TATACARA PENGGUNAAN DAN KESELAMATAN RANGKAIAN ICT KEMENTERIAN KESIHATAN MALAYSIA

1. PENGENALAN

Peningkatan penggunaan kemudahan teknologi maklumat dan komunikasi (ICT) dalam tugasan seharian terutama yang melibatkan Internet dan e-mel telah mendedahkan maklumat penting kepada pihak luar. Untuk memastikan maklumat-maklumat penting di Kementerian Kesihatan Malaysia (KKM) bebas daripada ancaman yang boleh merosakkan aset ICT KKM, semua pengguna perlu mematuhi dokumen Tatacara Penggunaan dan Keselamatan Rangkaian ICT di KKM seperti yang telah ditetapkan. Dokumen yang dikeluarkan oleh Bahagian Teknologi Maklumat Dan Komunikasi (BTMK) ini telah diperakukan oleh Mesyuarat Jawatankuasa Pemandu Bil. 3 Tahun 2005 pada 25 Oktober 2005 untuk diguna pakai ke seluruh KKM. 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. OBJEKTIF

Tujuan utama Tatacara Penggunaan dan Keselamatan Rangkaian ICT di KKM adalah sebagai panduan untuk pengguna demi menjamin kesinambungan urusan kerajaan dan menghindar kesan insiden keselamatan. Dalam era ICT masa kini keselamatan maklumat adalah menjadi perkara utama untuk mengelakkan daripada disalahgunakan oleh orang-orang yang tidak bertanggung jawab. 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 maruah organisasi dan negara. Justeru, Tatacara Penggunaan dan Keselamatan Rangkaian ICT di KKM perlu diwujudkan supaya dapat dijadikan panduan

kepada pengguna dengan tujuan menjamin kerahsiaan, integriti, sumber yang sah, kesahihan dan kebolehsediaan maklumat yang berterusan.

3. 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, penggodam atau diubah semasa penghantaran atau penerimaan. Tatacara ini melindungi keselamatan maklumat sesuatu organisasi dalam beberapa aspek seperti berikut :

(a) **Kerahsiaan (*Confidentiality*)**

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

(b) **Integriti (*Integrity*)**

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

(c) **Sumber Yang Sah (*Authenticity*)**

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

(d) **Kesahihan (*Accountability*)**

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

(e) **Kebolehsediaan (*Availability*)**

Data dan maklumat hendaklah boleh dicapai semasa diperlukan.

4. 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. Untuk menjamin keselamatan ICT KKM pengguna internet mestilah mematuhi prosedur dan garis panduan berikut :

(a) Tidak dibenarkan melawati laman web yang tidak beretika seperti porno atau laman web yang tidak dibenarkan atau bahan-bahan yang mengandungi unsur-unsur lucah.

(b) Dilarang memuat turun, menyimpan dan menggunakan perisian berbentuk hiburan atas talian seperti permainan elektronik, video dan lagu.

(c) Tidak memuat turun, menyimpan dan menggunakan perisian yang tidak berlesen.

(d) Dilarang memuat turun, memuat naik dan menyimpan maklumat internet yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan individu atau kerajaan.

(e) Forum atau perbincangan awam atas talian (*online forum*) mestilah mendapat kebenaran daripada Ketua Jabatan. Menggunakan kemudahan *chatting* melalui Internet adalah dilarang sama sekali.

(f) 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.

(g) Dilarang memuat turun fail-fail yang saiz besar yang melebihi 2 MB. Jika ia benar-benar diperlukan hendaklah mendapatkan khidmat nasihat dari pegawai pentadbir keselamatan dan rangkaian terlebih dahulu.

(h) Pengguna yang menggunakan aplikasi web adalah bertanggungjawab sepenuhnya ke atas maklumat yang dikunci masuk.

(i) Pencerobohan atau percubaan untuk menggodam laman web KKM adalah dilarang.

(j) Pengguna adalah dilarang untuk mendengar radio secara online kerana ia boleh mengganggu prestasi rangkaian KKM.

5. KESELAMATAN MEL ELEKTRONIK (E-MEL)

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

5.1 Prosedur Yang Harus Dipatuhi

Bagi memastikan penggunaan e-mel dapat beroperasi dengan sempurna dan berkesan, pengguna adalah dinasihatkan untuk mematuhi prosedur berikut :

(a) Dilarang menggunakan akaun e-mel milik orang lain, berkongsi e-mel atau memberi kepada orang lain.

(b) Pengguna tidak dibenarkan dengan sewenangnya memberikan e-mel KKM kepada orang lain kerana kemungkinan ianya akan menggalakkan penyebaran virus, e-mel *spamming*, dan *junk-mail* seperti iklan perniagaan.

(c) Jangan membuka e-mel dari penghantar yang tidak dikenali berkemungkinan mengandungi virus.

(d) Dilarang menyebarkan kod perosak seperti virus, *worm, Trojan Horse* dan *trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain.

(e) Pengguna tidak dibenarkan menggunakan e-mel untuk tujuan komersial, politik, perjudian, jenayah dan sebagainya.

(f) Dilarang membuka e-mel 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 . Ia berkemungkinan akan menyebarkan virus apabila dibuka.

(g) Menyebar perisian cetak rompak atau maklumat berbau politik, hasutan atau perkauman atau apa-apa maklumat yang menjejaskan reputasi KKM dan Perkhidmatan Awam melalui kemudahan e-mel KKM adalah dilarang. Pihak KKM tidak akan bertanggungjawab ke atas sebarang kesalahan jenayah dan seumpamanya berkaitan e-mel.

(h) Pihak Pentadbir Sistem boleh memantau semua e-mel KKM jika perlu tanpa mendapat kebenaran pengguna.

5.2 Tanggungjawab Pengguna

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 :

(a) Pengguna adalah digalakkan menggunakan webmail KKM jika ingin membuat capaian e-mel umpamanya ketika bertugas di luar KKM. Sila lawati laman web KKM di http://www.moh.gov.my.

(b) Saiz fail kepilan (attachment file) termasuk kandungan e-mel yang dibenarkan untuk penghantaran adalah tidak melebihi 1.0 MB sahaja. Saiz fail yang besar akan mengganggu prestasi e-mel server dan sistem rangkaian KKM.

(c) Pengguna webmail KKM adalah dinasihatkan supaya kerap melakukan penyelenggaraan agar saiz storan untuk menyimpan e-mel tidak melebihi 5.0MB. Penyelenggaraan boleh dilakukan dengan memadam atau menyalin mana-mana e-mel yang telah dibaca atau diambil tindakan. Ini bertujuan untuk menjamin prestasi server e-mel.

(d) Pengguna e-mel perisian *outlook* (Microsoft Outlook /Outlook Express) hendaklah sentiasa menyelenggarakan e-mel terutama *folder INBOX* tidak melebihi 5.0 MB dengan ini akan mempercepatkan capaian perisian e-mel *outlook* dan prestasi komputer pengguna. Ini boleh dilakukan sama ada dengan memadam (delete), menyalin (archive) atau mencetak mana-mana e-mel yang telah dibaca atau diambil tindakan.

(e) Pengguna juga digalakkan untuk mencetak dan mendokumenkan semua e-mel yang penting untuk

mengelakkan kehilangan maklumat penting apabila berlaku kerosakan kepada *hard disk* komputer.

(f) Pengguna hendaklah membuat salinan dan menyimpan fail kepilan ke satu *folder* berasingan dari setiap e-mel yang penting bagi tujuan *backup* jika berlaku masalah kepada *hard disk* komputer. Pengguna juga tidak digalakkan meninggalkan e-mel di dalam server selepas dibaca.

(g) Lakukan imbasan ke atas semua fail dan fail kepilan bagi mengenal pasti fail-fail yang diserang virus dengan perisian antivirus *Officescan*.

(h) Memastikan kemudahan e-mel digunakan dan dibiarkan aktif pada keseluruhan waktu bekerja supaya e-mel yang di alamatkan sampai tepat pada masanya dan tindakan ke atasnya dapat disegerakan.

(i) Untuk keselamatan dokumen rahsia rasmi dan maklumat terperingkat yang dihantar melalui e-mel, adalah perlu untuk mendaftarkan Sijil Digital (Digital Certificate) kepada pengguna termasuk pegawai di Pejabat Luar Negara.

(j) Kementerian tidak akan bertanggung jawab ke atas e-mel yanghilang bagi pengguna yang tidak mematuhi polisi penggunaan e-mel.

(k) Nama pegawai dan kakitangan KKM yang bertukar atau berhenti hendaklah dimaklumkan kepada BTMK agar akaun e-mel mereka dapat dikemaskinikan dengan segera.

6. 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 seperti *hard disk* dan menyebabkan maklumat, kehilangan atau kerosakan maklumat penting dan mungkin juga disebar kepada orang-orang berkenaan tanpa pengetahuan pengguna.

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

(a) Pengguna PC mestilah sentiasa melakukan nyah virus (virus scanning) disket atau CD yang di bawa dari luar untuk pengesahan sama ada terdapat virus atau tidak. Dengan itu kementerian dapat mengawal keselamatan maklumat dan data dari dirosakkan oleh serangan virus.

(b) Pengguna adalah dinasihatkan untuk menggunakan perisian anti-virus yang sah.

(c) Pengguna adalah dikehendaki melakukan nyah virus sekerap yang mungkin komputer dan notebook yang digunakan. Ini bertujuan memberitahu pengguna sama ada komputer yang digunakan adalah benar-benar bebas dari virus.

(d) Sekiranya terdapat serangan atau jangkitan virus ke atas dokumen atau komputer, sila berhubung dengan Bahagian Teknologi Maklumat Dan Komunikasi.

7. PENGGUNAAN DAN PENGURUSAN RANGKAIAN

7.1 Infrastruktur Rangkaian

Hanya pengguna KKM sahaja yang dibenarkan mengguna rangkaian KKM.

Pengguna luar yang hendak menggunakan kemudahan rangkaian KKM hendaklah mendapatkan kebenaran BTMK.

7.2 Pengurusan Alamat IP

(a) Sebarang permohonan untuk menggunakan *static* IP hendaklah melalui BTMK dengan mengisi borang yang disediakan.

(b) Pengguna adalah dilarang sama sekali untuk menukar atau meletakkan IP di dalam komputer masing-masing tanpa kebenaran.

(c) Sebarang pertukaran pengguna yang menggunakan *static* IP hendaklah dimaklumkan kepada pihak BTMK.

(d) *Static* IP yang diberikan kepada pengguna tidak boleh digunakan untuk kepentingan sendiri. Sekiranya pengguna didapati menyalahgunakan *static* IP dengan menukar konfigurasi PC kepada server tanpa memaklumkan kepada BTMK, PC pengguna berkenaan akan dikeluarkan dari rangkaian.

7.3 Sambungan Rangkaian

(a) Semua permohonan baru untuk mendapatkan sambungan rangkaian mestilah melalui BTMK.

(b) Pengguna tidak dibenarkan memutuskan/menyambung sambungan kabel UTP pada mana-mana *port* dalam rak peralatan rangkaian tanpa kebenaran dari pihak BTMK.

(c) Pengguna tidak dibenarkan menukar maklumat yang terdapat pada UTP *port*.

(d) Perbuatan yang boleh merosakkan UTP *port*, kabel UTP atau rak peralatan rangkaian serta peralatannya adalah dilarang.

(e) Sebarang kerosakan pada kabel UTP, network point dan network *port* pada mana-mana switch/hub hendaklah dilaporkan kepada BTMK.

7.4 Dial-Up

(a) Kemudahan dial-up hanya diberikan untuk tujuan rasmi.

(b) Permohonan menggunakan kemudahan dial-up adalah dengan mengisi borang yang disediakan.

(c) Pengguna yang menggunakan kemudahan dial-up pada waktu pejabat hendaklah memutuskan sambungan ke rangkaian. Setelah menggunakan kemudahan dial-up, pengguna dikehendaki mengimbas keseluruhan komputer yang digunakan sebelum menyambung semula ke rangkaian KKM.

7.5 FTP

(a) Fail-fail yang bersaiz besar yang dimuat turun hendaklah dilakukan selepas waktu pejabat.

7.6 Pengenalan Dan Katalaluan

(a) Semua pengguna baru hendaklah memohon id-pengguna dengan mengisi borang Permohonan Id Pengguna.

(b) Id-pengguna yang tidak aktif selepas 3 bulan akan dibekukan dan akan dimansuhkan selepas 4 bulan. Pengecualian akan

diberikan kepada pengguna yang memaklumkan kepada BTMK keperluan akaun masing-masing.

(c) Penukaran katalaluan perlulah dibuat oleh setiap pengguna sekurang-kurangnya sebulan sekali.

8. KESELAMATAN RANGKAIAN

8.1 Keselamatan rangkaian (network security) adalah merupakan satu langkah keselamatan utama untuk mengawal aset ICT dari dicerobohi. Reka bentuk rangkaian yang betul dan baik adalah merupakan satu faktor keselamatan rangkaian komputer sesebuah organisasi. Untuk menjamin keselamatan rangkaian di KKM, pihak BTMK telah membangunkan satu reka bentuk rangkaian yang tersusun dan sentiasa dikemas kini dan mengutamakan keselamatan.

8.2 Pemantauan juga dilakukan dari semasa ke semasa untuk memastikan keselamatan rangkaian dan server KKM di dalam *DMZ zone, Secured Zone* dan lain-lain sentiasa berada di dalam keadaan baik. Pengguna tidak dibenarkan membuat memuat turun apa juga perisian seperti *screen saver*, *games* dengan sesuka hati, ini akan memberi impak kepada prestasi rangkaian (network performance) dan kemungkinan adanya virus.

8.3 *Firewall* diwujudkan untuk mengawal capaian ke atas sistem yang telah dibangunkan dan memastikan keselamatan ke atas aset-aset di dalam rangkaian KKM supaya tidak di ceroboh oleh pihak yang tidak bertanggungjawab. *Firewall* yang bertindak sebagai *IP Port Forwarding* dan *Network Address Translations* (NAT) diwujudkan untuk memastikan hanya server-server dan perkhidmatan *port* tertentu sahaja dibenarkan kepada pengguna dari luar untuk mencapai server-server di KKM.

8.4 Selain dari menyediakan infrastruktur rangkaian yang baik, BTMK juga sentiasa memantau setiap log di dalam setiap server untuk memastikan tidak ada capaian yang tidak sah dibuat ke atas server berkenaan.

8.5 Kaedah *frame relay* digunakan dalam sistem rangkaian WAN yang menghubungkan cawangan dan Ibu Pejabat KKM adalah bertujuan untuk memastikan tahap keselamatan semasa penghantaran dan penerimaan maklumat.

8.6 *Proxy* atau *webcache server* dan *viruswall server* juga diwujudkan bagi mengawal serta memantau penggunaan internet. Ia berfungsi mengawal pengguna dari melayari laman web serta mengawal pengguna dari memuat turun fail-fail tertentu seperti gambar lucah, *screen saver*, lagu, video dan sebagainya.

9. KESELAMATAN KATA LALUAN (PASSWORD)

Kata laluan adalah merupakan kata kunci atau *pin number* 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 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 aksara (contoh: P6s*wO~d).

(c) Sekiranya kata laluan telah dicerobohi atau disyaki dicerobohi, hendaklah dilaporkan kepada pegawai keselamatan ICT BTMK dan kata laluan sedia ada akan diubah dengan serta merta.

(d) Kata laluan perlu ditukar sekurang-kurangnya sebulan sekali.

10. KESELAMATAN FIZIKAL KOMPUTER DAN *NOTEBOOK*

Keselamatan fizikal meliputi komputer (personel komputer), *notebook* dan perkakasan terlibat seperti cakera keras (*harddisk)*, pencetak, pengimbas dan lain-lain. Pengguna komputer atau *notebook* hendaklah sentiasa mematuhi garis panduan berikut:

(a) Setiap komputer atau *notebook* mestilah mempunyai kata laluan.

(b) Komputer atau *notebook* perlulah dilakukan pengemaskinian *Microsoft Windows, patches* dan *services pack* yang terkini. Sila hubungi helpdesk BTMK untuk bantuan.

(c) Setiap komputer atau *notebook* perlulah ada *computer name* dan *perisian antivirus Trendmicro* iaitu *Officescan*.

(d) Dilarang mengubah atau meminda *computer name* dan *description* dalam komputer.

(e) Jangan biarkan komputer berada atas talian jika tidak digunakan dan log *off* komputer sebelum meninggalkan pejabat.

(f) Sekiranya penyelenggaraan komputer hendak dilaksanakan, pengguna komputer perlu memastikan semua maklumat penting telah disalin *(backup*) dengan sempurna sebelum dilakukan penyelenggaraan.

(g) Pastikan komputer atau *notebook* pejabat tidak digunakan oleh orang yang tidak berkenaan bagi urusan yang ditetapkan dan hanya untuk urusan rasmi sahaja.

(h) 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.*

(i) Pastikan bekalan atau punca elektrik ditutup semasa pemasangan atau penyambungan peralatan komputer dan aksesorinya atau setelah selesai menggunakan komputer atau *notebook.*

(j) Pastikan komputer atau *notebook* tidak terdedah secara terus kepada pancaran matahari/haba dan elakkan komputer daripada kawasan tarikan kuasa magnet/kuasa voltan yang tinggi.

(k) Pastikan komputer atau *notebook* diletakkan di tempat dingin dan kering persekitarannya dan di tempat yang selamat.

(l) Rehatkan komputer atau *notebook* jika digunakan secara berterusan.

(m) Tamatkan *not responding* dengan kekunci *Ctrl-Alt-Del* jika komputer *hang*.

(n) Pastikan komputer atau *notebook* mempunyai *system date* & *time* yang betul untuk tujuan audit dan penghantaran e-mel.

(o) Sentiasa keluar daripada *windows* atau tutup komputer dengan cara yang betul bagi mencegah ralat sistem iaitu klik *start* dan klik *shut down*. Tidak dibenarkan menutup komputer secara fizikal iaitu dengan menutup suis atau mencabut *plug* dan sebagainya.

(p) Dilarang menghentak/mengetuk dengan apa cara sekalipun sama ada sengaja atau tidak sengaja ke atas komputer atau *notebook*.

(q) Tidak dibenarkan membaiki sendiri komputer atau *notebook* jika ada masalah atau kerosakan.

11. TATACARA PENGURUSAN DISKET

Disket adalah merupakan salah satu media storan elektronik yang digunakan untuk menyimpan data atau kandungan fail. Untuk menjamin keselamatan kandungan pengguna adalah dinasihatkan supaya mengikuti garis panduan berikut :

(a) Setiap Bahagian mestilah mempunyai kaedah atau prosedur kawalan penggunaan disket yang akan merekodkan jumlah penggunaan disket untuk pegawai dan kakitangan dan pelupusan disket.

(b) Disket yang diperoleh adalah untuk tujuan rasmi sahaja.

(c) Setiap disket perlulah dilabelkan mengikut Bahagian/Unit/Nama

(d) Disket yang mengandungi maklumat atau rahsia rasmi mestilah disimpan dengan selamat dan dilabelkan mengikut pengelasannya sama ada Terhad atau Sulit dan mestilah disimpan di tempat yang selamat.

(e) Pengguna adalah dilarang membawa keluar atau memberi disket yang mengandungi maklumat rahsia rasmi kepada orang lain. Ini adalah untuk mengelak dari berlakunya pembocoran rahsia.

(f) Pengguna hendaklah memastikan saiz fail yang disimpan di dalam disket tidak melebihi ruang storan (1.4 MB) yang diperuntukkan dan mengutamakan penyimpanan fail yang perlu sahaja. Sekiranya perlu disarankan untuk melakukan kaedah pemampatan (compress) untuk mengurangkan saiz fail.

(g) Disket yang mengandungi maklumat yang tidak diperlukan lagi, perlulah dipadamkan *(delete*) sebelum digunakan untuk tujuan yang lain.

(h) Elakkan disket dari terkena debu atau habuk, 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.

(i) Sekiranya disket yang digunakan adalah yang telah lama jangka hayatnya, kandungan fail atau maklumat di dalamnya perlulah di pindahkan ke media lain seperti CD, *cartridge*, *thumb drive* dan lain-lain media storan.

(j) Disket yang rosak atau tidak boleh digunakan lagi, perlulah di format semula untuk memadamkan kesemua data di dalamnya sebelum dilupuskan. Ini dilakukan sama ada dengan mericih, menggunting atau dibakar sebelum dibuang.

12. KESELAMATAN PERALATAN ICT DI BILIK *SEVER*

Untuk memastikan server penting sentiasa selamat dari pencerobohan atau sebarang gangguan dan membolehkan ia dicapai sepanjang masa, semua server hendaklah diletakkan di dalam bilik server yang mempunyai kemudahan keselamatan, penyaman udara khas dan kemudahan perlindungan suhu dan kebakaran. Bilik server juga seharusnya dilengkapkan dengan ciri-ciri keselamatan lain seperti *firewall* dan UPS. Semua maklumat penting KKM merupakan aset yang perlu dilindungi sebaik mungkin bagi menjamin keselamatannya. Beberapa langkah telah dilaksanakan bagi melindungi server tersebut. Antaranya adalah :

(a) Satu sistem *Security Access Door* digunakan untuk memantau dan mengawal pengguna yang keluar masuk ke bilik sever.

(b) Hanya pengguna yang mempunyai *card access door* sahaja yang boleh memasuki bilik server.

(c) Setiap server mestilah dilabelkan penggunaannya bagi memudahkan setiap pentadbir menjalankan tugas masing-masing.

(d) Pastikan bilik server sentiasa bersih dan komputer tidak terdedah kepada habuk.

(e) Penghawa dingin mestilah berfungsi dengan baik di mana suhunya di dalam lingkungan ±19.5°C dan kelembapan di paras 50.7%.

(f) Semua peralatan keselamatan, UPS penghawa dingin mestilah diselenggarakan sekerap yang mungkin.

(g) Semua kertas cetakan yang tidak digunakan perlulah diricih (shred).

13. 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 :

13.1 Pembaik pulih Sistem

Pembaik pulih Sistem adalah merupakan proses baik pulih akibat dari kemusnahan atau kehilangan data yang berlaku atas banyak sebab antaranya adalah :-

- kegagalan server berfungsi
- kerosakan fizikal *hard disk*
- masalah kesilapan dalam pemprograman

Proses pembaik pulih sistem terbahagi kepada dua peringkat iaitu **prosedur *backup*** dan **prosedur baik pulih.**

13.1.1 Prosedur *Backup*

(a) *Backup* keseluruhan semua data dan aplikasi termasuk *Operating System* (OS) dibuat pada setiap malam untuk semua server berpandukan prosedur-prosedur *backup* yang telah ditetapkan.

Kekerapan penjanaan data *backup* adalah mengikut kepentingan data-data tersebut secara berperingkat dari harian hinggalah bulanan.

Selain *backup* keseluruhan data-data, terdapat juga *backup* yang dilakukan kepada transaksi selepas *backup* sehingga ke transaksi paling akhir diproses sebelum kerosakan berlaku iaitu dengan penjanaan *backup* yang dipanggil *logical log backup.*

(b) *Backup* atau salinan data ke dalam disket atau media lain perlu dilakukan setiap hari untuk mengelakkan kehilangan data sekiranya berlaku kerosakan *hard disk.*

(c) Pelabelan nama fail yang disalin (backup) untuk memudahkan carian fail dari semasa ke semasa.

(d) *Backup* sistem aplikasi dan sistem operasi perlu diadakan sekurang-kurangnya sekali bagi setiap keluaran versi terbaharu 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 tiga (3) salinan dan setiap satu disimpan di lokasi yang berlainan. Lokasi-lokasi tersebut adalah :-

- Lokasi di mana sistem tersebut beroperasi.
- Lokasi *off-site* pertama – di Bahagian Teknologi Maklumat Dan Komunikasi
- Lokasi *off-site* kedua – di bangunan lain yang berdekatan atau mana-mana Jabatan Kerajaan lain yang berdekatan dan mempunyai kemudahan 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.

13.1.2 Prosedur Baik pulih

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.

13.2 Pelan Pemulihan Bencana

Data-data kritikal disalin *(backup)* ke dalam pita dan disimpan di bilik server, di samping itu pendua bagi data-data tersebut telah 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 sebaginya.

14. KHIDMAT NASIHAT

Sebarang kemusykilan atau pertanyaan berkaitan Tatacara Penggunaan dan Keselamatan Rangkaian ICT di KKM, sila hubungi Bahagian Teknologi Maklumat Dan Komunikasi (BTMK).

15. PENUTUP

Tatacara Penggunaan dan Keselamatan Rangkaian ICT di KKM ini akan dilaksanakan secara menyeluruh. Oleh itu, semua pihak terutama pengguna perlu memberikan kerjasama penuh dengan mematuhi tatacara yang disediakan. Aspek keselamatan merupakan tanggungjawab bersama dan tidak hanya dikhususkan kepada satu pihak sahaja. Bersama-samalah menjayakan hasrat KKM ini untuk memastikan maklumat sentiasa boleh dipercayai dan ia boleh dicapai pada bila-bila masa tanpa sebarang keraguan.

Kementerian Kesihatan Malaysia
30 Disember, 2005