POLISI PENGGUNAAN MEL ELEKTRONIK
UNIVERSITI MALAYSIA KELANTAN

Universiti Malaysia
KELANTAN

POLISI PENGGUNAAN MEL ELEKTRONIK
UNIVERSITI MALAYSIA KELANTAN

1.0 TUJUAN

1.1 Polisi ini bertujuan untuk menerangkan tatacara dan kriteria penggunaan mel elektronik yang perlu dipatuhi oleh warga Universiti Malaysia Kelantan (UMK) supaya:

1.1.1 Memberikan langkah-langkah perlindungan dan penguatkuasaan, agar penggunaan emel terkawal dan perlindungan keselamatan yang lebih mantap dapat diwujudkan;

1.1.2 Penyebaran dan perkongsian maklumat adalah terkawal;

1.1.3 Memastikan maklumat yang disampaikan adalah jelas dan tepat; dan

1.1.4 Maklumat yang disampaikan tidak akan menjejaskan kepentingan perkhidmatan awam dan kedaulatan Negara.

2.0 LATAR BELAKANG

2.1 Universiti Malaysia Kelantan (UMK) sentiasa berusaha meningkatkan kecekapan dalam proses komunikasi di kalangan anggota dan di antara agensi-agensi kerajaan yang lain dan orang ramai. Penggunaan sistem mel elektronik telah membuka peluang kepada komunikasi yang lebih cepat dan mudah. Selain daripada memudah dan mempercepatkan komunikasi, kaedah ini dapat mengurangkan penggunaan kertas dan akhirnya menyumbang kepada peningkatan produktiviti dan kualiti perkhidmatan.

2.2 Namun begitu, penggunaan 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

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

2.4 Sehubungan itu, garis panduan ini disediakan untuk memperkukuhkan lagi pelaksanaan dan penggunaan mel elektronik di Universiti bagi memastikan ianya berfungsi dengan lebih berkesan.

3.0 TATACARA PENGGUNAAN MEL ELEKTRONIK

3.1 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.

3.2 Setiap setiap staf Universiti mempunyai e-mel rasmi yang digunakan untuk tujuan rasmi dan didaftarkan di bawah domain milik Universiti Malaysia Kelantan. Contoh alamat e-mel rasmi yang ialah ahmad@umk.edu.my. E-mel rasmi boleh dibahagikan kepada dua kategori iaitu e-mel rahsia rasmi dan e-mel bukan rahsia rasmi.

3.2.1 **E-mel Rahsia Rasmi**

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

3.2.2 **E-mel Bukan Rahsia Rasmi**

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

3.3 Berikut adalah kaedah penggunaan e-mel yang betul dan disesuaikan pemakaiannya di Universiti:-

3.3.1 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.

3.3.2 Format

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.

3.3.3 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 1 hari bekerja** 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.

3.3.4 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 25MB. Sekiranya kepilan melebihi saiz ini, khidmat storan awan (*cloud storage*) Universiti boleh digunakan.

3.3.5 Penerimaan

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

3.3.6 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.

3.3.7 Penyimpanan

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 adalah digalakkan bagi tujuan keselamatan.

3.3.8 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).

3.3.9 Tarikh dan Masa Sistem Komputer

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

3.4 Pengguna adalah **dilarang** daripada melakukan sebarang aktiviti yang melanggar tatacara penggunaan e-mel rasmi Universiti seperti:

3.4.1 Menggunakan akaun milik orang lain, berkongsi akaun atau memberi akaun kepada orang lain;

3.4.2 Menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah;

3.4.3 Menggunakan e-mel untuk tujuan komersial atau politik;

3.4.4 Menghantar dan memiliki bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian dan jenayah;

3.4.5 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;

3.4.6 Menyebarkan kod perosak seperti virus, *worm*, *trojan horse* dan *trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;

3.4.7 Menghantar semula berulang kali e-mel yang gagal sampai ke destinasi sehingga boleh menjejaskan sistem e-mel penerima sebelum menyiasat punca e-mel gagal dihantar; dan

3.4.8 Membenarkan pihak ketiga untuk menjawab e-mel kepada penghantar asal bagi pihaknya.

3.5 Jika pengguna disyaki telah melakukan kesalahan seperti perkara 3.4, siasatan akan dilakukan dan tindakan boleh dikenakan kepada pengguna mengikut prosedur dan peraturan sedia ada.

4.0 KAWALAN KESELAMATAN E-MEL

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

4.1.1 **Keselamatan Fizikal**

Komputer hendaklah diletakkan di tempat yang mempunyai kawalan fizikal yang selamat daripada pencerobohan atau sebarang bentuk capaian tidak sah.

4.1.2 **Keselamatan Dokumen Elektronik**

Bagi memastikan semua fail yang dihantar dan diterima bebas daripada sebarang bentuk ancaman keselamatan, perisian antivirus dan penapis kod jahat (*malicious codes)* perlulah dikemas kini dari semasa ke semasa.

Semua maklumat rahsia rasmi atas talian yang telah dikelaskan perlu berada dalam bentuk enkripsi sepanjang masa, manakala maklumat rahsia rasmi yang tidak diperlukan atas talian mesti dipindahkan segera ke media storan elektronik sekunder dalam bentuk enkripsi 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.

4.1.3 **Tandatangan Digital**

a. Sistem e-mel yang mengandungi maklumat rahsia rasmi mesti menggunakan sijil digital (*digital certificate*) yang dikeluarkan oleh pihak berkuasa perakuan tempatan yang ditauliahkan oleh Kerajaan Malaysia iaitu Pihak Berkuasa Persijilan (*Certification Authority*) atau yang setara dengannya.

b. Setiap e-mel yang dihantar hendaklah disertakan dengan tandatangan digital (*digital signature*) untuk tujuan pengesahan identiti penghantar.

c. Pentadbir akaun emel khas bagi kegunaan Pusat Tanggungjawab, Fakulti, Persatuan/Kesatuan, kumpulan atau sebagainya hendaklah menyertakan tandatangan digital individu yang dipertanggungjawabkan ke atas emel khas tersebut.

4.1.4 **Keselamatan Pengendalian E-mel Rahsia Rasmi**

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

a. Enkripsi mesti dilakukan ke atas semua dokumen rahsia rasmi yang dihantar, diterima dan disimpan;

b. Penerima e-mel rahsia rasmi mesti mengesahkan kesahihan dokumen apabila ditandatangani secara digital oleh pengirim;

c. Penerima mesti membuat akuan penerimaan e-mel rahsia rasmi sebaik sahaja menerimanya;

d. 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; dan

e. Universiti 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*.

5.0 TANGGUNGJAWAB PENTADBIR SISTEM MEL ELEKTRONIK

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

5.1.1 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;

5.1.2 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;

5.1.3 Menghalang kemasukan maklumat dari laman Internet yang berunsur ganas, lucah, permainan elektronik atas talian, judi dan lain-lain aktiviti yang dilarang;

5.1.4 Menggunakan skema berikut bagi mewujudkan kata nama pengguna:-

a. Bagi pengguna yang mempunyai nama keluarga.
< Singkatan Nama >< Nama Keluarga >@< Nama Domain >
Contoh: gmorris@umk.edu.my dan etsiah@umk.edu.my

b. Bagi pengguna yang tidak mempunyai nama keluarga,
< Nama >@< Nama Domain > atau
< Nama >.< Singkatan Nama Bapa >@< Nama Domain >
Contoh:- fadli@umk.edu.my atau azmin.mr@umk.edu.my

5.1.5 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;

5.1.6 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

5.1.7 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.

5.1.8 Menyah-aktifkan akaun pengguna yang tamat perkhidmatan dalam tempoh empat bulan selepas tarikh penamatannya. Akaun pengguna ini hendaklah disimpan selama sekurang-kurangnya tiga tahun sebelum dilupuskan.

6.0 TANGGUNGJAWAB PENGGUNA

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

6.1.1 menggunakan akaun atau alamat e-mel yang diperuntukkan oleh jabatan;

6.1.2 memaklumkan kepada pentadbir sistem ICT dengan segera sekiranya mengesyaki akaun telah disalahgunakan;

6.1.3 Menggunakan kata laluan yang baik dengan ciri-ciri keselamatan yang bersesuaian dengan merujuk Amalan Baik Keselamatan Kata Laluan di **Lampiran A**;

6.1.4 Memastikan setiap fail yang dimuat turun bebas dari virus sebelum digunakan;

6.1.5 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;

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

6.1.7 Mengadakan salinan pendua kepada media storan elektronik seperti disket dan sebagainya bagi tujuan keselamatan;

6.1.8 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;

6.1.9 Menggunakan kemudahan password *screensaver* atau log keluar apabila hendak meninggalkan komputer;

6.1.10 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

6.1.11 Memaklumkan kepada pentadbir sistem ICT atau pegawai keselamatan ICT (ICTSO) sekiranya berlaku atau mengesyaki berlakunya insiden keselamatan ICT.

7.0 TARIKH KUATKUASA

7.1 Polisi ini berkuatkuasa mulai tarikh ia dikeluarkan dan warga UMK haruslah mematuhinya.

8.0 KHIDMAT NASIHAT

8.1 Sebarang kemusykilan berkaitan dengan Polisi ini bolehlah dirujuk kepada:-

Pusat Komputeran dan Informatik,
Universiti Malaysia Kelantan, Kampus Kota,
Karung Berkunci 36, Pengkalan Chepa,
16100 Kota Bharu. Kelantan.
Tel.: 09-7717117, Faks: 09-7717172
E-mel: cci@umk.edu.my

9.0 PENUTUP

9.1 Polisi ini mengandungi amalan-amalan terbaik tatacara penggunaan mel elektronik yang patut diikuti oleh semua warga UMK dan akan dikemas kini dari semasa ke semasa selaras dengan arus perkembangan teknologi dan perundangan. Dokumen ini hendaklah dibaca bersama dengan dokumen *Dasar Keselamatan Teknologi Maklumat dan Komunikasi Universiti Malaysia Kelantan, Peraturan Pelaksanaan Dasar ICT Universiti Malaysia Kelantan, Malaysian Public Sector Management of Information & Communications Technology Security Handbook (MyMIS)* dan *Buku Arahan Keselamatan.*

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 unik untuk setiap akaun yang berbeza.

5. Kata laluan hendaklah mempunyai saiz sekurang-kurangnya dua belas (12) aksara dengan gabungan alphanumerik dan simbol khas.

6. Pastikan kata laluan merupakan suatu yang tidak mudah diteka atau dijangkakan.

7. Elakkan dari menggunakan semula kata laluan yang pernah digunakan.

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