



KERAJAAN MALAYSIA

**PEKELILING KEMAJUAN PENTADBIRAN AWAM
BILANGAN 1 TAHUN 2003**

**GARIS PANDUAN MENGENAI
TATACARA PENGGUNAAN INTERNET
DAN MEL ELEKTRONIK
DI AGENSI-AGENCI KERAJAAN**

**JABATAN PERDANA MENTERI
MALAYSIA
28 November 2003**

Dikelilingkan kepada:

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Ketua Pengurusan Badan Berkanun Persekutuan
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Ketua Pengurusan Pihak Berkuasa Tempatan



JABATAN PERDANA MENTERI MALAYSIA
KOMPLEKS JABATAN PERDANA MENTERI
PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN
62502 PUTRAJAYA

Telefon : 603-88881199
Faks : 603-88883721

Rujukan kami : UPTM 159/526/9 Jld.3(9)

Tarikh : 28 November 2003

Semua Ketua Setiausaha Kementerian
Semua Ketua Jabatan Persekutuan
Semua Ketua Pengurusan Badan Berkanun Persekutuan
Semua Y.B. Setiausaha Kerajaan Negeri
Semua Ketua Pengurusan Pihak Berkuasa Tempatan

**PEKELILING KEMAJUAN PENTADBIRAN AWAM
BILANGAN 1 TAHUN 2003**

**GARIS PANDUAN MENGENAI
TATACARA PENGGUNAAN INTERNET DAN MEL ELEKTRONIK
DI AGENSI-AGENSI KERAJAAN**

TUJUAN

Pekeliling ini bertujuan untuk menyediakan garis panduan mengenai tatacara penggunaan Internet dan mel elektronik di agensi-agensi Kerajaan serta perkara-perkara berkaitan yang perlu diberi perhatian dan diambil tindakan oleh agensi-agensi Kerajaan.

LATAR BELAKANG

2. Kerajaan sentiasa berusaha meningkatkan kecekapan dalam proses komunikasi di kalangan anggota-anggotanya dan juga di antara agensi Kerajaan dengan swasta dan orang ramai. Penggunaan teknologi maklumat dan komunikasi (ICT) telah membuka peluang kepada komunikasi yang lebih cepat dan mudah. Salah satu kaedah komunikasi yang semakin luas penggunaannya dalam sektor awam ialah Internet dan mel elektronik (e-mel). Selain daripada memudah dan mempercepatkan komunikasi, kaedah ini dapat mengurangkan penggunaan kertas dan akhirnya menyumbang kepada peningkatan produktiviti dan kualiti perkhidmatan.

3. Namun begitu, penggunaan Internet dan e-mel yang sistematik, cekap dan pantas ini jika tidak diuruskan dengan baik boleh menjejaskan keselamatan terhadap data, dokumen atau sebarang maklumat melalui penghantaran media elektronik. Dengan itu, kawalan yang teratur dan perlindungan keselamatan ICT yang bersesuaian perlu diwujudkan supaya penggunaan

Internet dan e-mel bukan sahaja dapat meningkatkan kecekapan berkomunikasi, tetapi juga dapat menjamin keselamatan maklumat yang dihantar dan diterima.

TATACARA PENGGUNAAN

4. Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan ini dirumus bagi memenuhi keperluan penggunaan, langkah-langkah perlindungan dan penguatkuasaan, agar penggunaan Internet dan e-mel yang terkawal dan perlindungan keselamatan yang lebih mantap dapat diwujudkan. Langkah ini akan dapat mengurangkan kesan negatif ke atas maklumat seperti pencerobohan, kecurian dan pengubahsuaian data.

TANGGUNGJAWAB AGENSI

5. Semua agensi Kerajaan adalah dikehendaki untuk mengambil perhatian kepada Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan seperti yang dilampirkan kepada Pekeliling ini. Bagi maksud ini, semua Ketua Jabatan adalah diminta melaksanakan tanggungjawab yang ditetapkan dan mengambil tindakan-tindakan berikut:

- (a) memastikan seorang pentadbir sistem ICT dilantik dan bertanggungjawab dalam melaksanakan tindakan-tindakan sebagaimana yang ditetapkan di dalam tatacara ini;
- (b) mengenal pasti pengurusan dan kawalan keselamatan ICT yang perlu diberi perhatian semasa penggunaan Internet dan e-mel, bergantung kepada tahap sensitiviti maklumat; dan
- (c) memastikan program-program kesedaran keselamatan ICT diberikan kepada semua pengguna agar penggunaan Internet dan e-mel dapat dilaksanakan dengan cara yang betul dan selamat.

PEMAKAIAN

6. Tertakluk kepada penerimaannya oleh pihak berkuasa masing-masing, peruntukan Pekeliling ini dipanjangkan kepada semua Perkhidmatan Awam Negeri, Pihak Berkuasa Berkanun Negeri dan Pihak Berkuasa Tempatan.

TARIKH KUAT KUASA

7. Pekeliling ini berkuat kuasa mulai tarikh ia dikeluarkan.



TAN SRI SAMSUDIN BIN OSMAN
Ketua Setiausaha Negara

(Lampiran kepada
Pekeliling Kemajuan
Pentadbiran Awam
Bilangan 1 Tahun 2003)

**GARIS PANDUAN MENGENAI
TATACARA PENGGUNAAN INTERNET DAN
MEL ELEKTRONIK
DI AGENSI-AGENCI KERAJAAN**

Unit Pemodenan Tadbiran dan
Perancangan Pengurusan Malaysia
(MAMPU)
Jabatan Perdana Menteri

KANDUNGAN

Perkara	Muka Surat
PENGENALAN	5
TATACARA PENGGUNAAN INTERNET	5
TATACARA PENGGUNAAN E-MEL	7
PENGARKIBAN	9
KAWALAN KESELAMATAN INTERNET DAN E-MEL	10
TANGGUNGJAWAB PENTADBIR SISTEM ICT	11
TANGGUNGJAWAB PENGGUNA	12
KHIDMAT NASIHAT	13
PENUTUP	13

SENARAI LAMPIRAN

- LAMPIRAN A – Contoh Format E-mel Bukan Rahsia Rasmi
- LAMPIRAN B – Contoh Format E-mel Rahsia Rasmi
- LAMPIRAN C – Amalan Baik Keselamatan Kata Laluan

GARIS PANDUAN MENGENAI TATACARA PENGGUNAAN INTERNET DAN MEL ELEKTRONIK DI AGENSI-AGENSİ KERAJAAN

PENGENALAN

Perkembangan teknologi maklumat dan komunikasi (ICT) telah membolehkan maklumat dihantar dan diterima dengan pantas. Kemudahan ini telah membawa kepada peningkatan penggunaan Internet dan mel elektronik atau e-mel dalam sektor awam. Hakikat ini turut dipengaruhi oleh bilangan pengguna dan kepentingan maklumat yang kian meningkat dari semasa ke semasa. Komunikasi secara elektronik juga dilihat sebagai salah satu saluran penting dalam membantu mewujudkan perkongsian maklumat. Tambahan pula, kaedah ini membolehkan proses penghantaran dan penerimaan sesuatu maklumat dilaksanakan dengan lebih cepat dan mudah. Bagaimanapun, pengurusan Internet dan e-mel yang tidak terkawal boleh menjejaskan keselamatan maklumat. Justeru, perlindungan keselamatan yang bijaksana perlu diwujudkan dan disesuaikan bagi menjamin kesahihan, keutuhan dan kebolehsediaan maklumat yang berterusan.

2. Tujuan utama garis panduan ini ialah untuk menerangkan tatacara penggunaan Internet dan e-mel, meningkatkan tahap keselamatan sistem komunikasi dokumen rasmi Kerajaan dan mengurangkan risiko gangguan operasi Internet dan e-mel.

TATACARA PENGGUNAAN INTERNET

3. Teknologi Internet telah memudahkan perhubungan antara pengguna dan menyediakan akses kepada banyak maklumat dalam pelbagai bentuk format dengan menyediakan sumber pembelajaran, rekreasi, penyelidikan, analisis, rujukan dan bahan-bahan lain yang berfaedah. Perkhidmatan Awam dalam usahanya menuju ke arah pemodenan tadbiran telah melihat Internet sebagai satu *platform* untuk penambahbaikan perkhidmatan yang disediakan. Dalam konteks ini, penjawat awam perlu menggunakan kemudahan Internet dengan cara yang bertanggungjawab dan konsisten.

4. Internet adalah infrastruktur saluran global dan merupakan punca maklumat yang tidak terkawal. Dengan sebab itu, ketepatan maklumat Internet tidak boleh ditentukan. Justeru, penjawat awam perlu memainkan peranan dan bertindak secara bijak menilai kesahihan, ketepatan dan kesesuaian sesuatu maklumat yang diperolehi agar kerja yang dilaksanakan tidak menyimpang dari tujuan sebenar jabatan.

5. Penggunaan Internet dengan cara yang tidak bertanggungjawab adalah dianggap sebagai pelanggaran tatacara yang boleh mengancam keselamatan, keutuhan dan kerahsiaan maklumat, melemahkan sistem ICT dan pengurusan rekod elektronik, mengganggu sistem rangkaian ICT dan merosakkan imej Perkhidmatan Awam. Oleh yang demikian, bagi menjamin kemudahan Internet digunakan dengan selamat, adalah wajar setiap agensi menentukan latihan yang bersesuaian, penggunaan teknologi yang kukuh dan dasar yang menyeluruh agar pelanggaran seumpamanya tidak berlaku.

6. Berikut adalah tatacara yang mesti diikuti dalam menggunakan Internet.

(a) Hak Akses Pengguna

Hak akses hendaklah dilihat sebagai satu kemudahan yang disediakan oleh agensi untuk membantu melicinkan pentadbiran atau memperbaiki perkhidmatan yang

7

disediakan. Pengguna harus mengambil maklum bahawa semua aset ICT di bawah kawalannya (termasuk maklumat) adalah hak milik Kerajaan.

- (b) **Memilih Laman**
Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan.
- (c) **Pengesahan Maklumat**
Bahan yang diperolehi dari Internet perlulah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah juga dinyatakan.
- (d) **Muat Naik Bahan**
Bahan rasmi yang hendak dimuat naik ke Internet hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik.
- (e) **Muat Turun Bahan**
Tindakan memuat turun hanya dibenarkan ke atas bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh jabatan sahaja.
- (f) **Perbincangan Awam**
Hanya pegawai yang mendapat kebenaran sahaja boleh melibatkan diri dan menggunakan kemudahan ini. Kandungan perbincangan awam seperti *newsgroup* dan *bulletin board* mestilah mendapat pengesahan daripada Ketua Jabatan tertakluk kepada dasar dan tatacara yang telah ditetapkan. Perlu diingat bahawa setiap maklumat yang dikongsi melambangkan imej Kerajaan. Dengan sebab itu, setiap pengguna mestilah bertindak dengan bijaksana, jelas dan berupaya mengekalkan konsistensi dan keutuhan maklumat berkenaan.

7. Penjawat awam adalah **dilarang** daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan Internet seperti:

- (a) memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen;
- (b) menyedia dan menghantar maklumat berulang-ulang berupa gangguan;
- (c) menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan, imej atau bahan-bahan yang mengandungi unsur-unsur lucah;
- (d) menyedia, memuat naik, memuat turun dan menyimpan maklumat Internet yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej Kerajaan;
- (e) menyalahgunakan kemudahan perbincangan awam atas talian seperti *newsgroup* dan *bulletin board*;
- (f) memuat naik, memuat turun dan menyimpan gambar atau teks yang bercorak penentangan yang boleh membawa keadaan huru-hara dan menakutkan pengguna Internet yang lain;
- (g) memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti permainan elektronik, video dan lagu;
- (h) menggunakan kemudahan *chatting* melalui Internet;

- (i) menggunakan kemudahan Internet untuk tujuan peribadi;
- (j) menjalankan aktiviti-aktiviti komersial dan politik;
- (k) melakukan aktiviti jenayah seperti menyebarkan bahan yang membabitkan perjudian, senjata dan aktiviti penganas;
- (l) memuat naik, memuat turun, menghantar dan menyimpan kad elektronik, video, lagu dan kepilang fail melebihi saiz 2 megabait yang boleh mengakibatkan kelembapan perkhidmatan dan operasi sistem rangkaian komputer; dan
- (m) menggunakan kemudahan modem peribadi untuk membuat capaian terus ke Internet.

TATACARA PENGGUNAAN MEL ELEKTRONIK

8. Mel elektronik atau e-mel adalah merupakan aplikasi yang membolehkan pengguna berkomunikasi antara satu dengan lain dalam bentuk mesej elektronik. Aplikasi e-mel ini digunakan secara meluas dan membenarkan komunikasi lebih daripada dua hala dengan cara yang pantas dan lebih sesuai untuk penulisan yang ringkas.

9. Setiap penjawat awam mempunyai e-mel rasmi yang digunakan untuk tujuan rasmi dan didaftarkan di bawah agensi Kerajaan. Salah satu contoh alamat e-mel rasmi ialah ahmad@jpm.gov.my. E-mel rasmi boleh dibahagikan kepada dua kategori iaitu e-mel rahsia rasmi dan e-mel bukan rahsia rasmi.

(a) E-mel Rahsia Rasmi

E-mel yang mengandungi maklumat atau perkara rahsia rasmi yang mesti diberi perlindungan untuk kepentingan keselamatan yang dikelaskan mengikut pengelasanannya sama ada *Terhad, Sulit, Rahsia* atau *Rahsia Besar*.

(b) E-mel Bukan Rahsia Rasmi

E-mel yang tidak mengandungi maklumat atau perkara rahsia rasmi.

10. Semua agensi digalakkan untuk mewujudkan satu alamat e-mel khusus bagi memudahkan orang ramai berhubung dengan agensi berkenaan sekiranya memerlukan penjelasan lanjut, membuat aduan atau mengemukakan pandangan. Contoh alamat e-mel khusus agensi ialah gcert@mampu.gov.my.

11. Berikut adalah kaedah penggunaan e-mel yang betul dan disesuaikan pemakaiannya di setiap agensi Kerajaan.

(a) Pemilikan Akaun E-mel

Pemilikan akaun e-mel bukanlah hak mutlak seseorang. Ia adalah kemudahan yang tertakluk kepada peraturan jabatan dan boleh ditarik balik jika penggunaannya melanggar peraturan. Akaun atau alamat e-mel yang diperuntukkan oleh jabatan sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang.

(b) **Format**

E-mel adalah salah satu saluran komunikasi rasmi Kerajaan. Ini bermakna, setiap e-mel mestilah mengandungi rujukan fail, tarikh dan logo rasmi. Contoh format e-mel bukan rahsia rasmi adalah seperti di **Lampiran A** dan format bagi e-mel rahsia rasmi adalah seperti di **Lampiran B**.

Penggunaan huruf besar kandungan e-mel adalah tidak digalakkan dan dianggap tidak beretika. Sebaik-baiknya, gabungan huruf besar dan huruf kecil digunakan dan dipraktikkan di tempat-tempat yang bersesuaian di samping mengamalkan penggunaan bahasa yang betul, ringkas dan sopan.

Pengguna juga perlu memastikan bahawa subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan.

(c) **Penghantaran**

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 lain. Bagaimanapun, penggunaan 'blind cc' (bcc) tidak digalakkan.

Kemudahan 'reply' digunakan untuk menjawab e-mel kepada penghantar asal dan 'forward' untuk memanjangkan e-mel atau dimajukan kepada penerima lain. Sebagai amalan baik, e-mel penghantar hendaklah dijawab **selewat-lewatnya 4 hari** dari tarikh e-mel berkenaan diterima. Kemudahan penghantaran e-mel jawab automatik semasa berada di luar pejabat bagi tempoh waktu yang panjang, boleh dipertimbangkan penggunaannya oleh Jabatan.

(d) **Penghantaran Bersama Fail Kepilan**

Penghantar hendaklah mengamalkan penggunaan fail kepilan, misalnya mengepilkan fail minit mesyuarat dan elakkan dari menghantar dan menerima fail e-mel yang bersaiz melebihi 2 megabait. Sekiranya perlu, kaedah pemampatan untuk mengurangkan saiz fail adalah disarankan.

(e) **Penerimaan**

Pengguna seharusnya mengelakkan dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui.

(f) **Mengenal Pasti Identiti Pengguna**

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

(g) **Penyimpanan**

Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik agensi masing-masing.

Pengguna hendaklah memastikan jumlah e-mel yang disimpan di dalam kotak masuk e-mel adalah tidak melebihi ruang storan yang telah diperuntukkan dan mengutamakan penyimpanan e-mel yang perlu sahaja. Penyimpanan salinan e-mel pada sumber storan kedua seperti disket adalah digalakkan bagi tujuan keselamatan.

(h) **Pemusnahan dan Penghapusan**

E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan. (Contoh: draf kertas kerja, draf minit, kertas makluman dan brosur).

(i) **Tarikh dan Masa Sistem Komputer**

Sebelum sesuatu mesej dihantar, perlu ditentukan tarikh dan masa sistem komputer adalah tepat.

12. Pengguna adalah **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 ditekah oleh undang-undang Kerajaan Malaysia;
- (f) menyebarkan kod perosak seperti virus, *worm*, *trojan horse* dan *trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;
- (g) menghantar semula e-mel yang gagal sampai ke destinasi sebelum menyiasat punca kejadian; dan
- (h) membenarkan pihak ketiga untuk menjawab e-mel kepada penghantar asal bagi pihaknya.

PENGARKIBAN

13. Rekod elektronik rasmi adalah merupakan rekod awam mengikut tafsiran Akta Arkib Negara Malaysia No. 44/1966. Ia merangkumi sebarang mesej atau rekod komputer (termasuk

fail kepilang) yang diwujudkan, dihantar, diserahkan, dijawab, diedar, disimpan, disalin, dipapar, dibaca atau dicetak oleh sistem atau perkhidmatan rekod elektronik sesebuah agensi Kerajaan.

- (a) **Rekod Elektronik yang Penting**
Rekod elektronik rasmi yang penting perlu disimpan di dalam sistem komputer jabatan sehingga tindakan ke atasnya selesai. Jabatan mestilah menghantar rekod elektronik yang penting dan mempunyai nilai arkib ke Arkib Negara untuk simpanan kekal.
- (b) **Rekod Elektronik yang Tidak Penting**
Rekod elektronik rasmi yang tidak penting tetapi tindakan perlu diambil ke atasnya, tidak perlu dihantar ke Arkib Negara. Contohnya, makluman dan draf.
- (c) **Pemindahan Rekod Elektronik ke Arkib Negara**
Bagi rekod-rekod elektronik yang penting dan mempunyai nilai arkib yang hendak dipindahkan ke Arkib Negara Malaysia mestilah di dalam format dan tatacara yang ditentukan oleh Arkib Negara.
- (d) **Penghapusan dan Pelupusan Rekod Elektronik**
Sebarang cadangan penghapusan atau pelupusan rekod-rekod elektronik yang mempunyai nilai arkib perlulah dirujuk dan mendapat kelulusan daripada Arkib Negara Malaysia.

KAWALAN KESELAMATAN INTERNET DAN E-MEL

14. Internet dan e-mel adalah terdedah kepada ancaman seperti pencerobohan, penyelewengan, pemalsuan, pemintasan dan pembocoran rahsia. Dengan itu, keselamatan Internet dan e-mel perlu untuk melindungi maklumat rahsia rasmi dan maklumat bukan rahsia rasmi Kerajaan dari capaian tanpa kuasa yang sah. Keselamatan Internet dan e-mel bergantung kepada faktor-faktor sokongan berikut.

- (a) **Keselamatan Fizikal**
Komputer hendaklah diletakkan di tempat yang mempunyai kawalan fizikal yang selamat daripada penceroboh atau sebarang bentuk capaian tidak sah.
- (b) **Keselamatan Dokumen Elektronik**
Bagi memastikan semua fail yang dihantar dan diterima bebas daripada sebarang bentuk ancaman keselamatan, perisian anti-virus dan penapis *malicious codes* perlulah dikemas kini dari semasa ke semasa.

Semua maklumat rahsia rasmi atas talian perlu berada dalam bentuk teks sifer sepanjang masa, manakala maklumat rahsia rasmi yang tidak diperlukan atas talian mesti dipindahkan segera ke media storan elektronik sekunder dalam bentuk teks sifer dan hendaklah dikelaskan. Peraturan mengelaskan maklumat digital telah digariskan dalam dokumen *Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS)*, Buku Arahan Keselamatan dan Surat Pekeliling Am Bil. 2 Tahun 1987 "Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986".

Sekiranya penyelenggaraan komputer hendak dilaksanakan, agensi perlu memastikan semua maklumat bukan rahsia rasmi atau rahsia rasmi di dalam komputer berkenaan telah dikeluarkan dan selamat sebelum menghantar komputer untuk penyelenggaraan.

(c) **Tandatangan Digital**

Agensi Kerajaan yang mengendalikan maklumat rahsia rasmi mesti menggunakan tandatangan digital yang dikeluarkan oleh pihak berkuasa perakuan tempatan yang ditauliahkan oleh Kerajaan Malaysia iaitu Pihak Berkuasa Persijilan (Certification Authority).

(d) **Keselamatan Pengendalian E-mel Rahsia Rasmi**

Perkara-perkara berikut perlu dilaksanakan bagi menentukan keselamatan dan kesahihan e-mel rahsia rasmi iaitu:

- (i) penyulitan mesti dilakukan ke atas semua e-mel rahsia rasmi yang dihantar, diterima dan disimpan;
- (ii) penerima e-mel rahsia rasmi mesti mengesahkan kesahihan dokumen apabila ditandatangani secara digital oleh pengirim;
- (iii) penerima mesti membuat akuan penerimaan e-mel rahsia rasmi sebaik sahaja menerimanya;
- (iv) e-mel rahsia rasmi bertanda *Rahsia Besar* dan *Rahsia* tidak boleh dimajukan kepada pihak lain. Sementara e-mel bertanda *Sulit* dan *Terhad* yang hendak dimajukan kepada pihak lain memerlukan izin daripada pemula dokumen;
- (v) e-mel yang melibatkan maklumat rahsia rasmi yang hendak dimusnahkan perlulah ditulis ganti (overwrite) sekurang-kurangnya tiga (3) kali dengan fail yang lain sebelum dipadamkan; dan
- (vi) agensi perlu menentukan sistem e-mel rahsia rasmi yang disambungkan kepada Internet atau Intranet mesti mempunyai sistem keselamatan yang mencukupi seperti *Firewall* dan *Virtual Private Network*.

TANGGUNGJAWAB PENTADBIR SISTEM ICT

15. Bagi memastikan pengendalian Internet dan e-mel agensi beroperasi dengan sempurna dan berkesan, pentadbir sistem ICT adalah bertanggungjawab:

- (a) menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan Ketua Jabatan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat. Pentadbir sistem ICT boleh membekukan akaun pengguna, jika perlu, semasa pengguna bercuti panjang, berkursus atau pun menghadapi tindakan tatatertib;
- (b) menggunakan perisian pemecahan kata laluan yang dibenarkan untuk mengenal pasti kata laluan pengguna yang lemah dan kemudiannya mencadang dan memperakukan ciri-ciri kata laluan yang lebih baik kepada pengguna;

- (c) menghalang kemasukan maklumat dari laman Internet yang berunsur ganas, lucas, permainan elektronik atas talian, judi dan lain-lain aktiviti yang dilarang;
- (d) menyimpan jejak audit selama sekurang-kurangnya dua (2) bulan di dalam pelayan e-mel berkenaan, tertakluk kepada kemampuan ruang storan, dan tiga (3) tahun di dalam media storan lain;
- (e) menjalankan pemantauan dan penapisan kandungan fail elektronik dan e-mel secara berkala jika difikirkan perlu tanpa terlebih dahulu merujuk kepada pengguna. Ini bertujuan memastikan pelaksanaannya mematuhi dasar dan tatacara yang ditetapkan;
- (f) melaksanakan jadual penstoran dan pengarkiban e-mel agensi. Penyimpanan media storan sama ada di luar atau di dalam kawasan mestilah mempunyai ciri-ciri keselamatan fizikal yang terjamin bagi mengelak daripada sebarang risiko seperti kehilangan maklumat bernilai;
- (g) memaklumkan kepada Ketua Jabatan sekiranya mengalami insiden keselamatan seperti pencerobohan sistem, serangan virus atau sebarang masalah kerosakan. Pentadbir sistem ICT hendaklah mengurus dan menangani insiden yang berlaku dengan segera dan sistematik sehingga keadaan kembali pulih. Agensi juga perlu melaporkan setiap insiden kepada GCERT mengikut Pekeliling Am Bil. 1 Tahun 2001 "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)"; dan
- (h) melaksanakan penyelenggaraan ke atas sistem e-mel dengan baik dan menentukan segala *patches* terkini yang disediakan oleh pihak pembekal perisian dipasang dan berfungsi dengan sempurna.

TANGGUNGJAWAB PENGGUNA

16. Pengguna hendaklah mematuhi tatacara penggunaan Internet dan e-mel yang telah ditetapkan agar keselamatan ke atas pemakaiannya akan terus terjamin. Peranan dan tanggungjawab pengguna adalah seperti berikut:

- (a) menggunakan akaun atau alamat e-mel yang diperuntukkan oleh jabatan;
- (b) memaklumkan kepada pentadbir sistem ICT dengan segera sekiranya mengesyaki akaun telah disalahgunakan;
- (c) menggunakan kata laluan yang baik dengan ciri-ciri keselamatan yang bersesuaian dengan merujuk Amalan Baik Keselamatan Kata Laluan di **Lampiran C**;
- (d) memastikan setiap fail yang dimuat turun bebas dari virus sebelum digunakan;
- (e) bertanggungjawab sepenuhnya terhadap semua kandungan fail elektronik termasuk e-mel di dalam akaun sendiri. Dengan itu, pengguna perlu bertindak bijak, profesional dan berhati-hati apabila berkomunikasi menerusi saluran elektronik;
- (f) berhenti dan memutuskan talian dengan serta-merta sekiranya kakitangan menerima dan disambungkan ke laman Internet yang mengandungi unsur-unsur tidak menyenangkan;
- (g) mengadakan salinan atau penduaan pada media storan kedua elektronik seperti disket dan sebagainya bagi tujuan keselamatan;

- (h) memastikan kemudahan e-mel digunakan dan dibiarkan aktif pada keseluruhan waktu bekerja supaya e-mel yang dialamatkan sampai tepat pada masanya dan tindakan ke atasnya dapat disegerakan;
- (i) menggunakan kemudahan *password screen saver* atau log keluar apabila hendak meninggalkan komputer;
- (j) memaklumkan kepada pentadbir sistem ICT sekiranya berada di luar pejabat dalam tempoh waktu yang panjang, bercuti atau bertukar tempat kerja bagi memudahkan penyelenggaraan dilakukan; dan
- (k) memaklumkan kepada pentadbir sistem ICT atau pegawai keselamatan ICT (ICTSO) sekiranya berlaku atau mengesyaki berlakunya insiden keselamatan ICT.

KHIDMAT NASIHAT

17. Sebarang kemusykilan berkaitan dengan Pekeliling ini dan Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik bolehlah dirujuk kepada MAMPU, manakala kemusykilan berkaitan dengan Arahan Keselamatan hendaklah dirujuk kepada Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia dan kemusykilan mengenai pengarkiban e-mel hendaklah dirujuk kepada Arkib Negara Malaysia. Permohonan untuk keterangan lanjut mengenai kandungan dokumen ini boleh ditujukan kepada:

Unit Pemodenan Tadbiran dan Perancangan
Pengurusan Malaysia (MAMPU)
Jabatan Perdana Menteri
Aras 6, Blok B2, Parcel B
Kompleks Jabatan Perdana Menteri
Pusat Pentadbiran Kerajaan Persekutuan
62502 PUTRAJAYA.

Tel.: 03-88882250, Faks: 03-88883286
E-mel: ictsec@mampu.gov.my

PENUTUP

18. Garis Panduan ini mengandungi amalan-amalan terbaik penggunaan Internet dan mel elektronik yang patut diikuti oleh semua anggota Perkhidmatan Awam dan akan dikemas kini dari semasa ke semasa selaras dengan arus perkembangan teknologi maklumat dan komunikasi (ICT) dan perundangan. Dokumen ini hendaklah dibaca bersama dengan dokumen *Malaysian Public Sector Management of Information & Communications Technology Security Handbook* (MyMIS) dan Buku Arahan Keselamatan.

Contoh Format E-mel Bukan Rahsia Rasmi

To: ahmad@mod.gov.my	
Cc: ali@kabinet.jpm.my	
Subject: Program Latihan Khidmat Negara	No.Ruj.: KP/JLKN (17(2))
 JABATAN LATIHAN KHIDMAT NEGARA KEMENTERIAN PERTAHANAN MALAYSIA ARAS 8-10, MENARA TH SELBORN 153 JALAN TUN RAZAK 50400 KUALA LUMPUR	

Contoh Format E-mel Rahsia Rasmi

To: aziz@agc.gov.my	
Cc: razak@mampu.gov.my	
Subject: Pandangan ke atas Draf Akta EGA	No.Ruj.: UPTM(R) 159/338/12
	UNIT PEMODENAN TADBIRAN DAN PENGURUSAN PERANCANGAN MALAYSIA (MAMPU) ARAS 6, BLOK B2, PARCEL B KOMPLEKS JABATAN PERDANA MENTERI PUSAT PENTADBIRAN KERAJAAN PERSEKUTUAN 62502 PUTRAJAYA
RAHSIA	
RAHSIA	

Amalan Baik Keselamatan Kata Laluan

1. Rahsiakan kata laluan anda dari pengetahuan orang lain. Pendedahan kepada yang tidak berhak adalah satu kesalahan di bawah Akta Jenayah Komputer 1997.
2. Sekiranya kata laluan telah dikompromi atau disyaki dikompromi, hendaklah dilaporkan kepada pentadbir sistem ICT dan kata laluan sedia ada diubah dengan serta merta.
3. Kata laluan hendaklah diubah sekurang-kurangnya sekali dalam 30 hari.
4. Kata laluan hendaklah mempunyai saiz sekurang-kurangnya lapan (8) aksara dengan gabungan alphanumerik dan simbol khas. Contoh kata laluan yang baik adalah "j2-yU!pa". (AMARAN: Jangan guna kata laluan ini kerana ianya telah diketahui umum).
5. Elakkan dari menggunakan semula empat (4) kata laluan yang terdahulu.
6. Kata laluan hendaklah dihafal dan jangan sekali-kali disalin di mana-mana media.

