dengan kata laluan. Jangan tinggalkan komputer dalam keadaan melahu *(idle)* untuk tempoh masa yang panjang – tutup dan but semula apabila diperlukan.

4) Hubungi Penyelaras ICT Sekolah dengan serta merta untuk menukar kata laluan sekiranya anda mengesyaki seseorang telah berjaya menceroboh kata laluan anda.

5) Pengguna tidak boleh mengakses sistem komputer untuk tempoh masa tertentu selepas gagal memasukkan kata laluan yang betul sebanyak tiga (3) kali berturut-turut. Penyelaras ICT Sekolah perlu set semula kata laluan tersebut.

2.6 Garis Panduan Pembentukan Kata Laluan

Kelemahan utama kata laluan ialah kata laluan boleh diteka. Walaupun pengguna lain mungkin berputus asa selepas meneka berkali-kali, namun terdapat perisian yang dapat meneka dengan mudah berjuta-juta gabungan kata laluan dan memecahkan kata laluan. Berikut adalah garis panduan untuk membentuk kata laluan:

1) Pengguna dinasihati memilih kata laluan yang sukar diteka untuk mengekang serangan tekaan kata laluan.

2) Pengguna dikehendaki memilih kata laluan yang terdiri daripada pelbagai set aksara, tertakluk kepada polisi sistem.

3) Kata laluan hendaklah mempunyai saiz sekurang-kurangnya lapan (8) aksara dengan gabungan alphanumerik dan simbol. Contoh kata laluan yang baik adalah p@S5w07D.

2.7 Penukaran dan Penggunaan Semula Kata Laluan

1) Semua kata laluan lalai *(default)* hendaklah ditukar semasa log masuk kali pertama.

2) Amalan yang praktikal untuk mengehadkan kemungkinan kata laluan dicerobohi ialah mengubahnya dari semasa ke semasa, sekurang-kurangnya setiap 180 hari atau lebih kerap.

3) Pengguna tidak sepatutnya meneruskan penggunaan kata laluan yang telah dikompromi atau disyaki telah dikompromi.

4) Elakkan daripada menggunakan semula empat (4) kata laluan yang terakhir.

3 Keselamatan Fizikal Infrastruktur ICT

3.1 Pengenalan

Keselamatan fizikal ialah lapisan pertahanan utama dalam mana-mana seni bina keselamatan ICT. Keperluan untuk melindungi aset secara fizikal daripada ancaman nyata atau yang mungkin berlaku tidak boleh dipandang ringan. Kawalan keselamatan fizikal merupakan kaedah kawalan yang terbaik.

3.2 Tujuan

Garis panduan ini bertujuan menghalang akses tanpa kebenaran, kerosakan dan gangguan kepada infrastruktur ICT yang mungkin menyebabkan kerosakan kepada aset maklumat sekolah.

3.3 Tanggungjawab

Warga sekolah yang dibenarkan mengakses infrastruktur ICT dikehendaki mematuhi semua garis panduan yang telah ditetapkan.

3.4 Persekitaran Infrastruktur ICT

1) Semua kemudahan pengkomputeran yang terdapat di sekolah diguna untuk memudahkan operasi harian dan aktiviti pembelajaran warga sekolah. Oleh yang demikian, hanya pengguna yang sah seperti guru, murid dan kakitangan sekolah dibenar menggunakan kemudahan ini. Pihak ketiga (bukan warga

sekolah) yang ingin menggunakan kemudahan tersebut hendaklah mendapat kebenaran Pengetua/Guru Besar sekolah terlebih dahulu.

2) Pengguna atau pelawat yang menggunakan kemudahan di makmal komputer, pusat media dan pusat akses hendaklah mencatat nama, tarikh, masa dan tempoh akses dalam buku log.

3) Guru hendaklah memantau murid yang menggunakan makmal komputer. Murid yang hendak menggunakan komputer tanpa pemantauan guru hendaklah mendapat kebenaran terlebih dahulu daripada pihak yang berkenaan.

4) Akses ke makmal komputer selepas waktu persekolahan mestilah dikawal dan dipantau.

5) Pihak ketiga seperti vendor yang membekalkan perkhidmatan penyelenggaraan perkakasan ICT hendaklah sentiasa diselia dan dipantau ketika mereka berada di persekitaran infrastruktur ICT.

6) Pintu dan tingkap makmal komputer hendaklah dikunci apabila tidak digunakan.

7) Tidak dibenarkan sama sekali makan dan minum di persekitaran infrastruktur ICT.

8) Pengguna atau pelawat makmal komputer hendaklah menanggalkan kasut (jika perlu) untuk memastikan kebersihan makmal.

9) Pengguna hendaklah memastikan komputer ditutup dengan sempurna untuk mengelakkan kerosakan.

10) Pengguna hendaklah log keluar sistem bagi mengelakkan pengguna lain daripada mengakses sistem tersebut.

11) Pengguna hendaklah menjaga kebersihan dan kekemasan infrastruktur ICT sepanjang masa.

12) Pengguna tidak dibenarkan membawa keluar apa-apa kelengkapan atau peranti hak milik sekolah. Individu yang didapati mencuri atau cuba mencuri boleh dikenakan tindakan disiplin.

13) Pengguna tidak dibenarkan mengalih kedudukan peralatan (contohnya mengalih kedudukan monitor), membaiki peralatan yang rosak atau mengubah konfigurasi sistem tanpa kebenaran Penyelaras ICT Sekolah atau kakitangan yang bertanggungjawab.

14) Pengguna hendaklah melaporkan sebarang insiden atau ancaman keselamatan berpotensi kepada Penyelaras ICT Sekolah atau kepada kakitangan yang bertanggungjawab. Antaranya termasuklah kejadian seperti pecah masuk, kecurian, serta kegagalan fungsi perkakasan dan perisian.

15) Pengguna hendaklah mengelak daripada menutup ruang pengudaraan monitor komputer agar komputer tidak menjadi terlampau panas.

16) Semua kemudahan seperti pendingin hawa dan lampu hendaklah digunakan dengan betul. Pengguna dikehendaki menghidupkan suis kemudahan ini apabila menggunakan makmal komputer. Semua suis mestilah dimatikan selepas penggunaan.

4 Pengkomputeran Mudah Alih *(Mobile Computing)*

4.1 Pengenalan

Kemajuan teknologi telah memungkinkan peranti pengkomputeran mudah alih *(mobile computing devices)* digunakan oleh semua orang. Penggunaan meluas peranti pengkomputeran mudah alih ini telah menimbulkan pelbagai risiko keselamatan yang boleh menjejaskan kerahsiaan, integriti dan kebolehsediaan maklumat. Ciri peranti pengkomputeran mudah alih itu sendiri meningkatkan risiko kecurian berbanding peranti tetap. Peranti tetap biasanya ditempatkan di premis yang selamat dengan kawalan keselamatan fizikal yang baik, manakala peranti pengkomputeran mudah alih pula biasanya berada di luar kawalan keselamatan fizikal organisasi. Topik ini bertujuan mewujudkan garis panduan prosedur yang perlu dipatuhi oleh pengguna peranti pengkomputeran mudah alih.

4.2 Tujuan

Topik ini bertujuan memberi panduan keselamatan maklumat dan keselamatan fizikal untuk menggunakan peranti pengkomputeran mudah alih.

4.3 Tanggungjawab

Warga sekolah yang menggunakan peranti pengkomputeran mudah alih untuk memproses maklumat dikehendaki mematuhi garis panduan yang terdapat dalam topik ini.

4.4 Kegunaan Peranti Pengkomputeran Mudah Alih

1) Penggunaan peranti pengkomputeran mudah alih peribadi seperti komputer buku *(notebook),* komputer tablet *(tablet PCs),* komputer tatang (*palmtop*) dan telefon pintar *(smart phones)* untuk memproses maklumat adalah dilarang kecuali dengan izin pentadbir sekolah dan telah dikonfigurasi dengan kawalan keselamatan yang perlu seperti perisian *anti-malicious* atau *firewall* peribadi dengan bimbingan Penyelaras ICT Sekolah.

2) Peranti pengkomputeran mudah alih pihak ketiga (kepunyaan kontraktor atau vendor) hanya boleh disambungkan kepada rangkaian sekolah setelah mendapat kebenaran terlebih dahulu daripada pentadbir sekolah dan telah dikonfigurasi dengan kawalan keselamatan yang bersesuaian dengan penyeliaan Penyelaras ICT Sekolah untuk mengelakkan rangkaian sekolah daripada dijangkiti virus.

3) Semua peranti pengkomputeran mudah alih yang dimiliki oleh Kementerian Pelajaran Malaysia hendaklah dipasang dengan kawalan keselamatan bersesuaian seperti perisian anti virus sebelum diserahkan kepada pengguna. Peranti seperti ini hendaklah dikonfigurasi bagi menerima pengemaskinian keselamatan *(security updates)* secara automatik daripada server.

4) Penggunaan peranti pengkomputeran mudah alih tertakluk kepada tatacara Penggunaan Internet dan E-mel.

4.5 Keselamatan Fizikal

1) Peranti pengkomputeran mudah alih hendaklah dilindungi secara fizikal daripada kecurian khususnya apabila ditinggalkan di dalam kereta atau lain-lain jenis pengangkutan, bilik hotel, pusat persidangan dan tempat mesyuarat.

2) Peranti pengkomputeran mudah alih yang mengandungi maklumat penting, sensitif atau sulit tidak boleh ditinggalkan tanpa pengawasan dan jika boleh, hendaklah dikunci.

3) Peranti pengkomputeran mudah alih yang digunakan di tempat awam mestilah dijaga untuk mengelakkan risiko terjadinya pendedahan maklumat secara tidak sengaja kepada orang yang tidak berkenaan.

4) Pengguna peranti pengkomputeran mudah alih hendaklah melaporkan dengan segera sebarang kerosakan atau kehilangan aset Kementerian Pelajaran Malaysia kepada Penyelaras ICT Sekolah dan pentadbir sekolah.

5) Pergerakan peranti pengkomputeran mudah alih yang dimiliki oleh Kementerian Pelajaran Malaysia hendaklah direkodkan.

4.6 Penukaran Konfigurasi

1) Pengguna tidak dibenarkan menukar konfigurasi sistem peranti pengkomputeran mudah alih yang dibekalkan oleh Kementerian Pelajaran Malaysia kecuali bagi tujuan rasmi atau tujuan lain yang dibenarkan, seperti menukar konfigurasi rangkaian (contohnya alamat IP, alamat DNS dan sebagainya) berasaskan persekitaran rangkaian yang sedia ada.

2) Peranti pengkomputeran mudah alih yang dibekalkan oleh Kementerian Pelajaran Malaysia tidak boleh dipinda dengan apa-apa cara (contohnya meningkatkan keupayaan pemproses, menambah ingatan atau menukar papan litar). Pengguna hendaklah mendapatkan kebenaran daripada Penyelaras ICT Sekolah sekiranya ingin melakukan perubahan kepada perisian atau perkakasan. Hanya Penyelaras ICT Sekolah dibenarkan melaksanakan perubahan tersebut.

4.7 Penyambungan ke Rangkaian Tidak Dilindungi

1) Peranti pengkomputeran mudah alih dalam persekitaran rangkaian sekolah yang selamat dilindungi daripada serangan *malicious software* melalui pengemaskinian keselamatan *(security updates)* secara konsisten. Rangkaian di luar sekolah, sama ada rangkaian kawasan setempat tanpa wayar di lapangan terbang atau sambungan internet jalur lebar di rumah,

dianggap sebagai rangkaian tidak dilindungi. Dalam persekitaran seperti ini, peranti disambungkan terus ke internet tanpa apa-apa perlindungan seperti *firewall*. Keadaan ini menyebabkan peranti terdedah kepada pelbagai ancaman, termasuklah serangan langsung daripada entiti dalam internet, sama ada daripada pengguna atau *malicious code*.

2) Pengguna tidak dibenarkan membuat sambungan kepada rangkaian yang tidak dilindungi kerana ini memungkinkan pendedahan maklumat terperingkat kepada pihak yang tidak berkenaan.

3) Jika sambungan tersebut sememangnya diperlukan, maka pengguna perlu melakukan penyulitan (*encryption*) untuk maklumat terperingkat bagi mengelakkan pendedahan tanpa kebenaran. Penyulitan data *(Data encryption)* merupakan perlindungan terbaik untuk menghalang penyebaran maklumat terperingkat sekiranya peranti hilang atau dicuri. Maklumat yang dilindungi dengan teknik penyulitan yang mantap dan dilaksanakan dengan baik tidak lagi mempunyai apa-apa nilai.

5 Pengklasifikasian dan Pengendalian Maklumat

5.1 Pengenalan

Maklumat mestilah dikendalikan dengan sewajarnya bagi memastikan kerahsiaan, integriti dan kebolehsediaan maklumat tidak terjejas. Klasifikasi dan pengendalian maklumat dilaksanakan untuk melindungi rahsia negara. Maklumat sulit selalunya disimpan (atau sepatutnya disimpan) berasingan daripada maklumat biasa. Kesan pendedahan dan pindaan maklumat yang mungkin berlaku di sekolah dan Kementerian Pelajaran Malaysia berbeza-beza mengikut jenis maklumat. Justeru, usaha dan kos yang diperlukan untuk melindungi maklumat daripada risiko-risiko ini juga berbeza bergantung kepada jenis maklumat. Oleh yang demikian, asas-asas tertentu diperlukan untuk menentukan langkah-langkah keselamatan yang boleh digunakan untuk maklumat-maklumat yang berbeza.

5.2 Tujuan

Topik ini bertujuan memberi garis panduan bagi pengklasifikasian maklumat dan prosedur pengendalian maklumat yang sesuai dalam mengendalikan maklumat berdasarkan skema klasifikasi yang ditentukan.

5.3 Tanggungjawab

Warga sekolah yang dibenarkan mengakses maklumat sulit dikehendaki mematuhi panduan dalam topik ini.

5.4 Skop Perlindungan Maklumat

Semua maklumat sekolah tertakluk kepada panduan berikut tanpa mengambil kira:

1) cara maklumat dikemukakan (bentuk bertulis, pertuturan, elektronik atau bentuk lain);

2) teknologi yang digunakan untuk mengendali maklumat (contohnya kabinet fail, mesin faks, komputer dan rangkaian kawasan setempat);

3) lokasi maklumat (contohnya pejabat, makmal komputer atau bilik server); dan

4) kitar hayat maklumat (contohnya asal usul, kemasukan data ke dalam sistem, pemprosesan, penyebaran, penyimpanan dan pelupusan).

5.5 Klasifikasi Maklumat

Menurut Arahan Keselamatan kerajaan, maklumat diklasifikasikan kepada lima (5) tahap:

1) **Awam**: Dokumen/maklumat rasmi yang disediakan untuk pengetahuan, tontonan atau kegunaan awam.

2) **Terhad**: Maklumat/dokumen rasmi, tidak termasuk yang diklasifikasikan sebagai Rahsia Besar, Rahsia atau Sulit tetapi perlu dikelaskan mengikut tahap langkah keselamatan. Rujuk Jadual 1: Pengendalian Maklumat.

3) **Sulit**: Maklumat/dokumen rasmi, yang sekiranya didedahkan tanpa kebenaran, walaupun tidak membahayakan keselamatan negara – mungkin memberikan kesan kepada kepentingan atau maruah negara, aktiviti kerajaan atau individu; akan menyebabkan rasa malu atau kesukaran kepada pentadbiran negara; dan akan memberikan manfaat kepada pihak asing.

4) **Rahsia**: Dokumen/maklumat rasmi yang sekiranya didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kehilangan/kerosakan kepada kepentingan atau maruah negara; dan akan memberikan manfaat yang lebih banyak kepada pihak asing.

5) **Rahsia Besar**: Dokumen/maklumat rasmi yang sekiranya didedahkan tanpa kebenaran akan menyebabkan kehilangan/kerosakan yang besar kepada negara.

5.6 Pengendalian Maklumat

1) Pemilik aset hendaklah menentukan klasifikasi maklumat.

2) Pengendalian maklumat dalam apa-apa bentuk bergantung pada klasifikasi maklumat yang ditetapkan oleh pemilik aset.

3) Maklumat sulit memerlukan langkah keselamatan yang sewajarnya untuk melindungi kerahsiaan, integriti dan kebolehsediaan maklumat.

4) Prosedur operasi sedia ada atau yang terancang hendaklah mengambil kira semua pengguna yang dibenarkan melihat maklumat sulit berkenaan.

5) Pengguna perlu mengenal pasti pihak yang boleh membahayakan keselamatan maklumat sulit. Pengguna juga mestilah berpegang kepada garis panduan atau prosedur bagi mengelak pihak lain daripada melihat maklumat berkenaan.

6) Kawalan akses dan pengesahan yang sewajarnya perlu diimplementasi:

   a) untuk mengelakkan orang yang tidak berkenaan melihat maklumat sulit;

   b) kerana maklumat sulit bergantung pada tahap pengklasifikasian; dan

   c) supaya Penyelaras ICT Sekolah dan pemilik aset dapat menentukan tahap akses pengguna yang dibenarkan mengakses maklumat sulit.

7) Jadual berikut merupakan panduan pengendalian maklumat untuk setiap kitar hayat maklumat, bermula dengan proses mewujudkan maklumat sehingga memusnahkan maklumat.

Jadual 1: Pengendalian Maklumat

	Rahsia Besar	Rahsia	Sulit	Terhad	Awam
Pelabelan					
Pelabelan Media Elektronik	1) Dilabelkan sebagai 'Rahsia Besar' atau 'Rahsia' atau 'Sulit' atau 'Terhad'.				Tidak diperlukan
Pelabelan salinan keras *(hard copy)*	1) Dilabelkan sebagai 'Rahsia Besar' atau 'Rahsia' atau 'Sulit' atau 'Terhad' pada kulit depan dan kulit belakang, dan setiap halaman dokumen. Lihat Arahan Keselamatan – Fasal 48-52. 2) Dilabelkan dengan peringatan. Lihat Arahan Keselamatan – Fasal 53.				Tidak diperlukan
Rujukan	Pemilik maklumat berkenaan hendaklah bekerjasama dengan kakitangan pentadbiran sekolah untuk menentukan nombor rujukan bagi setiap dokumen yang dihasilkan.				Tidak diperlukan

	Rahsia Besar	Rahsia	Sulit	Terhad	Awam
Penyimpanan					
Penyimpanan dalam Media Tetap	Penyulitan maklumat dilakukan jika diperlukan atau menggunakan kawalan lain seperti kawalan akses, pengurusan kata laluan dan bentuk-bentuk kawalan rangkaian lain.				Tidak diperlukan
Penyimpanan dalam Media Boleh Tukar	Penyulitan maklumat dilakukan jika diperlukan atau menggunakan kawalan lain seperti kawalan akses, pengurusan kata laluan dan bentuk-bentuk kawalan rangkaian lain.				Tidak diperlukan
Penyimpanan Fizikal	1) Bilik kebal atau peti besi berkunci. 2) Kerja yang sedang dijalankan boleh disimpan dalam kabinet (besi) yang berkunci. 3) Lihat Arahan Keselamatan – Fasal 58 – 60.		1) Kabinet (besi). 2) Lihat Arahan Keselamatan – Fasal 58 – 60.		Tiada storan khas diperlukan

	Rahsia Besar	Rahsia	Sulit	Terhad	Awam
Menghantar / Memindahkan / Memproses					
Menghantar dokumen	1) Akuan penerimaan setelah menerima dokumen (2 salinan) perlu disediakan. 2) Pembungkusan mel untuk dokumen dibawa dengan selamat: a) Hanya satu (1) sampul yang mempunyai tanda, nombor rujukan, nama dan alamat diperlukan. b) Sampul mestilah dimeterai. 3) Pembungkusan mel untuk dokumen dibawa secara tidak selamat: a) Dua (2) sampul diperlukan. b) Sampul dalam mempunyai tanda, nombor rujukan, nama dan alamat; c) Sampul luar mempunyai nama dan alamat dan mestilah dimeterai.				Tidak diperlukan

	Rahsia Besar	Rahsia	Sulit	Terhad	Awam
	4) Lihat Arahan Keselamatan – Fasal 61 – 65.				
Faks/Telefon/ Telegraf	1) Tidak dibenarkan. 2) Lihat Arahan Keselamatan – Fasal 66.				Tiada sekatan
Membawa Dokumen Keluar dari Pejabat	1) Kelulusan bertulis daripada Ketua Setiausaha Kementerian Pelajaran Malaysia 2) Lihat Arahan Keselamatan – Fasal 67.		1) Kelulusan bertulis daripada Ketua Jabatan diperlukan. 2) Lihat Arahan Keselamatan – Fasal 67.		Tiada sekatan
Menghantar melalui Rangkaian Awam	1) Penyulitan jika perlu.				Tidak diperlukan

	Rahsia Besar	Rahsia	Sulit	Terhad	Awam
Menyalin	1) Kebenaran daripada pemilik maklumat diperlukan. 2) Bilangan salinan yang dikeluarkan perlu dipantau. 3) Lihat Arahan Keselamatan – Fasal 55-57.				Tiada sekatan
Siaran kepada Pihak Ketiga					
Siaran kepda pihak ketiga	1) Tidak boleh disiarkan kepada negara lain tanpa kelulusan Kerajaan Malaysia. 2) Siaran kepada pihak ketiga adalah terhad berdasarkan keperluan tertentu dengan kebenaran pemilik maklumat. 3) Siaran kepada akhbar tidak dibenarkan tanpa kelulusan pemilik maklumat. 4) Lihat Arahan Keselamatan – Fasal 68 – 70.				Sampah

	Rahsia Besar	Rahsia	Sulit	Terhad	Awam
Pemberian Hak Akses					
Pemberian Hak Akses	1) Hak akses diberikan oleh pemilik maklumat. Kawalan akses dilaksanakan oleh Penyelaras ICT Sekolah.				Tidak diperlukan
Pelupusan					
Pelupusan Fizikal	1) Tidak dibenarkan melainkan dengan jelasnya diarahkan oleh pemilik maklumat. Pemusnahan menyeluruh mestilah dilaksanakan. 2) Pelupusan mestilah direkodkan. 3) Dokumen mestilah dimusnahkan dengan menggunakan pencarik kertas. 4) Lihat Arahan Keselamatan – Fasal 71 – 74.				Sampah
Pelupusan Elektronik	Pelupusan kekal				Pelupusan biasa

	Rahsia Besar	Rahsia	Sulit	Terhad	Awam
Kehilangan Dokumen/Maklumat					
Melaporkan kehilangan	1) Kehilangan dokumen/maklumat hendaklah dilaporkan dengan segera kepada pentadbir sekolah dalam masa 24 jam. 2) Siasatan perlu dijalankan untuk menganggarkan kesan kehilangan tersebut. Laporan kepada pihak berkuasa seperti polis dibuat jika perlu. 3) Lihat Arahan Keselamatan – Fasal 75 – 76.				Tidak diperlukan

GLOSARI

Aksara alphanumerik *(Alphanumeric characters)*	Terdiri daripada gabungan set aksara abjad dan aksara angka.
Kebolehsediaan *(Availability)*	Kadar atau peratusan jumlah masa sesuatu maklumat/peralatan boleh digunakan atau boleh dikendalikan tanpa ralat dalam tempoh tertentu.
Jalur lebar *(Broadband)*	Jalur frekuensi saluran penghantaran yang mempunyai lebar jalur yang melebihi frekuensi bunyi 3000 hertz.
Kerahsiaan *(Confidentiality)*	Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran.
E-mel *(E-Mail)*	Surat, pesanan, atau mesej dalam bentuk fail komputer yang dikirim dan diterima melalui sistem rangkaian komputer. Singkatan e-mel. Sinonim surat elektronik, mel komputer.
Penyulitan *(Encryption)*	Penukaran data kepada bentuk kod sulit untuk membolehkan data dikirim dengan selamat tanpa difahami oleh pihak lain.
Media boleh tukar *(Exchangeable Media)*	Media yang digunakan untuk menyimpan data yang boleh dikeluarkan dari mesin. Contohnya cakera liut, pita magnet dan cakera padat.
Firewall	Sistem yang direka bentuk untuk mengelakkan akses tanpa kebenaran kepada/daripada rangkaian persendirian.

Media tetap *(Fixed media)*	Media yang boleh menyimpan data dalam kapasiti yang besar dan merupakan bahagian tetap peranti. Contohnya pemacu keras.
Pemilik maklumat *(Information Owner)*	Individu/Bahagian/Jabatan/Unit yang dirujuk sebagai tuan punya aset.
Integriti *(Integrity)*	Tahap kesahihan, ketepatan, keselanjaran dan kesempurnaan data/maklumat yang disimpan, dihantar, atau diproses oleh sistem.
Internet *(Internet)*	Sistem perangkaian antarabangsa yang membolehkan pengguna mencapai maklumat pangkalan data dari seluruh dunia.
Rangkaian Kawasan Setempat *(Local Area Network)*	Rangkaian komputer yang dihadkan untuk menyambungkan komputer dan peranti perisian yang berada dalam suatu kawasan kecil yang sama, seperti bilik, tapak, atau bangunan kecil. Singkatan LAN.
Malicious Code	Kod yang dimuatkan ke dalam komputer tanpa pengetahuan dan kebenaran pemilik komputer khusus untuk merosakkan atau melumpuhkan sistem. Contoh termasuklah virus, *worm* dan *Trojan horse*.
Perisian *Malicious (Malicious software)*	Program yang dimuatkan ke dalam komputer tanpa pengetahuan dan kebenaran pemilik komputer khusus untuk merosakkan atau melumpuhkan sistem. Contoh termasuklah virus, *worm* dan *Trojan horse*.

Peranti pengkomputeran mudah alih *(Mobile Computing devices)*	Peranti yang mudah dialihkan dan boleh disambung kepada sistem infrastruktur rangkaian dan/atau sistem data untuk penghantaran data dengan menggunakan wayar (kabel/ dawai telefon) atau penghantaran data tanpa wayar (gelombang radio/ inframerah). Contohnya komputer riba, dan telefon pintar.
Kata laluan *(Password)*	Kata yang terdiri daripada gabungan huruf dan/atau nombor yang membentuk kod unik. Kata ini perlu dimaklumkan kepada sistem sebelum pengguna dibolehkan menggunakan sumber sistem. Kaedah ini melindungi sistem daripada digunakan oleh orang yang tidak mempunyai kebenaran penggunaan.
Penyelaras ICT Sekolah *(ICT Coordinator)*	Individu yang dilantik oleh pihak sekolah untuk bertanggungjawab mengurus dan menyelaras infrastruktur ICT sekolah.
Hapus Kekal *(Secure delete)*	Menghapuskan sesuatu fail/data elektronik secara kekal.
Spam	Mel elektronik yang tidak diminta oleh penerima tetapi dihantar berulang kali dalam kuantiti yang banyak.
Trojan horse	Atur cara yang dianggap berfaedah tetapi sebenarnya mengandungi arahan untuk menceroboh dan merosakkan keselamatan sistem komputer apabila atur cara dilaksanakan.
Pengguna *(Users)*	Warga sekolah yang menggunakan kemudahan ICT yang disediakan. Sebagai contoh guru, murid, kerani, pentadbir dan yang lain.

Virus *(Virus)*	Atur cara komputer yang disorok di dalam atur cara lain dan dapat menyalin dirinya sendiri ke dalam perisian lain apabila atur cara itu digunakan.
Tanpa wayar *(Wireless)*	Kaedah komunikasi yang menggunakan gelombang untuk menghantar data ke beberapa peranti.
Worm	Atur cara yang memadamkan data daripada ingatan komputer secara perlahan-lahan.

Rujukan

1) *Malaysian Public Sector Management of Information & Communications Technology Security Handbook* (MyMIS), 2002.

2) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet Dan Mel Elektronik Di Agensi-agensi Kerajaan.

3) Arahan Keselamatan Pengguna Kata Laluan (AK 0002).

4) Prosedur dan Dasar Pengurusan Keselamatan Sekolah Bestari Versi 2.0.

5) Kamus Komputer, Dewan Bahasa dan Pustaka Kuala Lumpur, 2002.

Pertanyaan

Sebarang pertanyaan tentang buku ini hendaklah dialamatkan kepada:

Pengarah
Bahagian Teknologi Pendidikan
Kementerian Pelajaran Malaysia
Pesiaran Bukit Kiara
50604 Kuala Lumpur
(u.p: Sektor Perkhidmatan ICT)

Tel.: 03-2098 7788
Faks: 03-2098 6242
E-mel: pict@moe.edu.my

PENYUMBANG

PENASIHAT

Dato' Haji Yusoff bin Harun	Pengarah Bahagian Teknologi Pendidikan

PANEL PENGARANG

Khalidah binti Othman	Bahagian Teknologi Pendidikan
Chan Foong Mae	Bahagian Teknologi Pendidikan
Anthony Gerard Foley	Bahagian Teknologi Pendidikan
Haji Mohd Azman bin Ismail	Bahagian Teknologi Pendidikan
Mohd Arifen bin Naim	Bahagian Teknologi Pendidikan
Yap Ley Har	Bahagian Teknologi Pendidikan
Junainiwati binti Mohd Deris	Bahagian Teknologi Pendidikan
Roimah binti Dollah	Bahagian Teknologi Pendidikan
Nik Fajariah binti Nik Mustaffa	Bahagian Teknologi Pendidikan
Rozina binti Ramli	SMK Aminuddin Baki,Kuala Lumpur
Nirmal Kaur	SMK Victoria, Kuala Lumpur
Mohd Hisham bin Abdul Wahab	SMK(L) Methodist, Kuala Lumpur
Ab. Aziz bin Mamat	Sekolah Seri Puteri, Cyberjaya, Selangor
Abd Aziz bin Mohd Hassan	SMK USJ 8, Selangor
Widiana binti Ahmad Fazil	SMK Pandan Jaya, Selangor
Rogayah binti Harun	Kolej Tunku Kurshiah,Negeri Sembilan
Mohd Zali bin Zakri	SM Sains Tuanku Jaafar, Negeri Sembilan
Jaya Lakshmi a/p Mutusamy	SMK(A) Persekutuan Labu, Negeri Sembilan
Azmi bin Abdul Latif	SMK(A) Persekutuan Labu, Negeri Sembilan
Haji Zulkiflee bin A. Rahman	SM Teknik Muar, Johor
Daud bin Yusof	SMK Buluh Kasap, Johor

PANEL PENTERJEMAH

Fazlina binti Hashim	Bahagian Teknologi Pendidikan
Yap Ley Har	Bahagian Teknologi Pendidikan
Mak Sheau Yun	Bahagian Teknologi Pendidikan
Norhazira binti Md. Haza	Bahagian Teknologi Pendidikan
Ahmad bin Haji Taba	Bahagian Teknologi Pendidikan
Junainiwati binti Mohd. Deris	Bahagian Teknologi Pendidikan
Shazril Helmi bin Samsudin	Bahagian Teknologi Pendidikan
Rasyidi bin Johan	Universiti Pendidikan Sultan Idris
Salman Firdaus bin Sidek	Universiti Pendidikan Sultan Idris
Wee Siu Hiang	SMK Victoria, Kuala Lumpur
Ab. Aziz bin Mamat	Sekolah Seri Puteri, Selangor
Marzila binti Mohamed	SMK(P) Sri Aman, Selangor
Mohd Naser bin Ishak	SMK Victoria, Kuala Lumpur
Mohamad Nasir bin Abd. Aziz	Sekolah Seri Puteri, Selangor
Rahim bin Omar	SK Seri Bintang Utara, Kuala Lumpur
Norra binti Zakaria	SMK St. John, Kuala Lumpur