



**KERAJAAN MALAYSIA**

**SURAT PEKELILING AM KETUA SETIAUSAHA  
KEMENTERIAN KESIHATAN  
BILANGAN 7 TAHUN 2011**

**TATACARA PENGGUNAAN DAN KESELAMATAN ICT KKM  
VERSI 3.0**

**BAHAGIAN PENGURUSAN MAKLUMAT (BPM)  
KEMENTERIAN KESIHATAN MALAYSIA**

**Dikelilingkan kepada:**

**Semua Setiausaha Bahagian  
Semua Pengarah Bahagian  
Semua Pengarah Kesihatan Negeri  
Semua Pengarah Institut Kesihatan  
Semua Pengarah Hospital**



**KETUA SETIAUSAHA  
KEMENTERIAN KESIHATAN MALAYSIA**

Aras 12, Blok E7, Kompleks E,  
Pusat Pentadbiran Kerajaan Persekutuan,  
62590 Putrajaya

Telefon: 03-88832533  
Fax : 03-88895245

Rujukan Kami : ( 19 ) dlm KKM/BPM/190/4/6 Jld 2  
Tarikh : 20 September 2011

Semua Setiausaha Bahagian  
Semua Pengarah Bahagian  
Semua Pengarah Kesihatan Negeri  
Semua Pengarah Institut Kesihatan  
Semua Pengarah Hospital

---

**SURAT PEKELILING AM KETUA SETIAUSAHA KEMENTERIAN KESIHATAN  
MALAYSIA BILANGAN 7 TAHUN 2011**

---

**TATACARA PENGGUNAAN DAN KESELAMATAN ICT KKM VERSI 3.0**

**TUJUAN**

Surat Pekeliling Am ini bertujuan untuk menggantikan garis panduan yang sedia ada mengenai tatacara penggunaan dan keselamatan ICT di Kementerian Kesihatan Malaysia.

**LATAR BELAKANG**

2. MAMPU telah mengemas kini **Dasar Keselamatan ICT (DKICT) MAMPU** kepada **versi 5.3**, berkuat kuasa pada 24 Mei 2010. MAMPU juga telah mengeluarkan **Surat Pekeliling Am Bilangan 3 Tahun 2009 – “Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam”**, pada 17 November 2009 dan **Surat Arahan Ketua Pengarah MAMPU - “Pengurusan Kesenambungan**

**Perkhidmatan Agensi Sektor Awam”, pada 22 Januari 2010.** Langkah-langkah pengemaskinian dilakukan bagi memastikan tatacara sentiasa seiring dengan keperluan penguatkuasaan kawalan dan langkah-langkah menyeluruh dalam melindungi aset ICT kerajaan.

3. Sehubungan dengan itu **Surat Pekeliling Am Kementerian Kesihatan Malaysia Bil. 2/2009 – “Tatacara Penggunaan dan Keselamatan ICT KKM”** telah dikemas kini selaras dengan perkhidmatan semasa KKM dan teknologi ICT yang berubah. Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Kementerian Kesihatan Malaysia Bil. 3/2011 yang telah diadakan pada 16 Ogos 2011 telah bersetuju untuk mengguna pakai dan menguatkuasakan peraturan-peraturan yang ditetapkan di dalam surat pekeliling ini.

#### **TANGGUNGJAWAB AGENSI**

5. Semua agensi di bawah Kementerian Kesihatan Malaysia adalah dikehendaki mematuhi **Tatacara Penggunaan Dan Keselamatan ICT KKM Versi 3.0** dan melaksanakan tanggungjawab yang ditetapkan di dalamnya.

#### **PERANAN BAHAGIAN PENGURUSAN MAKLUMAT (BPM)**

6. BPM bertanggungjawab di dalam memastikan kepatuhan kepada Surat Pekeliling ini di Kementerian Kesihatan Malaysia.

#### **TARIKH KUATKUASA**

7. Surat Pekeliling Am ini berkuatkuasa mulai tarikh ia dikeluarkan.

## **PEMBATALAN**

8. Dengan berkuat kuasanya **Surat Pekeliling Am ini, maka Surat Pekeliling Am Kementerian Kesihatan Malaysia Bilangan 2 Tahun 2009** adalah dibatalkan.

**“BERKHIDMAT UNTUK NEGARA”**



**DATUK KAMARUL ZAMAN BIN MD ISA**

s.k

Ketua Pengarah Kesihatan  
Timbalan Ketua Setiausaha (Pengurusan)  
Timbalan Ketua Setiausaha (Kewangan)  
Timbalan Ketua Pengarah Kesihatan (Kesihatan Awam)  
Timbalan Ketua Pengarah Kesihatan (Perubatan)  
Timbalan Ketua Pengarah Kesihatan (Penyelidikan dan Sokongan Teknikal)  
Pengarah Kanan (Kesihatan Pergigian)  
Pengarah Kanan (Perkhidmatan Farmasi)  
Pengarah Kanan (Keselamatan dan Kualiti Makanan)  
Setiausaha Sulit Kanan YB Menteri Kesihatan  
Setiausaha Sulit Kanan YB Timbalan Menteri Kesihatan



# **TATACARA PENGGUNAAN DAN KESELAMATAN ICT KEMENTERIAN KESIHATAN MALAYSIA**

**20 September 2011**

**Versi 3.0**

## SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUAT KUASA
6 Mac 2007	1.0	JPICT Bil 1/2007	5 Jun 2007
21 Disember 2009	2.0	JPICT Bil 4/2009	23 Disember 2009
16 Ogos 2011	3.0	JPICT Bil 3/2011	20 September 2011

## JADUAL PINDAAN

TARIKH	VERSI	BUTIRAN PINDAAN	MUKA SURAT
22 Mac 2011	3.0	<p><b>i. Kemaskini perkara 4.2.3 seperti berikut:</b>  memuat turun, menyimpan dan menggunakan perisian yang tidak <u>tulen</u>;  (TPDKICT Terdahulu : <u>berlesen</u>)</p>	11
		<p><b>ii. Kemaskini perkara 4.2.7 seperti berikut:</b>  memuat turun fail-fail yang bersaiz besar sehingga 10 MB. Bagi saiz fail melebihi 10 MB ianya hendaklah mendapatkan khidmat nasihat dari Pentadbir <u>Emel</u> terlebih dahulu;  (TPDKICT Terdahulu : <u>Rangkaian</u>)</p>	12
		<p><b>iii. Kemaskini perkara 4.2.8 seperti berikut:</b>  pengguna yang menggunakan aplikasi web adalah bertanggungjawab sepenuhnya ke atas maklumat yang <u>di key-in</u>  (TPDKICT Terdahulu : <u>dikunci masuk</u>)</p>	12
		<p><b>iv. Kemaskini perkara 4.2.19 seperti berikut:</b>  menggunakan <u>proxy</u> selain dari yang telah ditetapkan oleh Pentadbir <u>Rangkaian</u>; dan  (TPDKICT Terdahulu : menggunakan <u>proxy lain</u> selain dari yang telah ditetapkan oleh Pentadbir <u>Sistem</u>)</p>	13
		<p><b>v. Kemaskini perkara 9.0 (c) Keselamatan Kata Laluan seperti berikut:</b>  (c) kata laluan perlu ditukar <u>dalam tempoh</u></p>	34

		<p><u>90 hari;</u> (TPDKICT Terdahulu : <u>setiap 30 hari</u>)</p>	
		<p><b>vi. Penambahan perkara 9.0 (e) Keselamatan Kata Laluan seperti berikut:</b> (e) ID pengguna tidak boleh digunakan sebagai kata laluan; (TPDKICT Terdahulu : Tidak wujud)</p>	34
		<p><b>vii. Penambahan perkara 15.0 (i) Pembangunan Aplikasi</b> (i) Setiap aplikasi perlu direka dengan fungsi menguatkuasakan tamat masa sesi yang terbiar (<i>idle timeout</i>) , iaitu apabila tiada aktiviti pengguna untuk tempoh masa yang tertentu, sesi akan ditamatkan. Pengguna perlu log masuk semula selepas penamatan <i>idle timeout</i> tersebut. Saranan bagi tempoh tamat masa adalah 15 minit. (TPDKICT Terdahulu : Tidak wujud)</p>	48



## Isi Kandungan

1.0	PENGENALAN .....	6
2.0	OBJEKTIF .....	7
3.0	KESELAMATAN MAKLUMAT .....	8
3.1	Kerahsiaan ( <i>Confidentiality</i> ) .....	8
3.2	Integriti ( <i>Integrity</i> ) .....	8
3.3	Sumber Yang Sah ( <i>Authenticity</i> ) .....	8
3.4	Kesahihan ( <i>Accountability</i> ) .....	8
3.5	Kebolehsediaan ( <i>Availability</i> ).....	8
4.0	KESELAMATAN INTERNET .....	9
4.1	TATACARA PENGGUNAAN INTERNET .....	9
4.1.1	Hak Terhadap Capaian Oleh Pengguna .....	9
4.1.2	Pemilihan Laman Yang Hendak Dilayar .....	10
4.1.3	Pengesahan Maklumat .....	10
4.1.4	Muat Naik Bahan .....	10
4.1.5	Muat Turun Bahan .....	10
4.1.6	Perbincangan atau Forum Awam.....	10
5.0	KESELAMATAN MEL ELEKTRONIK (EMEL).....	14
5.1	TATACARA PENGGUNAAN EMEL .....	14
5.2	Larangan dan Salahlaku Pengguna Emel.....	18
5.3	Tanggungjawab dan Peranan Pengguna Emel .....	20
5.4	Tanggungjawab Pentadbir Emel.....	21
5.5	Kelayakan .....	25
6.0	KAWALAN KESELAMATAN EMEL DAN INTERNET .....	26
6.1	Keselamatan Fizikal .....	26
6.2	Keselamatan Dokumen Elektronik.....	26
6.3	Tandatangan Digital .....	27
6.4	Keselamatan Pengendalian Emel Rahsia Rasmi.....	27
7.0	KESELAMATAN DARI ANCAMAN VIRUS .....	29
8.0	PENGGUNAAN DAN PENGURUSAN RANGKAIAN .....	30
8.1	Infrastruktur Rangkaian .....	30
8.2	Tanggungjawab Pentadbir Rangkaian.....	31
8.3	Pengurusan Alamat Internet Protokol (IP) .....	32
8.4	Sambungan Rangkaian.....	32
8.5	Dial-Up / Jalur Lebar ( <i>Broadband</i> ) / Rangkaian Tanpa Wayar ( <i>wireless</i> ).....	33
8.6	<i>File Transfer Protocol</i> (FTP) .....	33
9.0	KESELAMATAN KATA LALUAN .....	34
10.0	KESELAMATAN RANGKAIAN ( <i>NETWORK SECURITY</i> ) .....	35
11.0	KESELAMATAN FIZIKAL PERKAKASAN ICT KKM .....	37
12.0	TATACARA PENGURUSAN MEDIA STORAN.....	40
13.0	KESELAMATAN PERKAKASAN ICT DI PUSAT DATA/BILIK SERVER KKM ...	42
14.0	KESELAMATAN PERISIAN SISTEM DAN PANGKALAN DATA .....	44
14.1	Pembaik Pulih Sistem .....	44
14.2	Pelan Pemulihan Bencana ( <i>Disaster Recovery Plan</i> ).....	47
15.0	PEMBANGUNAN SISTEM APLIKASI.....	48
16.0	PERANAN DAN TANGGUNGJAWAB SEMUA FASILITI KKM .....	50
17.0	KHIDMAT NASIHAT .....	51
18.0	PENUTUP .....	52

# TATACARA PENGGUNAAN DAN KESELAMATAN ICT KEMENTERIAN KESIHATAN MALAYSIA

## 1.0 PENGENALAN

Peningkatan penggunaan kemudahan teknologi maklumat dan komunikasi (ICT) dalam tugas seharian terutama yang melibatkan aplikasi internet dan emel telah mendedahkan maklumat penting kepada pihak luar. Untuk memastikan maklumat-maklumat penting di Kementerian Kesihatan Malaysia (KKM) bebas daripada ancaman yang boleh mengancam keselamatan aset ICT KKM, semua pengguna perlu mematuhi dokumen Tatacara Penggunaan dan Keselamatan ICT di KKM seperti yang telah ditetapkan. Dokumen ini dikeluarkan oleh Bahagian Pengurusan Maklumat (BPM) bagi meminda dan membuat penambahan terhadap dokumen yang sedia ada seiring dengan perkembangan teknologi maklumat dan perundangan siber. Dokumen ini telah diperakukan oleh Mesyuarat Jawatankuasa Pemandu Bil. 3 Tahun 2011 pada 16 Ogos 2011 untuk diguna pakai ke seluruh KKM berkuatkuasa pada 20 September 2011. Dokumen ini selaras dengan Pekeliling Am Bil. 3 Tahun 2000 dan Pekeliling Kemajuan Perkhidmatan Awam Bil. 1 Tahun 2003 yang dikeluarkan oleh Jabatan Perdana Menteri dan ia telah disesuaikan bagi kegunaan KKM.

## 2.0 OBJEKTIF

Tujuan utama Tatacara Penggunaan dan Keselamatan ICT di KKM adalah sebagai panduan pengguna demi menjamin kesinambungan urusan kerajaan dan menghindar kesan insiden keselamatan. Dalam era ICT masa kini keselamatan maklumat adalah menjadi perkara utama yang harus dielakkan daripada disalahguna oleh orang yang tidak bertanggungjawab. Maklumat adalah berharga kerana kebanyakan informasi tersebut adalah sensitif dan terperingkat. Penyalahgunaan maklumat oleh orang yang tidak bertanggungjawab bukan sahaja akan memberi ruang kebocoran rahsia malah menjejaskan reputasi organisasi dan negara. Justeru, Tatacara Penggunaan dan Keselamatan ICT di KKM perlu dipinda selaras dengan perkembangan teknologi supaya dapat dijadikan panduan kepada pengguna dengan tujuan menjamin kerahsiaan, integriti, sumber yang sah, kesahihan dan kebolehsediaan maklumat yang berterusan.

### 3.0 KESELAMATAN MAKLUMAT

Tatacara ini juga bertujuan untuk menjamin dan meningkatkan lagi tahap keselamatan maklumat yang dicapai, dihantar atau pun dirujuk. Matlamat utama ialah supaya maklumat sentiasa bebas dari sebarang bentuk ancaman seperti virus, penggadam atau diubah semasa penghantaran atau penerimaan. Tatacara ini melindungi keselamatan maklumat sesuatu organisasi dalam beberapa aspek seperti berikut:

#### 3.1 Kerahsiaan (*Confidentiality*)

Maklumat tidak boleh disebarikan sewenang-wenangnya atau dibiarkan dicapai tanpa kebenaran.

#### 3.2 Integriti (*Integrity*)

Data dan maklumat hendaklah tepat, lengkap, kemaskini dan tidak berlaku manipulasi. Ia hanya boleh diubah oleh pegawai yang dibenarkan.

#### 3.3 Sumber Yang Sah (*Authenticity*)

Punca data dan maklumat hendaklah dari punca yang sah dan tanpa keraguan.

#### 3.4 Kesahihan (*Accountability*)

Data atau maklumat hendaklah dijamin ketepatan, kesahihannya dan tidak disangkal.

#### 3.5 Kebolehsediaan (*Availability*)

Data dan maklumat hendaklah boleh dicapai semasa diperlukan.

## **4.0 KESELAMATAN INTERNET**

Teknologi internet telah memudahkan perhubungan antara pengguna dan menyediakan capaian banyak maklumat dalam pelbagai bentuk dan format dengan menyediakan penyelidikan, analisis, rujukan dan bahan-bahan lain yang berfaedah. Penggunaan internet dengan cara yang tidak bertanggungjawab adalah dianggap sebagai tindakan yang boleh mengancam keselamatan, keutuhan dan kerahsiaan maklumat, melemahkan dan mengganggu sistem dan rangkaian di KKM.

### **4.1 TATACARA PENGGUNAAN INTERNET**

Internet merupakan satu kemudahan saluran global dan punca maklumat yang tidak dapat dikawal. Oleh sebab itu amatlah sukar untuk menentukan ketepatan sesuatu maklumat yang diperolehi dari internet. Justeru adalah menjadi tanggungjawab semua warga KKM untuk memainkan peranan dan bertindak secara bijak dalam menilai kesahihan dan ketepatan sesuatu maklumat yang diperolehi agar tugas dan kerja yang dilaksanakan tidak menyimpang dari tujuan sebenar KKM. Berikut adalah tatacara penggunaan internet yang mesti dipatuhi dan diikuti dalam menggunakan internet.

#### **4.1.1 Hak Terhadap Capaian Oleh Pengguna**

lanya boleh dilihat sebagai satu kemudahan yang disediakan oleh KKM untuk memudahkan dan melicinkan semua urusan rasmi yang melibatkan aset ICT. Semua pengguna harus maklum bahawa semua aset ICT termasuk maklumat yang diperolehi adalah aset kerajaan.

#### **4.1.2 Pemilihan Laman Yang Hendak Dilayar**

Pengguna hanya dibenarkan melayari laman yang berkaitan dengan urusan rasmi kerja dan laman yang mendapat kebenaran khas dari Ketua Jabatan.

#### **4.1.3 Pengesahan Maklumat**

Semua bahan dan sumber maklumat yang diperolehi dari internet hendaklah disahkan ketepatan dan kesahihan. Menyatakan sumber rujukan maklumat yang diperolehi dari internet amatlah digalakkan.

#### **4.1.4 Muat Naik Bahan**

Bahan rasmi yang hendak dimuat naik mestilah mendapat pengesahan dan kebenaran daripada Ketua Jabatan sebelum dimuat naik.

#### **4.1.5 Muat Turun Bahan**

Semua bahan yang hendak dimuat turun hendaklah dipastikan sah seperti perisian yang berdaftar dan di bawah Hak Cipta Terpelihara. Semua bahan yang dimuat turun dari internet hendaklah digunakan untuk tujuan yang dibenarkan sahaja.

#### **4.1.6 Perbincangan atau Forum Awam**

Hanya warga KKM yang mendapat kebenaran sahaja boleh menggunakan kemudahan ini. Namun begitu, semua maklumat dan kandungan bagi forum awam ini perlulah mendapat kebenaran rasmi dari Ketua Jabatan. Ini kerana semua maklumat yang hendak dikongsi akan melambangkan imej dan nama baik KKM.

## 4.2 LARANGAN DAN SALAH LAKU PENGGUNA INTERNET

Penggunaan kemudahan internet secara tidak beretika dan bertanggungjawab boleh mengancam keselamatan, keutuhan dan kerahsiaan sesuatu maklumat, melemahkan sistem ICT dan merosakkan imej KKM dan juga Perkhidmatan Awam. Sehubungan dengan itu, sekiranya berlaku penyalahgunaan terhadap kemudahan internet, tindakan boleh diambil terhadap mereka yang terlibat seperti yang telah ditetapkan di dalam Perintah Am, Bab D Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993. Pengguna internet adalah dilarang sama sekali melakukan perkara yang berikut:

- 4.2.1. melayari laman web yang tidak beretika seperti porno atau laman web yang tidak dibenarkan atau bahan-bahan yang mengandungi unsur-unsur lucah;
- 4.2.2. memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti permainan elektronik, video dan lagu;
- 4.2.3. memuat turun, menyimpan dan menggunakan perisian yang tidak tulen;
- 4.2.4. memuat turun, memuat naik dan menyimpan maklumat internet yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan individu atau kerajaan;
- 4.2.5. menyertai forum atau perbincangan awam atas talian (*online forum*) tanpa kebenaran daripada Ketua Jabatan;
- 4.2.6. bagi pengguna internet digalakkan untuk mengaktifkan *popup blocker tool* bagi setiap internet *browser* yang digunakan untuk mengelakkan paparan imej-imej yang

tidak dikehendaki. Sebagai contoh *Yahoo Toolbar* atau *Google Toolbar*;

- 4.2.7. memuat turun fail-fail yang bersaiz besar sehingga 10 MB. Bagi saiz fail melebihi 10 MB ianya hendaklah mendapatkan khidmat nasihat dari Pentadbir Emel terlebih dahulu;
- 4.2.8. pengguna yang menggunakan aplikasi web adalah bertanggungjawab sepenuhnya ke atas maklumat yang di *key-in*;
- 4.2.9. menceroboh atau percubaan untuk menggodam laman web KKM;
- 4.2.10. mendengar radio secara *online* kerana ia boleh mengganggu prestasi rangkaian KKM;
- 4.2.11. membuat capaian terus ke internet atau mana-mana rangkaian luar dengan menggunakan modem atau perkakasan lain di dalam persekitaran rangkaian KKM tanpa kebenaran dari Pentadbir Rangkaian (seperti Jalur lebar (*broadband*) atau *Dial Up Modem*);
- 4.2.12. menggunakan kemudahan internet untuk tujuan peribadi;
- 4.2.13. menjalankan aktiviti-aktiviti berunsur komersial dan politik;
- 4.2.14. menggunakan kemudahan *chatting* melalui internet (seperti *Yahoo Mesenger* atau *IRC*);
- 4.2.15. melakukan aktiviti jenayah seperti menyebarkan bahan yang membabitkan perjudian, senjata dan aktiviti pengganas;
- 4.2.16. mengubah apa-apa juga konfigurasi terhadap rangkaian bagi niat untuk mendapatkan akses terhadap internet tanpa kebenaran dari Ketua Jabatan;
- 4.2.17. menyedia, memuat naik, memuat turun, menyimpan dan menyebarkan material, teks ucapan, imej atau bahan-bahan yang mengandungi unsur-unsur ganas dan berbau



perkauman;

- 4.2.18. memuat naik, memuat turun, menyimpan dan menyebarkan gambar atau teks yang bercorak penentangan yang boleh membawa keadaan huru-hara dan menakutkan pengguna internet yang lain;
- 4.2.19. menggunakan *proxy* lain selain dari yang telah ditetapkan oleh Pentadbir Rangkaian; dan
- 4.2.20. membuat cubaan berulang-ulang terhadap laman web yang telah disekat.

## 5.0 KESELAMATAN MEL ELEKTRONIK (EMEL)

Emel merupakan satu cara perhubungan yang paling mudah di antara pengguna dengan pelbagai pihak yang lain. Kementerian ini memandang serius mengenai aspek keselamatan perhubungan melalui emel di antara pegawai-pegawai KKM, terutama perhubungan dengan pegawai KKM di luar negara dan melibatkan dokumen terperingkat. Emel yang diperuntukkan oleh fasiliti KKM sahaja boleh digunakan dan hanya untuk tujuan rasmi.

Garis panduan ini diwujudkan untuk menerangkan tatacara penggunaan emel, mengurangkan risiko gangguan terhadap operasi emel KKM dan meningkatkan tahap keselamatan komunikasi dokumen elektronik rasmi KKM.

### 5.1 TATACARA PENGGUNAAN EMEL

5.1.1 Terdapat dua kategori emel rasmi:

- i. Emel rahsia rasmi
  - Mengandungi maklumat atau perkara rahsia rasmi yang mesti diberi perlindungan untuk kepentingan keselamatan yang dikelaskan mengikut pengelasannya sama ada *Terhad*, *Sulit*, *Rahsia* atau *Rahsia Besar*.
- ii. Emel bukan rahsia rasmi
  - tidak mengandungi maklumat atau perkara rahsia rasmi.

5.1.2 Kaedah pengendalian dan penggunaan emel adalah seperti yang berikut:

**i. Pemilikan Akaun Emel**

Emel merupakan satu kemudahan yang disediakan oleh KKM dan tertakluk kepada peraturan. Ianya boleh ditarik balik jika penggunaannya melanggar peraturan. Penggunaan akaun milik individu lain atau berkongsi akaun adalah dilarang. Kemudahan emel ini juga bukan merupakan hak mutlak individu dan perlu ditarik balik sekiranya individu bertukar keluar, berhenti atau berpencen dari KKM.

**ii. Format Emel**

Penghantar emel hendaklah memastikan bahawa kandungan emel adalah bersesuaian dan berkaitan dengan perkara yang dibincangkan sebelum penghantaran dibuat.

Penggunaan huruf besar di dalam emel adalah tidak digalakkan dan dianggap tidak beretika. Gabungan huruf besar dan kecil boleh digunakan di tempat-tempat tertentu yang difikirkan bersesuaian di samping mengamalkan penggunaan bahasa yang betul, ringkas dan sopan.

Setiap emel rasmi hendaklah disertakan dengan tandatangan emel (*email signature*) yang mengandungi maklumat asas pengirim seperti nama penuh, jawatan, jabatan, bahagian, unit, alamat pejabat, nombor telefon, nombor faksimili dan alamat

emel. Maklumat ini adalah penting untuk dihubungi dan mencerminkan prestasi imej sistem emel KKM.

### **iii. Penghantaran Emel**

Akaun emel rasmi hendaklah digunakan bagi tujuan penghantaran emel rasmi dan pastikan dihantar ke alamat emel yang betul. Penggunaan 'salinan kepada' (cc) adalah dibenarkan sekiranya emel tersebut perlu dimaklumkan kepada penerima lain. Walaubagaimanapun, penggunaan 'blind cc' adalah tidak digalakkan.

Kemudahan balas (*reply*) digunakan untuk menjawab emel kepada penghantar asal dan panjangkan (*forward*) untuk memanjangkan emel atau dimajukan kepada penerima lain.

Setiap emel rasmi yang diterima hendaklah dijawab dengan cepat dan diambil tindakan dengan segera apabila emel berkenaan diterima.

Penggunaan kemudahan emel jawab automatik hendaklah diaktifkan bagi pengguna yang akan berada di luar pejabat dan dinyahaktifkan selepas kembali ke pejabat.

### **iv. Penghantaran Bersama Fail Kepilan**

Saiz fail kepilan (*attachment file*) termasuk kandungan emel yang dibenarkan untuk penghantaran adalah tidak melebihi 10 MB sahaja.

Ini adalah arahan selaras dengan surat yang dikeluarkan oleh MAMPU bertajuk "Langkah-Langkah

Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan” rujukan UPTM159/526/9 Jld.4 (60) yang bertarikh 23 November 2007 dan “Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan” rujukan UPTM159/526/9 Jld.4(59) bertarikh 1 Jun 2007 yang berkaitan.

**v. Mengenal Pasti Identiti Pengguna**

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

**vi. Saiz Storan Penyimpanan**

Pengguna webmail KKM diberi kemudahan storan sebanyak 100MB bagi menyimpan emel. Saiz storan bagi pengurusan tertinggi adalah tiada had (*unlimited*).

Pengguna adalah dinasihatkan supaya melakukan penyelenggaraan agar saiz storan untuk menyimpan emel tidak melebihi 85% daripada saiz storan yang diberikan. Penyelenggaraan boleh dilakukan dengan memadam atau menyalin mana-mana emel yang telah dibaca atau diambil tindakan dengan menggunakan perisian *mail client* . Ini bertujuan untuk menjamin prestasi server emel dan mempercepatkan pengguna membuat capaian emel.

**vii. Pemusnahan dan Penghapusan**

Emel yang tidak diperlukan dan tidak mempunyai nilai arkib yang telah diambil tindakan hendaklah dihapuskan. (Contoh: draf kertas kerja, draf minit dan kertas makluman).

**viii. Pemeriksaan oleh Pentadbir Emel KKM**

Pentadbir emel KKM berhak untuk memantau emel pengguna sekiranya perlu tanpa mendapatkan kebenaran dari pengguna.

**ix. Penggunaan Kata Laluan**

Pengguna hendaklah mengikut tatacara kata laluan yang telah ditetapkan seperti yang dinyatakan dalam perkara 9.0.

## **5.2 Larangan dan Salahlaku Pengguna Emel**

Semua pengguna emel adalah tertakluk kepada garis panduan dan peraturan yang telah ditetapkan oleh KKM mengenai penggunaan emel. Sekiranya berlaku penyalahgunaan akaun emel untuk tujuan tertentu, tindakan terhadap pengguna emel boleh diambil mengikut yang telah ditetapkan di dalam Perintah Am, Bab D Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993. Pengguna emel adalah dilarang sama sekali melakukan perkara yang berikut:

- a. menggunakan akaun emel milik orang lain, berkongsi akaun atau memberi akaun kepada orang lain;

- b. menggunakan identiti palsu atau menyamar sebagai penghantar maklumat yang sah;
- c. menggunakan emel untuk tujuan komersial atau politik.
- d. membuka emel dari penghantar yang tidak dikenali dikhuatiri mengandungi virus;
- e. membalas emel yang diterima daripada sumber yang tidak diketahui dan diragui;
- f. menyebarkan kod perosak seperti virus, *worm*, *Trojan Horse* dan *trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain;
- g. membuka emel yang mengandungi fail kepilan (*attachment file*) seperti \*.scr, \*.com, \*.exe, \*.dll, \*.pif, \*.vbs, \*.bat, \*.asd, \*.chm, \*.ocx, \*.hlp, \*.hta, \*.js, \*.shb, \*.shs, \*.vb, \*.vbe, \*.wsf, \*.wsh, \*.reg, \*.ini, \*.diz, \*.cpp, \*.cpl, \*.vxd, \*.sys dan \*.cmd yang berkemungkinan akan menyebarkan virus apabila dibuka;
- h. menghantar, memiliki dan menyimpan bahan-bahan yang salah di sisi undang-undang seperti bahan lucah, perjudian dan jenayah;
- i. menyebarkan perisian cetak rompak atau maklumat berbau politik, hasutan atau perkauman atau apa-apa maklumat yang menjejaskan reputasi KKM dan Perkhidmatan Awam melalui kemudahan emel KKM. Pihak KKM tidak akan bertanggungjawab ke atas sebarang kesalahan jenayah dan seumpamanya berkaitan emel;
- j. menghantar dan melibatkan diri dalam emel yang berunsur emel sampah (junk), emel bom, emel *spam*, emel berantai, fitnah, ciplak dan aktiviti-aktiviti lain yang ditegah oleh undang-undang Kerajaan Malaysia;
- k. menghantar semula emel yang gagal sampai ke destinasi sebelum menyiasat punca kejadian;

- l. membenarkan pihak ketiga untuk menjawab emel kepada penghantar asal bagi pihaknya; dan
- m. menyedia atau menghantar maklumat berulang-ulang yang berupa gangguan.

### 5.3 Tanggungjawab dan Peranan Pengguna Emel

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

- a. mencetak dan mendokumenkan semua emel yang penting untuk mengelakkan kehilangan maklumat penting apabila berlaku kerosakan kepada *hard disk* komputer;
- b. membuat salinan dan menyimpan fail kepilan ke satu *folder* berasingan dari setiap emel yang penting bagi tujuan salinan (*backup*);
- c. melakukan imbasan ke atas semua fail yang akan dihantar dan fail kepilan yang diterima bagi memastikan fail-fail tersebut bebas daripada serangan virus;
- e. memaklumkan kepada pentadbir emel sekiranya hendak bertukar keluar KKM, berhenti dan bersara dari KKM selewat-lewatnya tiga (3) hari sebelum tarikh akhir perkhidmatan;
- f. memaklumkan kepada Pentadbir Sistem ICT dengan segera sekiranya mengesyaki akaun telah disalahgunakan;
- h. bertanggungjawab sepenuhnya terhadap semua kandungan di dalam akaun emel sendiri;
- i. menggunakan kemudahan emel jawab automatik setiap kali berada di luar pejabat atau bercuti dan dinyahaktifkan



semula emel jawab automatik setelah kembali ke pejabat;  
dan

- j. menggunakan kemudahan *forwarding* bagi pegawai yang akan meninggalkan pejabat bagi memastikan tindakan ke atas emel dapat diambil dengan kadar segera.

#### **5.4 Tanggungjawab Pentadbir Emel**

Bagi memastikan pengendalian emel KKM beroperasi dengan lebih efisien dan berkesan, Pentadbir Emel adalah bertanggungjawab:

- 5.4.1 memastikan setiap akaun emel yang diwujudkan atau dibatalkan telah mendapat kelulusan dari Ketua Jabatan tempat bertugas pemohon menggunakan borang permohonan individu atau berkumpulan. (Contoh borang boleh dimuat turun dari Laman Web KKM-[www.moh.gov.my](http://www.moh.gov.my)). Pembatalan akaun (pengguna yang berhenti, bertukar dan yang melanggar dasar dan tatacara penggunaan emel KKM) perlulah dilakukan dengan segera bagi memastikan keselamatan maklumat;
- 5.4.2 menggunakan perisian pemecahan kata laluan yang dibenarkan untuk mengenal pasti kata laluan emel pengguna yang lemah dan kemudiannya mencadangkan dan memperakukan ciri-ciri kata laluan yang lebih baik kepada pengguna. Aktiviti ini perlu dibuat sekurang-kurangnya tiga (3) bulan sekali;
- 5.4.3 menjalankan pemantauan dan penapisan kandungan fail elektronik dan emel secara berkala jika difikirkan perlu tanpa terlebih dahulu merujuk kepada pengguna. Ini bertujuan

memastikan pelaksanaannya mematuhi dasar dan tatacara yang ditetapkan;

5.4.4 memastikan sistem emel beroperasi dengan baik dan boleh dicapai sepanjang masa (24 X 7 X 365);

5.4.5 bagi akaun emel yang didapati tidak aktif untuk tempoh selama 3 bulan, Pentadbir Emel berkuasa untuk menyahaktifkan sementara (*disable*) akaun emel tersebut tanpa notis. Jika tiada aduan diterima dalam tempoh sebulan, Pentadbir Emel berkuasa untuk menghapuskan (*delete*) akaun tersebut;

5.4.6 pengurusan akaun emel bagi individu yang akan bersara, bertukar keluar dari Kementerian atau yang dikenakan tindakan tatatertib.

lanya bertujuan untuk memastikan semua akaun emel tersebut diuruskan dengan lebih efektif dan efisien bagi memastikan tidak berlaku kehilangan dan kebocoran maklumat yang penting dari emel tersebut.

i. Pemakaian

Prosedur ini merangkumi semua pegawai dan kakitangan yang akan bertukar keluar KKM, berhenti dan berpencen seperti yang berikut:

- a. bertukar keluar dari KKM;
- b. bersara wajib atau pilihan;
- c. kemudahan penggunaan emel ditarik balik atas sebab tertentu;

- d. bercuti untuk meneruskan pengajian (tidak ditugaskan semula ke KKM);
- e. mengikuti program anjuran agensi kerajaan (tidak ditugaskan semula ke KKM); dan
- f. ditamatkan perkhidmatan

#### 5.4.7 tatacara pemberian ID akaun emel.

Pengwujudan ID bagi akaun emel hendaklah mengikut garis panduan seperti yang ditetapkan seperti yang berikut:

- i) ID bagi akaun emel pengguna hendaklah menggunakan nama sebenar. Penggunaan nama samaran atau gelaran tidak dibenarkan.

Contoh:

[kamal@moh.gov.my](mailto:kamal@moh.gov.my) = betul

[kamal\\_happy@moh.gov.my](mailto:kamal_happy@moh.gov.my) = salah

- ii) Bagi ID baru yang mempunyai persamaan dengan yang sedia ada. Maka penggunaan pangkal huruf bagi nama bapa hendaklah digunakan seperti berikut:

Rohani binti Abdulah = [rohani.a@moh.gov.my](mailto:rohani.a@moh.gov.my)

Wong Pei Yee = [pywong@moh.gov.my](mailto:pywong@moh.gov.my)

Subashini A/P Maniam = [msubashini@moh.gov.my](mailto:msubashini@moh.gov.my)

#### 5.4.8 memberi latihan tatacara pengendalian dan pengurusan emel kepada pegawai sekiranya perlu;

5.4.9 program kesedaran tatacara dan pembudayaan penggunaan emel juga perlu dilaksanakan secara berkala bagi menjamin keberkesanan sistem emel;

5.4.10 memantau kestabilan server (*server health*) 24 x 7 x 365 dengan menguji capaian kepada sistem emel secara berkala dengan menggunakan peralatan yang dikenal pasti sesuai;

Ujian penghantaran emel dari sistem emel luaran (seperti yahoomail, gmail, hotmail dan lain-lain) ke emel agensi hendaklah dilaksanakan secara berjadual untuk memastikan bahawa capaian sistem emel agensi berkenaan berada dalam keadaan yang baik. Pengujian ini hendaklah dijadikan salah satu perkara dalam senarai semak harian Pentadbir Sistem emel.

5.4.10 memastikan *Standard Operating Procedures (SOP)* disediakan berdasarkan kepada garis panduan yang disediakan oleh MAMPU;

5.4.11 membuat salinan pendua atau *backup* emel pada setiap hari;

5.4.12 memastikan *Business Continuity Plan (BCP)* dan *Risk Assessment* disediakan bagi sistem emel di KKM; dan

5.4.13 mengadakan sesi perbincangan dengan pembekal-pembekal utama sistem emel dari semasa ke semasa untuk mencari jalan terbaik bagi memperbaiki pengurusan dan pengoperasian sistem emel secara berterusan.

## **5.5 Kelayakan**

Kelayakan kemudahan emel ini diberikan kepada kakitangan KKM yang menjalankan urusan komunikasi dan perhubungan elektronik secara rasmi.

## 6.0 KAWALAN KESELAMATAN EMEL DAN INTERNET

Kemudahan emel dan internet yang terdapat di KKM adalah terdedah kepada ancaman seperti pencerobohan, penyelewangan, pemalsuan, pemintasan dan pembocoran rahsia. Kawalan keselamatan terhadap emel adalah penting bagi memastikan tiada berlaku kebocoran maklumat dan rahsia penting kerajaan.

### 6.1 Keselamatan Fizikal

Semua perkakasan yang mempunyai capaian terhadap emel dan internet KKM seperti komputer peribadi, komputer riba atau PDA hendaklah diletak atau disimpan di tempat yang mempunyai kawalan dari penceroboh atau sebarang bentuk capaian yang tidak sah.

### 6.2 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, kakitangan yang bertanggungjawab perlu memastikan semua maklumat bukan rahsia rasmi atau rahsia rasmi di dalam komputer berkenaan telah dikeluarkan dan selamat sebelum menghantar komputer untuk penyelenggaraan kepada pihak ketiga.

### **6.3 Tandatangan Digital**

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

### **6.4 Keselamatan Pengendalian Emel Rahsia Rasmi**

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

- i. penerima emel rahsia rasmi mesti mengesahkan kesahihan dokumen apabila ditandatangani secara digital oleh pengirim;
- ii. penerima mesti membuat akuan penerimaan emel rahsia rasmi sebaik sahaja menerimanya;
- iii. emel rahsia rasmi bertanda *Rahsia Besar* dan *Rahsia* tidak boleh dimajukan kepada pihak lain. Sementara emel bertanda *Sulit* dan *Terhad* yang hendak dimajukan kepada pihak lain memerlukan izin daripada pemula dokumen;
- iv. emel yang melibatkan maklumat rahsia rasmi yang hendak dimusnahkan perlulah ditulis ganti (*overwrite*) sekurang-kurangnya tiga (3) kali dengan fail yang lain sebelum dipadamkan; dan

- v. Kementerian perlu menentukan sistem emel rahsia rasmi yang disambungkan kepada internet atau intranet mesti mempunyai sistem keselamatan yang mencukupi seperti *Firewall*.



## 7.0 KESELAMATAN DARI ANCAMAN VIRUS

Serangan virus komputer merupakan masalah besar yang hadapi oleh KKM dan di lain-lain organisasi. Kepelbagaian jenis virus akan menyebabkan kerosakan peralatan komputer. Ianya juga menyebabkan kehilangan atau kerosakan maklumat penting dan boleh disebarkan kepada orang-orang berkenaan tanpa pengetahuan pengguna.

Walaupun bagaimanapun untuk meningkatkan lagi tahap keselamatan semua pengguna dikehendaki mengambil langkah-langkah berikut :

- i. pengguna mestilah sentiasa melakukan imbasan nyah virus (*virus scanning*) terhadap semua media yang dibawa dari luar seperti disket, *thumb drive*, *external hard disk* untuk pengesanan sama ada terdapat virus atau tidak. Dengan itu dapat mengawal keselamatan maklumat dan data dari dirosakkan oleh serangan virus;
- ii. pengguna dimestikan untuk menggunakan perisian anti-virus yang sah;
- iii. pengguna adalah dikehendaki melakukan imbasan nyah virus sekerap yang mungkin atau secara berkala terhadap komputer dan *notebook* yang digunakan bagi memastikan ia bebas dari virus;
- iv. sekiranya terdapat serangan atau jangkitan virus ke atas dokumen atau komputer, sila laporkan kepada pasukan Pentadbir Sistem di fasiliti masing-masing; dan
- v. pengguna PDA dan *notebook* hendaklah sentiasa memastikan kemudahan tanpa wayar (seperti *bluetooth*, *wifi*, *infrared*) dinyahaktifkan sekiranya tidak digunakan bagi mengurangkan insiden ancaman keselamatan.

## 8.0 PENGGUNAAN DAN PENGURUSAN RANGKAIAN

### 8.1 Infrastruktur Rangkaian

- a. Penggunaan rangkaian di KKM hanya dibenarkan untuk warga KKM sahaja. Pengguna luar yang hendak menggunakan kemudahan rangkaian KKM hendaklah mendapatkan kebenaran Pentadbir Rangkaian KKM.
- b. Fasiliti yang telah dirangkaikan melalui MOH\*Net tidak dibenarkan menggunakan rangkaian yang lain (seperti jalur lebar) kecuali mendapat kelulusan Bahagian Pengurusan Maklumat (BPM) dengan mematuhi syarat-syarat yang telah ditetapkan.
- c. Fasiliti KKM disarankan mengguna *firewall*, *Intrusion Prevention System (IPS)* dan *content filtering* bagi memastikan rangkaian KKM dilindungi dari sebarang ancaman keselamatan.
- d. Rangkaian setempat (LAN) di fasiliti hanya boleh diintegrasikan antara talian MOH\*Net dan egNet sahaja. Manakala talian lain tidak dibenarkan kecuali dengan mendapat kebenaran dari BPM.
- e. Setiap peralatan ICT yang dirangkaikan ke talian MOH\*Net tidak boleh disambungkan ke rangkaian lain pada masa yang sama seperti jalur lebar (*broadband*) dan sebagainya.
- f. Penggunaan tanpa wayar setempat (*wireless LAN*) di fasiliti disarankan dilengkapi dengan ciri-ciri keselamatan seperti menggunakan sekurang-kurangnya pengesahan *WPA2* pada peralatan *wireless* dan *radius server*.
- g. Sebarang permohonan berkaitan dengan perkhidmatan rangkaian seperti *ftp*, *natting*, *DNS*, *port* dan lain-lain perlu dikemukakan secara rasmi dengan mengisi Borang Permohonan Keperluan Rangkaian dan kemukakan kepada

Pentadbir Rangkaian BPM selewat-lewatnya tiga (3) hari sebelum perkhidmatan diperlukan.

- h. Sekiranya *DNS*, *nattng* dan *port* yang diperlukan tidak digunakan lagi, pihak Pentadbir Rangkaian BPM perlulah dimaklumkan bagi tujuan memperkemaskini.

## 8.2 Tanggungjawab Pentadbir Rangkaian

- a. Memastikan rangkaian MOH\*net sentiasa boleh digunakan.
- b. Menyelesaikan masalah rangkaian MOH\*net.
- c. Memastikan perlindungan keselamatan maklumat dalam rangkaian dan infrastruktur sokongan terurus dan terkawal.
- d. Mengenalpasti dan mengemaskini *rules firewall* yang telah ditetapkan sahaja.
- e. Pemantauan aktiviti capaian pengguna MOH\*net dari masa ke semasa.
- f. Mengemaskini dan menambahbaik reka bentuk infrastruktur MOH\*net mengikut polisi keselamatan yang telah ditetapkan.
- g. Mengenalpasti aktiviti-aktiviti yang tidak normal seperti penggunaan rangkaian yang tinggi dengan membuat capaian ke laman yang tidak dibenarkan. Oleh itu, tindakan menyekat capaian ke rangkaian dilakukan.
- h. Memantau laluan trafik rangkaian dari masa ke semasa dan mengambil tindakan yang sewajarnya dengan kadar segera jika berlaku kesesakan trafik rangkaian atau rangkaian tidak dapat berfungsi dengan baik.
- i. Mengawal IP pengguna serta mengambil tindakan terhadap pengguna sekiranya berlaku penyalahgunaan IP.
- j. Mengawal dan sentiasa mengemaskini DNS dari masa ke semasa.

- k. Menghalang capaian yang tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

### **8.3 Pengurusan Alamat Internet Protokol (IP)**

- a. Sebarang permohonan untuk menggunakan IP Statik hendaklah diperolehi daripada Pentadbir Rangkaian di fasiliti masing-masing.
- b. Pengguna adalah dilarang sama sekali untuk menukar IP di dalam peralatan ICT masing-masing tanpa kebenaran Pentadbir Rangkaian di fasiliti masing-masing.
- c. Sebarang pertukaran pengguna yang menggunakan IP statik hendaklah dimaklumkan kepada Pentadbir Rangkaian di fasiliti masing-masing.
- d. IP statik yang diberikan kepada pengguna tidak boleh digunakan untuk kepentingan sendiri. Sekiranya pengguna didapati menyalahgunakan IP statik yang diberi, Pentadbir Rangkaian yang bertanggungjawab di fasiliti masing-masing berhak mengeluarkan pengguna tersebut dari rangkaian.

### **8.4 Sambungan Rangkaian**

- a. Semua permohonan baru untuk mendapatkan sambungan rangkaian LAN mestilah melalui Pentadbir Rangkaian di fasiliti masing-masing.
- b. Pengguna tidak dibenarkan memutuskan/menyambung sambungan kabel fizikal UTP pada mana-mana *port* dalam rak peralatan rangkaian tanpa kebenaran dari pihak Pentadbir Rangkaian di fasiliti masing-masing.
- c. Pengguna tidak dibenarkan menukar maklumat yang terdapat pada UTP *port*.

- d. Perbuatan yang boleh merosakkan UTP *port*, kabel UTP atau rak rangkaian serta peralatannya adalah dilarang.
- e. Sebarang kerosakan pada kabel UTP, *network point* dan *network port* pada mana-mana *switch/hub* hendaklah dilaporkan kepada Pentadbir Rangkaian di fasiliti masing-masing.

#### **8.5 Dial-Up / Jalur Lebar (*Broadband*) / Rangkaian Tanpa Wayar (*wireless*)**

- a. Kemudahan *dial-up / broadband* hanya diberikan untuk tujuan rasmi.
- b. Permohonan perkhidmatan *mobile broadband* bagi tujuan rasmi di luar pejabat hendaklah mengemukakan permohonan kepada Bahagian Pengurusan Maklumat.
- c. Pengguna di fasiliti KKM yang menggunakan MOH\*net tidak dibenarkan menggunakan *broadband*
- d. Pengguna yang telah menggunakan kemudahan selain MOH\*net seperti *broadband/dial-up/wireless*, dikehendaki mengimbas keseluruhan komputer yang digunakan sebelum menyambung semula ke rangkaian KKM.

#### **8.6 File Transfer Protocol (FTP)**

Penggunaan FTP hendaklah dilaksanakan dengan ciri-ciri keselamatan yang disarankan seperti menggunakan aplikasi *putty* bagi sistem pengoperasian *Linux*, *sftp* bagi sistem pengoperasian *Windows*, *SSL*, *VPN* dan sebagainya yang bersesuaian.

## 9.0 KESELAMATAN KATA LALUAN

Kata laluan adalah merupakan kata kunci yang menjadi hak individu dan menjadi rahsia dari pengetahuan orang lain. Oleh itu pengguna adalah dinasihatkan menjaga kata laluan masing-masing dengan teliti agar tidak dicerobohi oleh pengguna lain.

Bagi menjamin keselamatan kata laluan pengguna perlulah mematuhi prosedur berikut :

- a. rahsiakan kata laluan. Kata laluan hendaklah dihafal dan jangan sekali-kali disalin atau di papar di mana-mana media seperti buku catatan, disket, CD dan sebagainya kerana dikhuatiri akan diketahui dan disalahgunakan oleh orang lain;
- b. gunakan kata laluan yang kukuh melalui gabungan nombor, huruf, tanda dan simbol yang mempunyai sekurang-kurangnya lapan (8) aksara (contoh: P6swO~d!). (AMARAN: Jangan guna kata laluan ini kerana ianya telah diketahui umum);
- c. kata laluan perlu ditukar dalam tempoh 90 hari;
- d. elakkan dari menggunakan semula empat (4) kata laluan yang terdahulu;
- e. ID pengguna tidak boleh digunakan sebagai kata laluan;
- f. elakkan menggunakan kata laluan yang mengandungi maklumat yang berkaitan dengan pengguna, peralatan dan perisian yang diguna pakai;
- g. menukar serta merta kata laluan asal (*default password*) yang diterima daripada Pentadbir Sistem; dan
- h. sekiranya kata laluan telah dicerobohi atau disyaki dicerobohi, kakitangan KKM hendaklah melaporkan kepada CERT KKM dengan serta merta.

## 10.0 KESELAMATAN RANGKAIAN (*Network Security*)

10.1 Keselamatan rangkaian adalah merupakan satu langkah keselamatan utama untuk mengawal aset ICT daripada ancaman keselamatan seperti dicerobohi oleh pihak yang tidak bertanggungjawab. Untuk menjamin keselamatan rangkaian di KKM, pihak BPM sentiasa menghasilkan dan mengemaskinikan infrastruktur reka bentuk rangkaian dengan baik dan teratur.

Pentadbir Rangkaian di setiap fasiliti KKM perlu menyedia dan mengemaskini reka bentuk rangkaian untuk tujuan merancang, memantau dan menyenggara rangkaian.

10.2 Pemantauan dilakukan dari semasa ke semasa untuk memastikan keselamatan peralatan rangkaian seperti server KKM di dalam *DMZ zone*, *Secured Zone* dan lain-lain sentiasa berada di dalam keadaan baik.

Pengguna perlu mematuhi perkara 4.2 dan perkara 5.2. Tindakan disiplin akan diambil sekiranya ada penyalahgunaan kemudahan ICT seperti memuat turun perisian tanpa kebenaran kerana ini akan menjejaskan prestasi rangkaian (*network performance*) dan pendedahan rangkaian kepada ancaman keselamatan seperti virus.

10.3 *Rules firewall* hendaklah disediakan dan sentiasa dikemaskini di semua fasiliti KKM bagi tujuan mengawal capaian ke atas sistem yang telah dibangunkan dan memastikan keselamatan aset-aset ICT di dalam rangkaian KKM daripada ancaman keselamatan oleh pihak yang tidak bertanggungjawab.

- 10.4 Pentadbir Sistem bertanggungjawab memantau laporan log di setiap server untuk memastikan tiada capaian yang tidak sah dibuat ke atas server berkenaan.
- 10.5 Pengguna hendaklah menggunakan teknologi VPN bagi memastikan keselamatan maksimum semua maklumat yang dihantar dan diterima melalui transaksi atas talian jika ingin membuat capaian rangkaian antara fasiliti KKM dengan Ibu Pejabat KKM yang berpusat di Putrajaya.
- 10.6 *Proxy* atau *webcache server* dan *viruswall server* perlu diwujudkan bagi mengawal serta memantau penggunaan internet dari rangkaian KKM. Ia berfungsi mengawal pengguna membuat capaian laman web serta muat turun fail yang tidak dibenarkan seperti gambar lucah, *screen saver*, lagu, video dan sebagainya.



## 11.0 KESELAMATAN FIZIKAL PERKAKASAN ICT KKM

Keselamatan fizikal perkakasan ICT KKM merangkumi semua perkakasan ICT yang berada di KKM seperti komputer (*personel computer*), *notebook* dan perkakasan terlibat seperti cakera keras (*hard disk*), pencetak, pengimbas dan lain-lain. Semua pengguna perkakasan ICT KKM adalah bertanggungjawab terhadap perkakasan ICT yang diberikan. (Rujuk Dasar Keselamatan ICT KKM). Sebagai satu langkah bagi memastikan keselamatan perkakasan ICT KKM berada di dalam tahap maksima, pengguna hendaklah sentiasa mematuhi garis panduan berikut:

- a. setiap komputer, PDA atau *notebook* mestilah mempunyai kata laluan yang kukuh;
- b. setiap komputer, *notebook* dan server mestilah dilakukan pengemaskinian patches dan services pack *Microsoft Windows / Open Source* yang terkini;
- c. setiap server, komputer dan *notebook* hendaklah menggunakan perisian yang sah seperti antivirus, sistem pengoperasian dan lain-lain;
- d. setiap server, komputer dan *notebook* hendaklah mempunyai nama komputer dan dilarang mengubah atau meminda nama komputer dan konfigurasi dalam komputer yang disediakan tanpa kebenaran;
- e. setiap perolehan perkakasan ICT hendaklah yang tulen serta dari pengedar yang sah dan berdaftar (bukan klon);
- f. pastikan perkakasan ICT pejabat tidak digunakan oleh orang yang tidak berkenaan dan hanya untuk urusan rasmi sahaja;
- g. dilarang menggunakan alat penyambung kuasa elektrik bagi berbagai peralatan. Bekalan kuasa elektrik yang tidak stabil akan merosakkan komputer. Gunakan kemudahan *Uninterruptable Power Supply (UPS)* atau *Automatic Voltage Regulator (AVR)*

untuk memastikan bekalan elektrik sentiasa dibekalkan mengikut spesifikasi keperluan komputer/*notebook*;

- h. pastikan komputer atau *notebook* tidak terdedah secara terus kepada pancaran matahari/haba dan elakkan komputer daripada kawasan tarikan kuasa magnet serta kuasa voltan yang tinggi;
- i. pastikan bekalan punca elektrik ditutup semasa penyambungan peralatan komputer dan aksesoriya atau setelah selesai penggunaannya;
- j. pastikan komputer atau *notebook* diletakkan di tempat dingin dan kering persekitarannya serta di tempat yang selamat;
- k. konfigurasi komputer atau *notebook* kepada sleeping mode jika digunakan secara berterusan;
- l. tamatkan aplikasi tanpa tindakbalas (*not responding*) dengan kekunci Ctrl-Alt-Del jika komputer gagal berfungsi dengan baik seperti *hang*;
- m. pastikan komputer atau *notebook* mempunyai sistem masa dan tarikh yang betul untuk tujuan audit dan penghantaran emel;
- n. sentiasa keluar daripada tettingkap (*windows*) atau mematikan komputer dengan cara yang betul bagi mencegah ralat sistem. Tidak dibenarkan mematikan komputer secara fizikal iaitu dengan menutup suis atau mencabut plug dengan begitu sahaja;
- o. dilarang menghentak/mengetuk dengan apa cara sekalipun sama ada sengaja atau tidak sengaja ke atas komputer, *notebook* atau sebarang perkakasan ICT;
- p. sentiasa mempunyai salinan pendua (*backup*) bagi data-data penting yang terdapat di dalam komputer;
- q. pengguna adalah dilarang membaiki sebarang kerosakan terhadap perkakasan ICT tanpa kebenaran bagi mengelakkan kehilangan terus maklumat yang tersimpan di dalamnya;

- r. pengguna tidak dibenarkan menggunakan ID *Administrator* kecuali mendapat kebenaran dan tidak dibenarkan membuang instalasi (*uninstall*) mana-mana perisian yang telah dipasang; dan
- s. apabila pengguna tidak menggunakan komputer atau *notebook* buat sementara waktu, maka *lock computer* hendaklah dilakukan.

## 12.0 TATACARA PENGURUSAN MEDIA STORAN

Pengurusan media storan adalah garis panduan bagi menguruskan media storan yang mengadungi maklumat sulit dan rahsia rasmi kerajaan. Media storan merangkumi perkakasan seperti *cd*, *tape*, *thumb drive*, *memory card*, *external hard disk* dan lain-lain perkakasan yang boleh digunakan untuk menyimpan maklumat elektronik. Bagi menjamin keselamatan maklumat yang disimpan di dalam media storan, pengguna adalah dinasihatkan mengikut garis panduan yang berikut:

- a. pengguna hendaklah memastikan media storan yang dibekalkan hanya untuk kegunaan urusan rasmi KKM;
- b. setiap media perlulah dilabelkan mengikut Bahagian/Unit>Nama;
- c. media yang mengandungi maklumat atau rahsia rasmi mestilah disimpan dengan selamat dan dilabelkan mengikut pengelasannya sama ada Terhad , Sulit atau Rahsia;
- d. pengguna adalah dilarang menyalin, membawa keluar atau memberi media yang mengandungi maklumat rahsia rasmi kepada orang lain. Ini adalah untuk mengelak dari berlakunya pembocoran rahsia;
- e. pengguna disarankan untuk melakukan kaedah pemampatan (*compress*) untuk mengurangkan saiz fail bagi memaksimumkan penggunaan media storan;
- f. media yang mengandungi maklumat yang tidak diperlukan lagi, perlulah dipadamkan (*delete*) sebelum digunakan untuk tujuan yang lain;
- g. pengguna hendaklah memastikan keselamatan fizikal terhadap media dari ancaman seperti sinaran matahari, suhu panas, elektrostatik dan magnet serta disimpan di tempat yang selamat. Ini dapat mengelakkan maklumat atau data menjadi rosak (*corrupted*) atau tidak boleh dibaca;

- h. semua media storan yang rosak atau tidak boleh digunakan lagi, perlulah di format semula untuk memadamkan kesemua data di dalamnya sebelum dilupuskan dan dimusnahkan;
- i. setiap media storan mestilah sentiasa diimbis sebelum digunakan;
- j. pengguna tidak digalakkan untuk berkongsi penggunaan media storan bagi mengelakkan maklumat yang disimpan di dalam media storan diakses oleh pengguna yang tidak berhak; dan
- k. sebarang kehilangan dan ancaman terhadap maklumat yang terkandung di dalam media atau kehilangan media hendaklah dilaporkan kepada CERT KKM.

### 13.0 KESELAMATAN PERKAKASAN ICT DI PUSAT DATA/BILIK SERVER KKM

Bagi memastikan semua server yang ditempatkan di Pusat Data KKM berada di dalam keadaan yang selamat dan capaian terhadap server tersebut tidak diganggu, Pusat Data di fasiliti masing-masing hendaklah mempunyai kemudahan sistem pengurusan keselamatan, penyaman udara khas dan sistem perlindungan suhu dan alat pencegah kebakaran. Pusat Data juga hendaklah dilengkapi dengan UPS bagi memastikan semua server dapat beroperasi sekiranya berlaku gangguan bekalan elektrik sebelum diambil alih sepenuhnya oleh Genset.

Semua maklumat penting KKM merupakan aset yang perlu dilindungi sebaik mungkin bagi menjamin keselamatannya. Beberapa langkah perlu dilaksanakan bagi melindungi server tersebut seperti:

- a. setiap Pusat Data/Bilik Server hendaklah disediakan dengan sistem *Security Access Door* atau sentiasa berkunci bagi memantau dan mengawal pengguna yang keluar masuk ke bilik server;
- b. hanya pengguna yang dibenarkan sahaja boleh memasuki bilik server;
- c. setiap server mestilah dilabelkan bagi memudahkan setiap pentadbir menjalankan tugas masing-masing;
- d. pastikan bilik server sentiasa bersih, kemas, tidak menempatkan perkakasan yang tidak diperlukan dan server tidak terdedah kepada habuk;
- e. pastikan pengkabelan disusun dengan kemas dan teratur serta dilabelkan dengan betul;
- f. penghawa dingin mestilah berfungsi dengan baik di mana suhunya di dalam lingkungan  $\pm 19.5^{\circ}\text{C}$  dan kelembapan di paras 50.7%;

- g. semua peralatan keselamatan, UPS penghawa dingin mestilah diselenggarakan secara berkala;
- h. diagram kedudukan server hendaklah disediakan dan dipamerkan di dalam Pusat Data/Bilik Server KKM; dan
- i. semua pegerakan keluar dan masuk perkakasan di Pusat Data perlu direkodkan dan mendapat kebenaran dengan menggunakan borang permohonan yang disediakan.

## 14.0 KESELAMATAN PERISIAN SISTEM DAN PANGKALAN DATA

Data dan maklumat sistem aplikasi KKM yang telah dibangunkan dan beroperasi merupakan aset yang penting dan perlu dilindungi sebaik mungkin bagi menjamin keselamatannya. Beberapa langkah telah dikenal pasti dan dilaksanakan bagi melindungi aset-aset tersebut. Antaranya adalah:

### 14.1 Pembaik Pulih Sistem

Pembaik pulih sistem adalah merupakan proses baik pulih akibat dari kemusnahan atau kehilangan data yang berlaku disebabkan beberapa faktor. Antaranya adalah seperti yang berikut:

- a. kegagalan server berfungsi;
- b. kerosakan fizikal *hard disk*; dan
- c. masalah kesilapan dalam pemrograman.

Proses pembaik pulih sistem terbahagi kepada dua peringkat iaitu prosedur salinan pendua (*backup*) dan prosedur baik pulih (*restore*).

#### 14.1.1 Prosedur Salinan Pendua (*Backup*)

- a. *Backup* keseluruhan semua data dan aplikasi termasuk *Operating System* (OS) hendaklah dibuat sekurang-kurangnya pada setiap minggu untuk semua server berpandukan prosedur-prosedur *backup* yang telah ditetapkan. Namun *backup* keseluruhan secara bulanan wajib dilakukan.

Walaupun bagaimanapun, kekerapan penjanaan data *backup* adalah mengikut kepentingan data-data



tersebut secara berperingkat dari harian hinggalah bulanan.

- b. *Backup* atau salinan data ke dalam media storan perlu dilakukan setiap hari bagi sebarang perubahan atau *incremental* data untuk mengelakkan kehilangan data sekiranya berlaku kerosakan *hard disk*.
- c. Semua *backup* yang dilakukan hendaklah direkod, dilabel secara unik dan disimpan di tempat yang selamat. Ini adalah untuk memudahkan carian fail dari semasa ke semasa.
- d. *Backup* sistem aplikasi dan sistem operasi perlu diadakan sekurang-kurangnya sekali bagi setiap keluaran versi terbaru dari semasa ke semasa mengikut peraturan yang ditetapkan semasa perisian itu dibangunkan atau diperoleh atau mengikut garis panduan yang dikeluarkan dari semasa ke semasa. Faktor ketahanan dan jangka hayat media storan perlu diambil kira dalam menentukan kekerapan *backup*.
- e. *Backup* untuk data dan sistem aplikasi/sistem operasi dicadangkan dibuat dalam dua (2) salinan dan setiap satu disimpan di lokasi yang berlainan. Lokasi-lokasi tersebut adalah :-
  - i) Lokasi *on-site* - di mana sistem tersebut beroperasi.
  - ii) Lokasi *off-site* - di bangunan lain yang berdekatan atau mana-mana Jabatan Kerajaan

lain yang berdekatan dan mempunyai kemudahan keselamatan untuk menyimpan media *backup*.

- f. Penetapan lokasi simpanan *backup* ini adalah untuk memastikan data-data kritikal/penting masih boleh diselamatkan jika berlaku kerosakan atau kemusnahan secara fizikal, sebagai contoh jika berlaku bencana seperti kebakaran, banjir dan sebagainya.
- g. Setiap media *backup* yang dilakukan hendaklah diuji (*on-site dan off-site*) sekurang-kurangnya sekali setahun. Ini adalah bagi memastikan media backup tersebut berfungsi dengan baik (*readable and usable*) untuk tujuan baik pulih.
- h. *Standard Operating Procedure* (SOP) bagi setiap perkhidmatan ICT seperti aplikasi, rangkaian dan lain-lain hendaklah disediakan bagi memastikan kesinambungan perkhidmatan. Pengujian SOP hendaklah dilaksanakan sekurang-kurangnya setahun sekali.

#### **14.1.2 Prosedur Baik pulih (*Restore*)**

Dengan prosedur *backup* di atas, proses pembaik pulih boleh dilakukan sama ada dari peringkat paling kritikal seperti kegagalan seluruh *partition hard disk* atau pangkalan data, aplikasi, direktori sehingga ke atas fail tertentu dapat di baik pulih dengan mudah dan selamat.

## 14.2 Pelan Pemulihan Bencana (*Disaster Recovery Plan*)

Data-data kritikal disalin (*backup* di para 14.1.1) ke dalam media storan dan disimpan di bilik server. Di samping itu salinan pendua bagi data-data tersebut perlu dihantar dan disimpan di lokasi *off-site* sebagai salah satu pelan pemulihan bencana. Kaedah ini dilakukan bagi memastikan data-data kritikal masih boleh diselamatkan jika berlaku kerosakan atau kemusnahan secara fizikal di bilik server, sebagai contoh jika berlaku bencana seperti kebakaran, banjir dan sebagainya.

## 15.0 PEMBANGUNAN SISTEM APLIKASI

- a. Memastikan vendor yang dilantik mengetahui dan menggunakan tentang “*Secured Coding*” jika perlu.
- b. Mengubah konfigurasi asal (*default*) termasuk katalaluan, *port* dan sebagainya.
- c. Memastikan vendor menyediakan dan menyerahkan *Standard of Procedure (SOP)* bagi setiap aplikasi yang dibangunkan.
- d. Menutup *directory listing* setiap aplikasi kepada umum bagi mengelak data mudah dijejaki oleh pihak yang tidak bertanggungjawab.
- e. Memastikan vendor menyerahkan semua katalaluan berkaitan aplikasi seperti katalaluan pangkalan data dan server.
- f. Tidak menggunakan *IP address* sebagai URL bagi membuat capaian dan menutup *IP address* dari diketahui oleh umum.
- g. Menutup akses *anonymous*.
- h. Memastikan *port* yang diperlukan adalah untuk kegunaan aplikasi tersebut sahaja berfungsi. Penggunaan *port* seperti *port 445* hendaklah dielakkan dari diguna kerana ianya merupakan *file sharing* dan mudah menyebarkan virus.
- i. Setiap aplikasi perlu direka dengan fungsi menguatkuasakan tamat masa sesi yang terbiar (*idle timeout*), iaitu apabila tiada aktiviti pengguna untuk tempoh masa yang tertentu, sesi akan ditamatkan. Pengguna perlu log masuk semula selepas penamatan *idle timeout* tersebut. Saranan bagi tempoh tamat masa adalah 15 minit.
- j. Pengujian secara terperinci hendaklah dilakukan ke atas aplikasi atas talian terutamanya semasa input data bagi mengatasi masalah *web defacement* dan sebagainya.
- k. Setiap sistem aplikasi mestilah disediakan dengan *log file* dan *audit trail*.
- l. Setiap aplikasi sistem yang dibangunkan sentiasa mengemaskini *security patches* dan menggunakan versi terkini

seperti penggunaan *Content Management System (CMS)* iaitu *Joomla*;

- m. Memastikan sistem pangkalan data dan perisian pembangunan aplikasi hendaklah menggunakan *features* terkini.
- n. Memastikan dokumentasi sistem aplikasi disediakan dan dikemaskini dari masa ke semasa.
- o. Sebarang perubahan kepada ahli pasukan sistem aplikasi hendaklah dimaklumkan.

## **16.0 PERANAN DAN TANGGUNGJAWAB SEMUA FASILITI KKM**

Semua fasiliti KKM memainkan peranan yang penting bagi memastikan penggunaan dan keselamatan ICT KKM berada dalam tahap yang paling maksimum sepanjang masa.

## **17.0 KHIDMAT NASIHAT**

Sebarang pertanyaan dan kemusykilan berkaitan dengan garis panduan ini bolehlah dirujuk kepada Bahagian Pengurusan Maklumat. Permohonan untuk keterangan lanjut mengenai kandungan dokumen ini bolehlah diajukan kepada:

Bahagian Pengurusan Maklumat,  
Kementerian Kesihatan Malaysia,  
Aras 5, Blok E7, Parcel E,  
Pejabat Pentadbiran Kerajaan Persekutuan,  
62590 W.P. Putrajaya.

## **18.0 PENUTUP**

Garis panduan ini merupakan amalan-amalan terbaik dalam pengendalian keselamatan ICT dan mesti dipatuhi oleh semua pengguna di KKM. Garis panduan ini akan dikemaskini dari masa ke semasa selaras dengan arus perkembangan teknologi maklumat dan komunikasi serta perundangan.