1.0 PENGENALAN

Seiring dengan pembangunan dan pertumbuhan teknologi maklumat, Majlis Perbandaran Ampang Jaya (MPAJ) telah melaksanakan projek pengkomputeran bagi memastikan penyediaan perkhidmatan kepada pelanggan dapat dilakukan dengan pantas dan berkesan. Berdasarkan kepentingan tersebut, pengurusan MPAJ telah menyediakan dokumen ini bagi memastikan objektif perkomputeran ini tercapai.

Dasar Keselamatan Teknologi Maklumat dan Komunikasi (DKICT) untuk Majlis Perbandaran Ampang Jaya (MPAJ) ini disediakan bagi menggariskan peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MPAJ.

Dasar Keselamatan ini disediakan berdasarkan garis panduan yang dikeluarkan oleh Unit Permodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU), Garis Panduan Pengurusan Keselamatan ICT Sektor Awam Malaysia (MyMIS) dan tip dan kaedah pelaksanaan keselamatan terbaik (*best practices*) dari CyberSecurity Malaysia. Keselamatan ICT adalah meliputi semua data, peralatan ICT, perisian, rangkaian dan kemudahan ICT yang lain selaras dengan Pekeliling Am Bil. 3 Tahun 2000 Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan dan Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.

2.0 PENYATAAN DASAR

Keselamatan diikhtirafkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan

dari masa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud suatu keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan asset ICT.

Dasar Keselamatan ICT MPAJ adalah bertujuan untuk melindungi asset ICT dengan meminimumkan kesan insiden keselamatan. Ini adalah bertujuan untuk menjamin kesinambungan urusan dengan menekankan aspek kepenggunaan asset ICT serta prosedur keselamatan yang perlu diikuti oleh semua pegawai dan kakitangan seperti yang telah ditetapkan. Terdapat empat (4) komponen asas keselamatan ICT iaitu :

a. Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
b. Menjamin setiap maklumat adalah tepat dan sempurna;
c. Memastikan kebersediaan maklumat apabila diperlukan oleh pengguna; dan
d. Memastikan akses kepada sistem aplikasi hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT MPAJ merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut :

a. Kerahsiaan – Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
b. Integriti – Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;
c. Tidak Boleh Disangkal – Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

d. Kesahihan – Data dan maklumat hendaklah dijamin kesahihannya; dan
e. Ketersediaan – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

3.0 OBJEKTIF

Dasar Keselamatan MPAJ diwujudkan untuk menjamin kesinambungan urusan MPAJ dengan meminimumkan kesan insiden keselamatan ICT. Objektif utama Dasar Keselamatan ICT MPAJ adalah seperti berikut :

3.1 Menjamin semua aset ICT (maklumat elektronik dan bukan elektronik, perisian, data, rangkaian data dan peralatan) dan pengguna, peraturan, tanggungjawab serta kemudahan ICT yang terdapat di MPAJ adalah dilindungi sepenuhnya daripada kemusnahan, kehilangan, disalahgunakan atau penyelewengan;

3.2 Membantu dalam membimbing para pegawai dan kakitangan MPAJ menggunakan kaedah yang sistematik dan seragam dalam melaksanakan tugas-tugas dan tanggungjawab yang melibatkan ICT;

3.3 Memastikan kelancaran operasi harian MPAJ dan meminimumkan kerosakan atau kemusnahan;

3.4 Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integrity, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

3.5 Mencegah salah guna atau kecurian asset ICT MPAJ.

4.0 SKOP

Dasar Keselamatan ini merangkumi peralatan ICT serta semua bentuk maklumat elektronik yang bertujuan untuk menjamin kerahsiaan dan integriti maklumat tersebut serta kesahihan pengguna dan ketersediaan kepada semua pengguna yang dibenarkan.

Bagi menjamin keselamatan aset ICT sepanjang masa, Dasar Keselamatan MPAJ ini turut merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut :

a. Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan MPAJ. Contoh : komputer, pelayan, peralatan komunikasi dan sebagainya.

b. Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT.

c. Perkhidmatan

Perkhidmatan atau system yang menyokong asset lain untuk melaksanakan fungsi-fungsinya. Contohnya :

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses dan sistem biometrik; dan

iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebarana dan lain-lain.

d. Data atau maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif MPAJ. Contohnya, sistem dokumentasi, prosedur operasi, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan sebagainya.

e. Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian MPAJ bagi mencapai misi dan objektif Majlis. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

f. Premis Komputer dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara (a) hingga (e) di atas.

5.0 PRINSIP-PRINSIP

MPAJ menerimapakai prinsip keselamatan ICT berikut :

a. Capaian Atas Dasar Perlu Mengetahui

Capaian terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

Pertimbangan untuk capaian adalah berdasarkan kategori maklumat seperti mana yang dinyatakan di dalam dokumen "Arahan Keselamatan".

b. Hak Capaian Minimum

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan / atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna / bidang tugas

c. Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap asset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT.

d. Pengasingan

Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

e. Pengauditan

Tujuan aktiviti ini ialah untuk mengenal pasti insiden keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, router, firewall dan rangkaian hendaklah menyelenggarakan jejak-jejak audit.

f. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui Backup dan peraturan pemulihan atau suatu Pelan Pemulihan Bencana dan Pelan Kesinambungan Perkhidmatan.

g. Pematuhan

Tujuan utama ialah untuk menghindar, mengesan, melengah dan bertindakbalas terhadap sebarang perlanggaran Dasar Keselamatan ICT MPAJ.

h. Saling Bergantung

Langkah-langkah keselamatan ICT yang berkesan memerlukan pematuhan kepada semua prinsip-prinsip di atas. Setiap prinsip adalah saling lengkap melengkapi antara satu dengan lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorak sebanyak mungkin mekanisma keselamatan, dapat menjamin keselamatan yang maksimum.

6.0 PENGURUSAN KESELAMATAN ICT

6.1 Organisasi / Struktur Keselamatan ICT

Penglibatan pengurusan atasan adalah penting dalam merancang, menentu hala tuju, memantau keberkesanan dan membudayakan program keselamatan ICT. Pelaksanaan dasar ini akan dijalankan oleh

Yang DiPertua MPAJ dengan dibantu oleh Jawatankuasa Pemandu ICT MPAJ yang dianggotai oleh Pegawai Keselamatan ICT (ICTSO) serta wakil-wakil Jabatan dalaman.

6.2 Pengurusan Risiko

MPAJ melalui ICTSO akan melaksanakan penilaian risiko dari semasa ke semasa ke atas aset ICT jabatan bertujuan untuk memastikan ancaman, kelemahan dan risiko di MPK berada di tahap yang paling minimum.

6.3 Pengurusan Maklumat Sensitif

Pengurusan maklumat sensitif di MPAJ hendaklah mematuhi peraturan-peraturan yang telah ditetapkan di dalam Arahan Keselamatan. Maklumat sensitif yang dikirim secara elektronik hendaklah menggunakan sistem penyulitan yang diluluskan.

6.4 Pengurusan Keselamatan Internet

Teknologi Internet telah memudahkan perhubungan antara pengguna dan menyediakan akses kepada banyak maklumat dalam pelbagai bentuk format dengan menyediakan penyelidikan, analisis, rujukan dan bahan-bahan lain yang berfaedah. Penggunaan Internet dengan cara yang tidak bertanggungjawab adalah dianggap sebagai tatacara yang boleh mengancam keselamatan, keutuhan dan kerahsiaan maklumat, melemahkan dan menggangu sistem dan rangkaian ICT MPAJ.

Demi untuk menjamin keselamatan ICT MPAJ, pihak pengurusan telah menghadkan penggunaan Internet di mana semua pengguna mesti mencapai Internet melalui server utama MPAJ. Pengguna Internet mestilah mematuhi prosidur dan garis panduan berikut : -

a. Tidak dibenar melawati laman web yang tidak beretika seperti *porno* atau tidak dibenarkan (imej atau bahan-bahan yang mengandungi unsur-unsur lucah seperti *Sex, Gay, Lesbian, nude,* xxx dan seumpama dengannya).

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

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

d. Dilarang memuat turun atau naik (*download / upload*) serta menyimpan maklumat yang melibatkan sebarang pernyataan fitnah atau hasutan yang boleh memburuk dan menjatuhkan imej organisasi atau kerajaan.

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

f. Mengaktifkan *pop-up blocker tool* bagi semua penggunaan internet browser untuk menghalang *pop-up screen* yang berkemungkinan mengandungi *code / script* yang bervirus serta

berunsur promosi laman web serta iklan kerana ia akan menyibukkan trafik rangkaian MPAJ dan internet.

g. Dilarang memuat turun fail-fail yang saiz besar melebihi 2 MB. Sila dapatkan khidmat nasihat dari pegawai pentadbir keselamatan dan rangkaian jika ia diperlukan.

h. Semua capaian ke Internet mestilah melalui rangkaian komputer MPAJ sahaja. Dilarang membuat sambungan sendiri secara dial-up kepada mana-mana ISP (JARING, TmNet, TimeNet, dan lain-lain).

6.5 Pengurusan Keselamatan Mel Elektronik (emel)

E-mel merupakan satu media perhubungan yang paling mudah, cepat dan murah untuk berhubung dari satu pihak dengan satu pihak yang lain tidak kira jarak, masa dan tempat. Pihak MPAJ juga memandang serius di dalam keselamatan perhubungan melalui e-mel di antara pegawai-pegawai MPAJ, terutama perhubungan dengan pihak luar yang melibatkan dokumen terperingkat. E-mel rasmi yang diperuntukkan oleh MPAJ (mpaj.gov.my) hanya boleh digunakan untuk tujuan rasmi.

Sebagai langkah tambahan pengguna e-mel adalah dikehendaki mematuhi prosidur berikut : -

a. **Dilarang menggunakan akaun milik orang lain**, berkongsi akaun serta membenarkan akaun digunakan oleh orang lain **walaupun** untuk tujuan **tugas rasmi**.

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

c. Dilarang menyebarkan kod perosak seperti virus, *worm, Trojan Horse* yang boleh merosakkan sistem komputer dan maklumat pengguna lain.

d. Pengguna tidak dibenarkan menggunakan e-mel untuk tujuan komersial, politik, perjudian, jenayah dan perkara-perkara lain yang mana bukan urusan rasmi jabatan.

e. Semua e-mel yang mengandungi fail kepilan 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 akan ditapis dan ditahan penyebarannya kepada penerima kerana dikuatiri mengandungi virus.

f. Dilarang membuka e-mel yang mengandungi fail kepilan (*attachment file*) seperti *.exe, *.scr, *.gif, *.pif, *.com, *.dll, *.bat, *.vbs, *.icr, *.ocx dan sebagainya yang didapati meragukan.

g. *Scanning* akan dilakukan secara otomatik dari server anti virus ke atas semua fail dan *attachment file* pada komputer client bagi mengenal pasti fail-fail yang diserang virus dengan perisian antivirus yang digunakan secara rasmi oleh MPAJ.

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 tidak digalakkan dihantar melalui e-mel**, jika perlu pengguna hendaklah menggunakan **Sijil Digital** (*Digital Certificate*) untuk penghantaran dokumen tersebut melalui e-mel.

j. Saiz fail kepilan (*attachment file*) termasuk kandungan e-mel yang dihantar hanya dibenarkan bagi saiz yang tidak melebihi **4.0 MB** sahaja. Penghantaran e-mel yang bersaiz besar akan mengganggu prestasi e-mel server dan sistem rangkaian.

k. Pengguna yang menggunakan **Webmail MPAJ** hendaklah sentiasa menyelenggara e-mel supaya **saiz storan (*Inbox*)** yang digunakan untuk menyimpan e-mel tidak melebihi **20 MB**, ini adalah bagi menjaga prestasi server e-mel serta prestasi capaian e-mel melalui Webmail.

l. Pengguna e-mel perisian **outlook** hendaklah **sentiasa menyelenggara e-mel** supaya saiz setiap *folder* terutama *folder* INBOX tidak melebihi **500 MB**, ini adalah bagi menjamin prestasi perisian e-mel *outlook* dan komputer pengguna.

m. Pengguna hendaklah **mencetak e-mel yang penting** dan **difailkan** bagi **mengelak maklumat penting hilang** apabila berlaku kerosakan kepada *hard disk* komputer atau serangan virus.

n. Pengguna hendaklah membuat salinan dan **menyimpan *attachment file* ke satu *folder* berasingan** bagi semua e-mel yang

penting bagi tujuan *backup* jika berlaku masalah kepada *hard disk* komputer.

o. Pihak **MPAJ tidak akan bertanggung jawab** ke atas **e-mel yang hilang** bagi pengguna yang tidak mematuhi polisi penggunaan emel.

p. Alamat e-mel rasmi MPAJ hanyalah untuk kegunaan menghantar emel yang rasmi atau tugasan pejabat, sebarang e-mel yang tidak ada kaitan dengan tugasan pejabat adalah dilarang.

q. Penggunaan alamat e-mel yang tidak rasmi seperti *yahoo.com, hotmail.com, gmail.com* atau sebagainya adalah dilarang untuk tugas-tugas rasmi, sama ada untuk urusan dalaman atau luaran MPAJ.

r. Dilarang membuat penyebaran / *forward* e-mel yang tidak rasmi menggunakan alamat e-mel MPAJ.

6.6 Pengurusan Keselamatan Rangkaian

6.6.1 Rangkaian adalah merupakan satu sumber ICT yang utama bagi sesebuah organisasi pada masa kini. Oleh itu, keselamatan rangkaian (*network security*) adalah merupakan satu langkah keselamatan utama untuk mengawal aset ICT dari dicerobohi. Rekabentuk rangkaian yang betul dan baik adalah merupakan satu faktor keselamatan rangkaian komputer sesebuah organisasi. Untuk menjamin keselamatan rangkaian di MPAJ, pihak Bahagian Sistem Maklumat telah membangunkan satu rekabentuk rangkaian

yang tersusun dan sentiasa dikemas kini dan mengutamakan keselamatan.

6.6.2 Pemantauan juga dilakukan dari masa ke semasa untuk memastikan keselamatan rangkaian dan server MPAJ sentiasa berada di dalam keadaan baik. Pengguna tidak dibenarkan memuat turun apa juga perisian seperti *screen saver*, *games*, gambar dan perkara-perkara yang seperti dengannya kerana ia akan memberi impak kepada prestasi rangkaian (*network performance*) dan kemungkinan ada virus atau kod virus bersamanya.

6.6.3 *Firewall* diwujudkan bagi memastikan keselamatan ke atas asset-aset di dalam rangkaian MPAJ supaya tidak diceroboh oleh orang yang tidak bertanggung jawab. Melalui sistem *Firewall* tersebut hanya server-server dan perkhidmatan *port* tertentu sahaja yang dibenarkan kepada pengguna dari luar untuk mencapai server-server dalaman. Konfigurasi keselamatan setiap server diperkemaskan dan dikemaskini dari semasa ke semasa selain dari kawalan capaian oleh *firewall*.

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

6.6.5 *Firewall, Proxy* atau *webcache server, IPS, anti spamming* dan *viruswall server* juga diwujudkan bagi mengawal serta memantau penggunaan internet. Ia berfungsi mengawal pengguna dari melayari laman web *prono* atau lucah serta mengawal pengguna

dari memuat turun fail-fail tertentu seperti gambar lucah, lagu, video dan sebagainya.

6.7 Pengurusan Keselamatan Kata Laluan

Katalaluan adalah merupakan kunci atau *pin* yang menjadi hak individu yang mana ia perlu dirahsiakan dari pengetahuan orang lain. Oleh itu pengguna adalah dinasihatkan menjaga katalaluan masing-masing dengan teliti dari dicuri dan disalahguna oleh pengguna lain. Bagi menjamin keselamatan katalaluan, pengguna perlulah mematuhi prosidur berikut :-

a. Sekiranya katalaluan telah dicuri atau disyaki dicuri, laporan hendaklah dibuat kepada pentadbir sistem ICT dan kata laluan sedia ada hendaklah diubah dengan serta merta.

b. Katalaluan perlu ditukar sekerap mungkin dan dicadangkan sekurang-kurangnya sebulan sekali.

c. Panjang kataluan hendaklah mempunyai sekurang-kurangnya lapan (8) aksara dengan gabungan *alphanumeric* huruf kecil dan besar serta simbol khas.

d. Katalaluan hendaklah dihafal dan jangan sekali-kali disalin di mana-mana media terutama menulisnya di sebelah monitor.

6.8 Pengurusan Keselamatan Perkakasan Komputer (Computer Hardware)

Keselamatan meliputi komputer, *notebook* dan perkakasan terlibat seperti *hard disk*, pencetak, pengimbas dan lain-lain. Pengguna

seharusnya memastikan komputer atau *notebook* dan peralatan yang digunakan sentiasa mematuhi garis panduan berikut :-

a. Setiap komputer atau *notebook* mestilah mempunyai katalaluan.

b. Komputer atau *notebook* perlulah dilakukan pengemaskinian *Microsoft Windows, patches* dan *services pack* yang terkini.

c. Setiap komputer atau *notebook* perlulah ada *computer name* yang sesuai dengan pemilik.

d. Pastikan antivirus sentiasa dikemaskini supaya dapat menangani serangan virus yang baru.

e. Dilarang membuat instalasi perisian yang tidak berlesen atau perisian yang tidak rasmi penggunaannya di MPAJ ke dalam komputer atau *notebook*.

f. Dilarang membuat instalasi perisian *screen saver* atau *active desktop* kerana akan menyebabkan prestasi komputer menjadi perlahan.

g. Semua komputer hendaklah menggunakan *wallpaper desktop* korporat MPAJ.

h. Dilarang mengubah atau meminda *computer name* dan *description* dalam komputer.

i. Pastikan komputer atau *notebook* pejabat tidak digunakan oleh orang yang tidak berkenaan.

j. Pastikan komputer atau *notebook* diletakkan di tempat dingin dan kering serta selamat persekitarannya.

k. 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*.

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

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

n. Rehatkan komputer atau *notebook* jika terlalu kerap menggunakan secara berterusan.

o. Tamatkan proses *not responding* dengan kekunci *Ctrl-Alt-Del* jika PC *hang*. Tidak digalakkan menutup suis sekiranya PC menjadi *hang.*

p. Tidak digalakkan membuka program yang banyak secara serentak di dalam sistem komputer atau *notebook* bagi mengelakkan sistem menjadi *hang*.

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

r. Sentiasa matikan komputer dengan cara yang betul bagi mencegah kerosakan kepada *operating system* (OS) *Windows*.

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

t. *Notebook* yang digunakan atau dibawa ke luar pejabat hendaklah sentiasa dikunci dengan tali pengunci *notebook* sama ada semasa berkerja di meja mahupun di dalam kereta perlu dikunci pada kerusi atau sebagainya.

u. Tidak dibenarkan membaiki sendiri komputer atau *notebook* jika ada masalah atau kerosakan *major* kecuali ia melibatkan masalah yang mudah dan tidak memberi kesan kepada sistem operasi (OS) komputer.

v. Bahagian Sistem Maklumat MPAJ berhak untuk menghapus fail-fail atau maklumat-maklumat yang tidak ada kaitan dengan tugas rasmi seperti fail lagu dan gambar.

6.9 Pengurusan Keselamatan Tatacara Penjagaan Media Storan

Media storan yang popular digunakan pada masa sekarang adalah USB *drive*. Walau bagaimanapun, disket atau cakera liut masih lagi digunakan oleh sesetengah pengguna sebagai media storan elektronik untuk menyimpan data atau fail yang kecil untuk penyebaran

maklumat atau sebagai *backup*. Bagi memastikan data yang disimpan sentiasa selamat, pengguna dinasihatkan supaya mengikut prosidur tatacara penjagaan media storan seperti berikut :-

a. Elakkan disket dari terkena debu-debu atau habuk dan hendaklah disimpan di tempat yang selamat.

b. Sekiranya disket yang digunakan adalah yang telah lama jangka hayatnya, maka data atau fail hendaklah dipindahkan ke media lain yang lebih tahan lama dan selamat seperti CD/DVD.

c. Media storan yang rosak atau tidak boleh digunakan lagi, perlulah dimusnahkan sebelum dibuang. Ini adalah bagi memastikan maklumat di dalamnya betul-betul tidak dapat dicapai oleh orang lain.

d. CD/DVD hendaklah disimpan di tempat yang selamat agar ia tidak tercalar dan rosak.

e. Semua media stroran hendaklah tidak disimpan berhampiran dengan sumber-sumber yang bermagnet bagi mengelakkan data yang disimpan hilang atau rosak.

f. Semua media storan seperti disket, *CD, DVD* dan *Handy Drive* hendaklah dibuat pemeriksaan virus terlebih dahulu sebelum digunakan. Pemeriksaan virus tersebut hendaklah dibuat secara berkala bagi menjamin keselamatan data atau maklumat yang disimpan.

6.10 Pengurusan Keselamatan di Bilik Server

Semua server aplikasi MPAJ ditempatkan di bilik server Aras 15 Menara MPAJ untuk tujuan pengurusan server secara berpusat. Semua data-data yang disimpan di dalam server adalah aset yang penting dan perlu dilindungi sebaik mungkin bagi menjamin keselamatannya. Beberapa langkah telah dilaksanakan bagi melindungi server-server tersebut seperti berikut : -

a. Setiap server perlu dilabelkan untuk memudahkan pentadbir menjalankan tugas masing-masing.

b. Pengguna perlu mencatat buku log yang disediakan sebelum memasuki bilik server.

c. Pastikan bilik server sentiasa bersih supaya server serta peralatan-peralatan dan komputer tidak terdedah kepada habuk.

d. Penghawa dingin mestilah berfungsi dengan baik di mana suhunya berada dalam lingkungan ±19.5°C dan kelembapan di paras 50.7%. Pemantauan perlu sentiasa dilakukan agar tidak berlaku kebocoran yang boleh merosakkan peralatan-peralatan di bilik server.

e. Kertas-kertas cetakan yang tidak digunakan perlulah di *shred* / diricih.

6.11 Pengurusan Keselamatan Perisian Sistem dan Pangkalan Data

Data dan maklumat sistem aplikasi MPAJ yang telah dibangunkan dan sedang beroperasi adalah merupakan aset yang penting. Semua data dan maklumat perlu dilindungi sebaik mungkin bagi menjamin keselamatannya. Beberapa langkah telah dikenalpasti dan perlu dilaksanakan bagi melindungi aset-aset tersebut seperti berikut : -

6.11.1 Pembaikpulih Sistem

Pembaikpulih Sistem adalah merupakan proses baikpulih akibat dari kemusnahan atau kehilangan data yang berlaku atas banyak sebab. Di antaranya adalah :-

- kegagalan server berfungsi
- kerosakan fizikal *hard disk*
- masalah kesilapan dalam pemprograman
- kesan pencerobohan
- kesan bencana alam

Proses pembaikpulih sistem terbahagi kepada dua peringkat iaitu **prosidur backup** dan **prosidur baikpulih.**

a. <u>Prosidur Backup</u>

i. *Backup* semua data dan aplikasi termasuk *Operating System* (OS) dibuat pada setiap petang pada penghujung waktu pejabat untuk semua server. Beberapa prosidur *backup* dilakukan ke atas semua data-data yang disimpan di dalam server.

Kekerapan penjanaan data *backup* adalah mengikut kepentingan data-data tersebut secara berperingkat dari harian hinggalah bulanan. Selain backup terhadap data-data, terdapat juga backup yang dilakukan kepada transaksi selepas backup sehingga ke transaksi paling akhir diproses sebelum kerosakan berlaku.

Menjana backup ini dipanggil *backup logical log.*

ii. *Backup* atau salinan data ke dalam pita atau media lain perlu dilakukan setiap hari untuk mengelakkan kehilangan data sekiranya berlaku kerosakan *hard disk.*

iii. Labelkan setiap media storan *backup* yang digunakan bagi memudahkan proses baikpulih dilaksanakan.

iv. *Backup* sistem aplikasi dan sistem operasi perlu diadakan sekurang-kurangnya sekali bagi setiap keluaran versi terbaharu dari masa ke semasa mengikut peraturan yang ditetapkan semasa perisian itu dibangunkan atau diperolehi atau mengikut garis panduan yang dikeluarkan dari masa ke semasa. Faktor ketahanan dan jangka hayat media storan perlu diambil kira dalam menentukan kekerapan *backup*.

v. *Backup* untuk data dan sistem aplikasi / sistem operasi dicadangkan dibuat dalam tiga (3) salinan

dan setiap satu disimpan di lokasi yang berlainan. Lokasi tersebut adalah:-

- Lokasi di mana sistem tersebut beroperasi.
- Lokasi *off-site* pertama – di Bilik Kebal Aras 4, Jab Perbendaharaan MPAJ
- Lokasi *off-site* kedua – di bangunan lain yang berdekatan atau mana-mana Jabatan Kerajaan lain yang berdekatan dan mempunyai kemudahan untuk menyimpan media *backup*.

vi. 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.

b. <u>Prosidur Baikpulih</u>

Dengan prosidur *backup* di atas, proses membaikpulih boleh dilakukan sama ada dari peringkat paling kritikal seperti kegagalan seluruh *partition hardisk* atau pangkalan data *(database*), aplikasi, direktori sehingga ke atas fail tertentu dapat dibaikpulih dengan mudah dan selamat.

6.11.2 Pelan Pemulihan Bencana (*Disaster Recovery Centre*)

Data-data kritikal di *backup* ke dalam pita (*tape*) dan disimpan di bilik server, disamping itu pendua bagi data-data tersebut dihantar dan disimpan di agensi lain sebagai salah satu pelan pemulihan bencana. Amalan ini perlu 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.

6.12 Pengurusan Keselamatan Dari Ancaman Virus

Serangan virus komputer merupakan masalah yang sentiasa dihadapi oleh MPAJ dan lain-lain organisasi yang menggunakan komputer. Kepelbagaian jenis virus akan menyebabkan kerosakan sistem pengoperasian serta peralatan komputer lain seperti *hard disk*. Ia juga menyebabkan maklumat atau data penting menjadi rosak atau hilang dan mungkin juga ia disebar kepada orang-orang berkenaan tanpa pengetahuan pengguna.

Sebagai langkah keselamatan, MPAJ juga telah membuat tapisan di server *antispamming* untuk mengawal penyebaran virus melalui e-mel. Server akan menapis sebarang e-mel yang mempunyai fail *.exe, *.scr, *.gif, *.pif, *.com, *.dll, *.bat, *.vbs, *.icr dan *.ocx. Kesemua fail berkenaan adalah berkemungkinan besar pembawa virus. Untuk meningkatkan lagi tahap keselamatan di MPAJ, semua pengguna dikehendaki mengambil langkah-langkah berikut :-

a. Pengguna PC mestilah sentiasa melakukan nyah virus (*virus scan*) di PC dan semua media storan yang digunakan untuk mempastikan tidak ada virus sebelum ia digunakan. Dengan itu kita dapat mengawal keselamatan maklumat dan data dari dirosakkan oleh serangan virus.

b. Sekiranya terdapat serangan virus ke atas data atau dokumen dan jika virus tersebut tidak dapat dihapuskan, sila hubungi pihak Bahagian Sistem Maklumat MPAJ untuk bantuan teknikal.

c. Media storan seperti Disket, *handy drive, CD* atau DVD dan lain-lain yang diperolehi dari luar perlulah dis*can* atau dinyah virus terlebih dahulu sebelum digunakan. Dilarang membuka data atau dokumen yang virus yang tidak dapat dihapuskan. Sila dapatkan khidmat nasihat teknikal daripada Bahagian Sistem Maklumat MPAJ.

d. Semua *notebook* atau komputer PC dari luar hendaklah dis*can virus* terlebih dahulu sebelum ia disambung ke sistem rangkaian MPAJ. Sekiranya ia didapati mengandungi virus dan tidak dapat dihapuskan, sila berhubung dengan pihak Bahagian Sistem Maklumat untuk bantuan teknikal.

6.13 Pengurusan Outsourcing

Projek ICT boleh diuruskan oleh pihak ketiga sekiranya diperlukan dan telah mendapat kelulusan. Pihak ketiga termasuk juruperunding dan pembekal terikat dengan perjanjian untuk memastikan integriti dan kerahsiaan maklumat. Kebocoran maklumat rahsia rasmi boleh dikenakan tindakan di bawah Akta Rahsia Rasmi 1972.

6.14 Pelaporan Insiden Keselamatan ICT

Sebarang insiden keselamatan mestilah dilaporkan kepada pihak GCERT MAMPU. Prosedur operasi standard perlu disediakan oleh MPAJ dan diletakkan di bawah tanggungjawab Penolong Pegawai Teknologi Maklumat. Tindakan selanjutnya akan diputuskan oleh Pegawai Teknologi Maklumat.

7.0 PERUNDANGAN

7.1 Penguatkuasaan

Semua pengguna dikehendaki memahami dan mematuhi semua peraturan- peraturan yang terkandung dalam Dasar Keselamatan ICT MPAJ.

7.2 Pelanggaran Dasar Keselamatan ICT

Pelanggaran Dasar Keselamatan ICT akan dirujuk dan dilapor kepada ICTSO. Perkara ini boleh dirujuk kepada Lembaga Tatatertib dan sekiranya melibatkan unsur jenayah dilapor kepada pihak berkuasa.

8.0 PENYELENGGARAAN DOKUMEN

8.1 Pengendalian Perubahan Dokumen

Dasar keselamatan ICT tertakluk kepada perubahan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur perundangan dan kepentingan sosial. Dasar ini hendaklah dibaca bersama dengan dokumen-dokumen yang berkaitan dengan standard, garis panduan dan langkah keselamatan ICT Kerajaan yang akan dikeluarkan dari semasa ke semasa.

8.2 Pemberitahuan Perubahan

Sebarang perubahan terhadap dasar keselamatan ICT hendaklah dimaklumkan kepada semua personel dan pengguna.

8.3 Cadangan Pindaan

Sebarang cadangan pindaan berkaitan dengan dasar ini hendaklah dikemukakan kepada JKK ICT MPAJ.

Nama : Jawatankuasa Keselamatan ICT
Majlis Perbandaran Ampang Jaya (MPAJ)

Alamat : Majlis Perbandaran Ampang Jaya
Menara MPAJ, Jalan Pandan Utama
Pandan Indah 55100 Kuala Lumpur
Selangor Darul Ehsan

8.4 Penyemakan Semula

Dasar Keselamatan ICT tertakluk kepada semakan dan pindaan. Penyemakan semula hendaklah dilaksanakan oleh JKK ICT MPAJ dari semasa ke semasa selaras dengan perubahan dasar Kerajaan, teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial.

9.0 PENUTUP

Secara ringkasnya keselamatan ICT MPAJ ini perlu dilaksanakan secara menyeluruh. Sekiranya salah satu individu, unit, bahagian atau jabatan yang tidak melaksanakannya ia akan menjejaskan keselamatan keseluruhan MPAJ. Oleh itu, keselamatan ICT merupakan tanggungjawab semua pihak dan ia tidak hanya dikhususkan kepada satu pihak sahaja.

Garis panduan keselamatan ini juga akan dikemaskini dari semasa ke semasa tertakluk kepada keperluan keselamatan ICT dan arus perubahan global ICT.

Disediakan oleh :

ROSLIZA BINTI MOHD
PEGAWAI KESELAMATAN ICT (ICTSO)
MAJLIS PERBANDARAN AMPANG JAYA
JUN 2010

Disahkan oleh :

ABD. HAMID BIN HUSSAIN
KETUA PEGAWAI MAKLUMAT (CIO)
MAJLIS PERBANDARAN AMPANG JAYA
JUN 2010