**GARISPANDUAN MENGENAI TATACARA PENGGUNAAN INTERNET DAN MEL ELKTRONIK DI AGENSI-AGENSI KERAJAAN**

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

**TATACARA PENGGUNAAN INTERNET**

1. 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, menggangu 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.

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

(b) **Memilih Laman**
Laman yang dilayari dari Internet perlulah 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 amaln 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 Jabatan sebelum dimuat naik.

(e) **Muat Turun Bahan**
Tindakan memuat turun hanya dibenarkan ke atas bahan yang sah seperti perisian yang berdaftar dan di bawaj 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.

3. Perbincangan awam adalah **dilarang** daripada melakukan sebaran aktiviti yang melanggar tatacara penggunaan Internet seperti :

(a) memuat naik, memuat turun, menyimpan dan menggunakan perisian yang 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 pengganas;
(l) memuat naik, memuat turun, menghantar dan menyimpan kad elektronik, video, lagu dan kepilan 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**

4. 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 rasnu yang mesti diberi perlindungan untuk kepentingan keselamatan yang dikelaskan mengikut pengelasannya samada *Terhad, Sulit* atau *Rahsia Besar.*

(b) **E-mel Bukan Rahsia Rasmi**

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

5. 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 disamping 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 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.

6. 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 born, e-mel *sparm,* fitnah, ciplak atau aktiviti-aktiviti lain yang ditegah 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.

KAWALAN KESELAMATAN INTERNET DAN E-MEL

7. 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 melindundi maklumat rahsia rasmi dan maklumat bukan rahsia rasmi kerajaan dari capaian tanpa kuasa yang sah. Keselamatan Internet dan e-mel bergantung kepada factor-faktor sokongan berikut.

(a). **Keselamatan**
Komputer hendaklah diletakkan di tempat yang mempunyai kawalan fizikal yang selamat daripada pencerobohan 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 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 & Communication Technology Security Handbook(MyMIS),* Buku Arahan Keselamatn dan Surat Pekeliling Am Bil. 2 Tahun 1987 “Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi(Pindaan) 1986“.

Sekiran Penyelenggaraan komputer hendak dilaksanakan, agensi perlu memastikan semua maklumat bukan rahsia rasmi atau rasmi didalam 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 iaiti 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 kesahijan dokumen apabila tandatangani secara digital oleh pengirim;

iii. penerima mesti membuat akuan penerimaan e-mel rahsia rasmi sebaik sahaha 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 Intenet atau Intranet mesti mempunyai sistem keselamatan yang mencukupi seperti *Firewall* dan *Virtual Private Network*

**TANGGUNGJAWAP PENTADBIRAN SISTEM ICT**

8. Bagi memastikan pengendalian internet dan e-mel agensi beroperasi dengan sempurna dan berkesan, pentadbiran system **ICT** adalah bertanggungjawap:

(a) Menentukan setiap pengendalian akaun yang diwujudkan atau dibatalkan mendapat kelulusan Ketua Jabatan. Pembatalan akaun (pengguna yang berhenti , bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat. Pentadbiran system **ICT** boleh membekukan akaun pengguna , jika perlu, semasa pengguna bercuti panjang , berkursus atau pun menghadapi tindakan tattertib;

(b) Menggunakan perisian pemecahan kata laluan yang dibenarkan untuk mengenalpasti kata laluan pengguna yang lemah dan kemudiannya mencadang dan memperakukan cirri-ciri kata laluan yang lebih baik kepada pengguna;

(c) Menghalang kemasukan maklumat dari laman internet yang berunsur ganas, lucah, 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, tertakhluk 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 storan berkala jika difikirkan perlu tanpa terlebih dahulu merujuk kepada pengguna. Ini bertujuan 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 cirri-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 system, serangan virus atau sebarang masalah kerosakan.Pentadbiran system **ICT** hendakalah mengurus dan menangani insidan yang berlaku dengan segera dan sistematik sehingga keadaan kembali pulih. Agensi juga perlu melaporkan setiap insiden kepada **GCERT** megikuti Pekeliling Am Bil. 1 Tahun 2001 “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (**ICT**)”; dan

(h) Melaksanakan penyelenggaraan ke atas system e-mel dengan baik dan menentukan segera *patches* terkini yang disediakan oleh pihak pembekal perisian dipasang dan berfungsi dengan sempurna.

**TANGGUNGJAWAP PENGGUNA**

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

(a) Mengugunakan akaun atau alamat e-mel yang diperuntukan oleh kerajaan;

(b) Memaklumkan kepada pentadbiran system **ICT** dengan segera sekiranya mengesyaki akuan telah disalahgunakan;

(c) Menggunakan kata laluan yang baik dengan cirri-ciri keselamatan yang bersesuaian dengan merujuk Amalan Baik Keselamatan Kata Laluan di **Lampiran C.**

(d) Memastikan setiap fail yang muat turun bebas dari virus sebelum digunakan

(e) Bertanggungjawap sepenuhnya terhadap semua kendungan fail elektonik termasuk e-mel di dalam akaun sendiri. Dengan itu, pengguna perlu bertindak bijak, professional dan berhati-hati apebila berkomunikasi menerusi saluran elektronik;

(f) Berhenti dan memutuskan talian dengan serta-merta sekiranya kakitangan menerima dan disambungkan ke laman Internet yang mengandungi unsure-unsur tidak menyenangkan;

(g) Mengdakan saliran 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 logkeluar apabila hendak meninggalkan computer;

(j) Memaklumkan kepada pentadbir system **ICT** sekiranya berada di luar pejabat dalam tempoh waktu yang panjang, bercuti atau bertukar tempat kerja bagi memudahkan penyelenggaraan dilakukan; dan

(k) Memaklumkan kepada pentadbiran system **ICT** atau pegawai keselamatan **ICT** (I**CTSO**) sekiranya berlaku atau mengesyaki berlakunya insiden keselamatan **ICT.**