DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

MAJLIS PERBANDARAN AMPANG JAYA

Bahagian Teknologi Maklumat dan Komunikasi
Jabatan Perancangan Korporat

DKICT-MPAJ-01

15 APRIL 2021 | KELUARAN 4.1

ISI KANDUNGAN

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
4 Jun 2010	1.0	Jawatankuasa Pemandu ICT Bil 2/2010	28 Jun 2010
1 Ogos 2011	1.1	Jawatankuasa Pemandu ICT Bil 3/2010	5 Ogos 2011
7 Disember 2012	1.2	Jawatankuasa Pemandu ICT Bil 6/2010	12 Disember 2012
15 Julai 2013	2.0	Jawatankuasa Pemandu ICT Bil 4/2013	22 Julai 2013
06 Julai 2015	3.0	Jawatankuasa Pemandu ICT Bil 3/2015	07 Julai 2015
17 Julai 2019	4.0	Jawatankuasa Pemandu ICT Bil 3/2019	17 Julai 2019
15 April 2021	5.0	Jawatankuasa Pemandu ICT Bil 2/2021	15 April 2021

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 aset ICT.

Dasar Keselamatan ICT MPAJ adalah bertujuan untuk melindungi aset ICT dengan meminimumkan kesan insiden keselamatan. Ini adalah bertujuan untuk menjamin kesinambungan urusan dengan menekankan aspek kepenggunaan aset 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 :

a. 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;

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

c. Memastikan kelancaran operasi harian MPAJ dan meminimumkan kerosakan atau kemusnahan;

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

e. Mencegah salah guna atau kecurian aset 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 aset 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 kebakaran 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

dIndividu 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 aset 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.

PENILAIAN RISIKO KESELAMATAN ICT

MPAJ hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu MPAJ perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

MPAJ hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat MPAJ termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

MPAJ bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

MPAJ perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

(a) Mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

(b) Menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;

(c) Mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindaka yang dapat mengelak dan/atau mencegah berlakunya risiko; dan

(d) Memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan

BIDANG 01 **PEMBANGUNAN DAN PENYELENGGARAAN DASAR**	
0101 Dasar Keselamatan ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan MPAJ dan perundangan yang berkaitan	
010101 Pelaksanaan Dasar	
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	**Yang Dipetua** **MPAJ**
010102 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna MPAJ (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	**ICTSO**
Dasar Keselamatan ICT MPAJ adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan Dasar Keselamatan ICT MPAJ: (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemukakan cadangan pindaan secara bertulis kepasa ICTSO untuk pembentangan dan persetujuan Mesyuarata Pemandu (JPICT) MPAJ	**ICTSO**

(a) Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JPICT; dan (b) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	
010103 Penyelenggaraan Dasar	
Dasar Keselamatan ICT MPAJ adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT MPAJ: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Keselamatan ICT (JPICT) MPAJ; c. Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JPICT; dan d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	**ICTSO**
010104 Pengecualian Dasar	
Dasar Keselamatan ICT MPAJ adalah terpakai kepada semua pengguna ICT MPAJ dan tiada pengecualian diberikan.	**Semua**

BIDANG 02 **ORGANISASI KESELAMATAN**	
0201 Infrastruktur Organisasi Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif **Dasar Keselamatan ICT MPAJ.**	
020101 Yang Dipertua MPAJ	
Yang Dipertua MPAJ adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: a. Memastikan semua pengguna memahami peruntukan-peruntukan dibawah Dasar Keselamatan ICT MPAJ; b. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MPAJ; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT MPAJ; dan e. Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) MPAJ.	**Yang Dipertua MPAJ**
020102 Ketua Pegawai Maklumat (CIO)	
Ketua Pegawai Maklumat (CIO) bagi MPAJ ialah Timbalan Yang Dipertua MPAJ. Peranan dan tanggungjawab CIO adalah seperti berikut: a. Membantu Pengarah Bahagian ICT MPAJ dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Menentukan keperluan keselamatan ICT;	**CIO**

c. Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT MPAJ serta pengurusan risiko dan pengauditan; dan d. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MPAJ	
020103 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) bagi MPAJ ialah Pengarah Bahagian Perancangan Korporat ICT (BPICT), MPAJ. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Mengurus keseluruhan program-program keselamatan ICT MPAJ; (b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT MPAJ; (c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MPAJ kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MPAJ; (e) Menjalankan pengurusan risiko; (f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPAJ berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;	**ICTSO**

(h) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT Kerajaan (GCERT), MAMPU dan memaklumkannya kepada CIO; (i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan (j) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT. (k) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
020104 Pengurus ICT	
Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MPAJ; (b) Menentukan kawalan akses pengguna terhadap aset ICT MPAJ; (c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MPAJ.	**Pengurus ICT**
020105 Pentadbir Sistem ICT	
Pentadbir Sistem ICT bagi MPAJ ialah Timbalan Yang Dipertua Majlis Perbandaran Ampang Jaya, Pengarah Jabatan Perancangan Korporat, Bahagian Khidmat Pengurusan dan Sumber Manusia, Pegawai Teknologi Maklumat Bahagian Teknologi Maklumat dan Penolong Pegawai Bahagian Teknologi Maklumat.	

Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar,bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT MPAJ; (c) Memantau aktiviti capaian harian sistem aplikasi pengguna; (d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (e) Menganalisis dan menyimpan rekod jejak audit; (f) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan (g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, computer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	**Pentadbir Sistem ICT**
020106 Pengguna	
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPAJ; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT MPAJ dan menjaga kerahsiaan maklumat MPAJ; e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;	**Pengguna**

f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan

g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MPAJ sebagaimana **Lampiran B**.

020107 Jawatan Kuasa Pemandu ICT MPAJ

Jawatankuasa Pemandu ICT (JPICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT MPAJ.

Di MPAJ, Mesyuarat Pengurusan (MPAJ) juga berperanan sebagai JPICT MPAJ. Keanggotaan JPICT MPAJ adalah seperti berikut:

Pengerusi : Yang Dipertua MPAJ

Ahli :

(1) CIO MPAJ

(2) ICTSO MPAJ

(3) Semua Pengarah Bahagian

JPICT MPAJ

Bidang kuasa:

a. Memperakukan/meluluskan dokumen DKICT MPAJ;

b. Memantau tahap pematuhan keselamatan ICT;

c. Memperaku garis panduan, prosedur dan tatacara untuk aplikasi- aplikasi khusus dalam MPAJ yang mematuhi keperluan DKICT MPAJ;

d. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;

e. Memastikan DKICT MPAJ selaras dengan dasar-dasar ICT kerajaan semasa;

f. Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa;

g. Membincang tindakan yang melibatkan pelanggaran DKICT MPAJ; dan

h. Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden

020108 Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan (GCERT)

Tanggungjawab CERT MPAJ.

(a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden.

(b) Merekod dan menjalankan siasatan awal insiden yang diterima

(c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baikpulih minima.

(d) Menghubungi dan melapor insiden yang berlaku kepada GCERT MAMPU samada sebagai input atau tindakan seterusnya.

(e) Menjalankan penilaian untuk mempastikan tahap keselamatanICT dan mengambil tindakan pemulihan dan pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.

Keahlian GCERT MPAJ

- **Pengarah CERT (Timbalan Yang Dipertua - CIO)**
- **Pengurus CERT (Pegawai Teknologi Maklumat - ICTSO)**
- **Pegawai Teknologi Maklumat**
- **Penolong Pegawai Teknologi Maklumat**
- **Wakil Di Setiap Jabatan**

0202 Pihak Ketiga	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Rundingdan lain-lain).	
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPAJ; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; (d) Akses kepada aset ICT MPAJ perlu berlandaskan kepada perjanjian kontrak; (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT MPAJ; ii. Tapisan Keselamatan iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. (f) Menandatangani **Surat Akuan Pematuhan Dasar Keselamatan ICT MPAJ** sebagaimana **Lampiran B.**	**CIO, ICTSO, Pengurus ICT**, **Pentadbir Sistem ICT dan Pihak Ketiga**

BIDANG 03 PENGURUSAN ASET	
0301 Akauntabiliti Aset	
Objektif: **Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MPAJ.**	
030101 Inventori Aset ICT	
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini; b. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MPAJ; d. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan e. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya	**Pentadbir Sistem dan Semua**

0302 Pengelasan dan Pengendalian Maklumat (Maklumat Sensitif)	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
030201 Pengelasan Maklumat	
Pengelasan Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	Semua
030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa c. Menentukan maklumat sedia untuk digunakan d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;	**Semua**

(f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum	

BIDANG 04

KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan MPAJ, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga MPAJ hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.

040101 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan MPAJ serta pihak ketiga yang terlibat dalam menjaminkeselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MPAJ serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan danperaturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	**Semua**

040102 Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:	

(a) Memastikan pegawai dan kakitangan MPAJ serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MPAJ; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MPAJ secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan/atau undang- undang ke atas pegawai dan kakitangan MPAJ serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MPAJ; dan (d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujukkepada Bahagian Khidmat Pengurusan dan Sumber Manusia, MPAJ.	**Semua**
040103 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada MPAJ mengikut peraturan dan / atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MPAJ dan / atau terma perkhidmatan	**Semua**

BIDANG 05

KESELAMATAN FIZIKAL DAN PERSEKITARAN

050101 Kawalan Kawasan

Objektif:

Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

050101 Kawalan Kawasan	
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat (c) Memasang alat penggera atau kamera; (d) Mengehadkan jalan keluar masuk; (e) Mengadakan kaunter kawalan; (f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat (g) Mewujudkan perkhidmatan kawalan keselamatan; (h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini;	**CIO dan ICTSO**

(i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; (k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Setiap Pelawat perlu mendapatkan pengesahan daripada ketua kerani melalui Sistem @ Pelawat. Setiap pengguna MPAJ hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan balik kepada MPAJ apabila pengguna berhenti atau bersara; (c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama Menara Majlis Perbandaran Ampang Jaya (d) Amalan ini perlu dipatuhi. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (e) Kehilangan pas mestilah dilaporkan dengan segera.	**Semua**
050103 Kawasan Larangan (Pengurusan Keselamatan di Bilik Server)	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untukmelindungi aset ICT yang terdapat di dalam kawasan tersebut.	**Pentadbir Sistem**

Kawasan larangan di MPAJ adalah bilik Yang Dipertua MPAJ, bilik Timbalan Yang Dipertua, Bilik Server di tingkat 15. a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan b) Pihak ketiga adalah dilarang sam sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai. c) Setiap server perlu dilabelkan untuk memudahkan pentadbir menjalankan tugas masing-masing. d) Pengguna perlu mencatat buku log yang disediakan sebelum memasuki bilik server. e) 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.	
0502 Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT MPAJ dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
050201 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) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b) Setiap komputer atau *notebook* mestilah mempunyai katalaluan.	**Semua**

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

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

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

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

g) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;

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

j) Pengguna mesti memastikan perisian antivirus di computer peribadi mereka sentiasa aktif *(activated)* dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

k) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

l) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply (UPS);*

m) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;

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

o) Peralatan ICT yang hendak dibawa keluar dari premis MPAJ perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan;

p) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera

q) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

r) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih;

s) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

t) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;

u) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT.

v) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

w) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan

x) Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.

050202 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.	**Semua**

g. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan i. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu	
050203 Media Tandatangan Digital	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan (c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	**Semua**
050204 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MPAJ; (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT (c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-rom*, *disk* atau media berkaitan bag mengelakkan dari berlakunya kecurian atau cetak rompak; dan (d) *Source code* sesuatu sistem hendaklah disimpan dengan teraturdan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	**Semua**

050205 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b. Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT. g. Pinjaman perkakasan komputer perlu diisi didalam buku daftar keluar masuk.	**Pegawai Aset dan Bahagian Teknologi Maklumat MPAJ**
050206 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis MPAJ adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan	**Semua**

b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	
050207 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MPAJ dan ditempatkan di MPAJ. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MPAJ. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding,grinding, degauzing* atau pembakaran; (b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; (c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (d) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (e) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengiku tatacara pelupusan semasa yang berkuat kuasa; dan (f) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:	**Pegawai Aset dan Bahagian Teknologi Maklumat MPAJ**

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran computer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MPAJ; iii. Memindah keluar dari MPAJ mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MPAJ; dan v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
0503 Keselamatan Persekitaran	
Objekt: Melindungi aset ICT MPAJ dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301 Kawalan Persekitaran	
Bangunan yang menempatkan pusat data / bilik server hendaklah mempunyai kawalan persekitaran seperti berikut :	

i. Susun atur hendaklah dirancang dengan teliti dan mengambil kira ancaman yang akan dihadapi ii. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; iii. Menyediakan sistem pengudaraan (ventilation) yang mencukupi iv. Akses kepada saluran *riser* hendaklah sentiasa dikunci. v. Semua ruang pejabat khususnya kawasan yang mempunyaikemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; vi. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; Bangunan yang menempatkan pusat data / bilik server hendaklah menentukan ciri-ciri keselamatan seperti berikut : i. Bekalan kuasa elektrik mesti dari punca yang berasingan dan berkemampuan menampung semua beban termasuk server, alat penghawa dingin, alat penggera dan lain-lain ii. *"Centralized Uninterruptable Power Supply" (UPS)* dan / atau janakuasa sokongan *(back up)* hendaklah disediakan dan diuji setiap tiga bulan bagi menentukan bekalan kuasa berterusan.	
050302 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;	**Bahagian Teknologi Maklumat, MPAJ dan ICTSO**

b. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	
050303 Kabel	
Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *'trunking'* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	**Bahagian Teknologi Maklumat, MPAJ dan ICTSO**
050304 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MPAJ. b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras.	**Semua dan Pegawai Keselamatan Jabatan**

0504 Keselamatan Dokumen

Objektif:

Melindungi maklumat MPAJ dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.

050401 Dokumen

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	**Semua**

BIDANG 06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0601 Pengurusan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan	
060101 Pengendalian Prosedur	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat,pengendalian output, bantuan teknikal dan pemulihan sekiranyapemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	**Semua**
060102 Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk (b) pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;	**Semua**

(c) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung denganaset ICT berkenaan; (d) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (e) Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
060103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	**Pengurus ICT dan ICTSO**

0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
060201 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga Semua perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan (c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	**Semua**
0603 Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	**Pentadbir Sistem ICT dan ICTSO**

060302 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	**Pentadbir Sistem ICT dan ICTSO**
0604 Perisian Berbahaya	
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.	
060401 Perlindungan dari Perisian Berbahaya (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 :- Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System (IDS)*	**Pentadbir Sistem ICT dan ICTSO**

(b) (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; (c) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; (d) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; (e) Mengemas kini anti virus dengan *pattern* antivirus yang terkini; (f) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (g) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (h) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (i) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (j) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus. (k) 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.	
060402 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	**Semua**

0605 *Housekeeping*

Objektif:
Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

060501 *Backup*

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, backup hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat backup keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat backup ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat; c. Menguji sistem backup dan prosedur restore sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh Semua dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d. Menyimpan sekurang-kurangnya tiga (3) generasi backup; dan e. Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.	**Semua**

0606 Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
060601 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. 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. b. 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.	**Bahagian Teknologi Maklumat,** **MPAJ**

c. Firewall diwujudkan bagi memastikan keselamatan ke atas aset-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. d. 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. e. 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 porno atau lucah serta mengawal pengguna dari memuat turun fail-fail tertentu seperti gambar lucah, lagu, video dan sebagainya	
0607 Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060701 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	**Semua**
060702 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:	**Semua**

a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	
060703 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan system dokumentasi adalah seperti berikut: (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan system dokumentasi; dan (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	**Semua**

060704 Sanitasi Media	
Sanitasi media merupakan proses pelupusan data dan maklumat secara kekal agar maklumat tidak diguna pakai atau dimanipulasi oleh mana-mana pihak yang mempunyai kepentingan tertentu. Dalam melaksanakan sanitasi media, perkara-perkara berikut hendaklah dipatuhi :- a) Prosedur yang berkaitan dengan sanitasi media perlu dibangunkan, diterbitkan, dibudayakan dan dikemas kini selaras dengan perkembangan teknologi, amalan terbaik serta mengikut garis panduan yang ditetapkan oleh Kerajaan. b) Kaedah sanitasi yang sesuai sama ada secara logical atau fizikal perlu ditentukan mengikut jenis media yang digunakan. c) Sanitasi logikal boleh dilaksanakan sama ada secara sanitasi fail, sanitasi partition, sanitasi media storan ataupun tetapan asal (factory setting). d) Sanitasi fizikal boleh dilaksanakan melalui tiga kaedah iaitu tulis ganti secara fizikal, penyingkiran (purging) dan pemusanahan media secara fizikal (destroying). e) Keputusan untuk melaksanakan proses sanitasi perlu bersandarkan kepada pengelasan data, maklumat, rekod rasmi dan rahsia rasmi serta tahap risiko berkaitan dan bukannya terhadap jenis media. f) Tadbir urus sanitasi media haruslah dilaksanakan dengan mengguna pakai Jawatankuasa Pelupusan. g) Proses sanitasi media rahsia rasmi perlu memenuhi aspek perundangan dan pentadbiran yang berkuat kuasa. h) Setiap aktiviti sanitasi media elektronik hendaklah direkodkan dengan jelas bagi menjamin akauntabiliti pengurusan sanitasi di MPAJ. i) Sanitasi media elektronik secara fizikal perlu mematuhi keperluan undang-undang yang ditetapkan oleh Jabatan Alam Sekitar. j) Pihak MPAJ boleh melaksanakan proses sanitasi terhadap media yang ada melalui perkhidmatan yang ditawarkan oleh MAMPU melalui Makmal Forensik Digital (MyDFLab) MDFlab.	**Semua**

0608 Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara MPAJ dan agensi luar terjamin.	
060801 Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara MPAJ dengan agensi luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MPAJ; dan (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya. **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 yang mengawal data sensitif.	**Semua**
060802 Pengurusan Keselamatan Mel Elektronik (E-mel)	
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.	**Semua**

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) Semua kakitangan baru akan disediakan email MPAJ.

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

c) 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.

d) Dilarang menyebarkan kod perosak seperti virus, *worm, Trojan Horse*

yang boleh merosakkan sistem komputer dan maklumat pengguna lain.

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

f) 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.

g) 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.

h) *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.

i) 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.

j) 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.

k) Saiz fail kepilan (*attachment file*) termasuk kandungan e-mel yang dihantar hanya dibenarkan bagi saiz yang tidak melebihi **10 MB** sahaja. Penghantaran e-mel yang bersaiz besar akan mengganggu prestasi e- mel server dan sistem rangkaian.

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

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 files* 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. s) Saiz email untuk setiap kakitangan adalah berbeza mengikut jawatan. Berikut adalah saiz emel bagi kakitangan:- i) Pengarah/Ahli Majlis – 3GB ii) Pegawai A/Pegawai B/Ketua Kerani – 2GB iii) Kerani – 1GB iv) Pembantu Am/Buruh/Pemandu – 500MB	
0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)	
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang	
060901 E-Dagang	
Objektif: Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet.	**Semua**

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	
060902 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan c. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	**Semua**

0610 Pemantauan

Objektif:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

061001 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT MPAJ; (b) Serangan kod perosak (malicious code), halangan pemberian perkhidmatan (denial of service), spam, pemalsuan (forgery, phising), pencerobohan (intrusion), ancaman (threats) dan kehilangan fizikal (physical loss); (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah,berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; dan (h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	**ICTSO**

061002 Jejak Audit

Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara.	

Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti,rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
061003 Sistem Log	
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	**Pentadbir Sistem ICT**

061004 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d. Aktiviti pentadbiran dan operator sistem perlu direkodkan; e. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan f. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MPAJ atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	**Bahagian Teknologi Maklumat MPAJ dan Pentadbir Sistem ICT**

BIDANG 07 KAWALAN CAPAIAN	
0701 Dasar Kawalan Capaian	
Objektif: Mengawal capaian ke atas maklumat.	
070101 Keperluan Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Kawalan ke atas kemudahan pemprosesan maklumat.	**Bahagian Teknologi Maklumat, MPAJ dan Pentadbir Sistem ICT**

0702 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas aset ICT MPAJ.	
070201 Akaun Pengguna	
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi:- a. Akaun yang diperuntukkan oleh MPAJ sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identity pengguna; c. Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. d. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; e. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MPAJ. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; f. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan g. Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan	**Pentadbir Sistem ICT**

070202 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas	**Pentadbir Sistem ICT**
070203 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MPAJ seperti berikut: a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c) Panjang kata laluan mestilah sekurang-kurangnya lapan(8) aksara dengan gabungan huruf,angka dan simbol ; d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan daripada pengenalan identity pengguna;	**Semua dan Pentadbir Sistem ICT**

i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
070204 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	**Semua**

0703 Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian	
070301 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaianhendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MPAJ, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perlatan yang menjadi kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	**Semua dan Pentadbir Sistem ICT**
070302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet di MPAJ hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. b. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MPAJ; c. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan;	**Pentadbir Rangkaian**

e. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. f. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; g. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pengarah/ pegawai yang diberi kuasa; h. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; i. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet; j. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; k. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MPAJ; l. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti "*newsgroup"* dan "*bulletin board"*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; m. Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan n. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan	**Pentadbir Rangkaian**

ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	
0704 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian	
070401 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: (a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan (b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (a) Mengesahkan pengguna yang dibenarkan; (b) Mewujudkan jejak audit ke atas semua capaian system pengoperasian terutama pengguna bertaraf *super user;* dan (c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur '*log on'* yang terjamin;	**Pentadbir Sistem ICT dan ICTSO**

(b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Mengehadkan dan mengawal penggunaan program; dan (d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
0705 Kawalan Capaian Aplikasi dan Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi	
070501 Capaian Aplikasi dan Maklumat	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, Perkara-perkara berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); (c) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; (d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri- ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan	**Pentadbir Sistem ICT dan ICTSO**

(e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
0706 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh	
070601 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	**Semua**
070602 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	**Semua**

BIDANG 08

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif:

Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

080101 Keperluan Keselamatan Sistem Maklumat

a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c) Aplikasi perlu mengandungi semakan pengesahan (validation) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan system berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	**Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO**

080102 Pengesahan Data Input dan Output

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b) Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	**Pemilik Sistem dan Pentadbir Sistem ICT**
0802 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 Enkripsi	
Objektif: Pengguna hendaklah membuat enkripsi (encryption) ke atas maklumat sensitive atau maklumat rahsia rasmi pada setiap masa.	
080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia Semua rasmi secara elektronik.	
080203 Pengurusan Infrastruktur Kunci Awam (*PKI*)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	**Semua**
0803 Keselamatan Fail Sistem	

Objektif:
Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

080301 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi seperi berikut : (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; (c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan (e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	**Sistem ICT**

0804 Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080401 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. (c) Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; (d) Mengawal perubahan dan / atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (e) Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan (f) Menghalang sebarang peluang untuk membocorkan maklumat.	**Pemilik Sistem dan Pentadbir Sistem ICT**
080402 Pembangunan Perisian Secara *Outsource*	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik MPAJ.	**Bahagian Teknologi Maklumat dan Pentadbir Sistem ICT**

0805 Kawalan Teknikal Keterdedahan (*Vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080501 Kawalan dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas system pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut:: (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	**Pentadbir Sistem ICT**

BIDANG 09

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

090101 Mekanisme Pelaporan

Insiden keselamatan ICT bermaksud musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan GCERT MAMPU dengan kadar segera: (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa. (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	**Semua**

Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di MPAJ Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
0902 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada MPAJ. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan ICTSO dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti;	**ICTSO**

(b) Menyalin bahan bukti dan merekodkan semua maklumat aktivitipenyalinan;

(c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan;

(d) Menyediakan tindakan pemulihan segera; dan

(e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.

BIDANG 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	
1001 Dasar Kesinambungan Perkhidmatan	
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
100101 Pelan Kesinambungan Perkhidmatan	
Pelan Kesinambungan Perkhidmatan (Business Continuity Management - BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT MPAJ. Perkara- perkara berikut perlu diberi perhatian: (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; (c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (d) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;	**Koordinator PKP** **MPAJ**

(f) Membuat backup; dan

(g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.

Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:

(a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

(b) Senarai personel MPAJ dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden;

(c) Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;

(d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan

(e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diujisekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalampersekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan.

Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui pelan tersebut ,tanggiungjawab dan peranan mereka apabila pelan dilaksanakan. MPAJ hendaklah memastikan salinan pelan BCM sentiasa dikemaskini dan dilindungi seperti lokasi utama.

BIDANG 11 PEMATUHAN	
1101 Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT MPAJ.	
110101 Pematuhan Dasar	
Setiap pengguna di MPAJ hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MPAJ dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di MPAJ termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT MPAJ selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber MPAJ.	**Semua**
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	**ICTSO**

110103 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	**Semua**
110104 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di MPAJ adalah seperti di **Lampiran C.**	**Semua**
110105 Pelanggaran Dasar	
Sebarang pelanggaran dasar secara sengaja atau sebaliknya boleh menyebabkan: • Kehilangan hak capaian ke atas sumber maklumat atau; • Penilaian prestasi kerja yang buruk atau; • Dikenakan tindakan tatatertib atau; • Digantung kerja atau ditamatkan perkhidmatan atau; • Ditamatkan kontrak atau; • Dikenakan tindakan undang-undang.	**Semua**

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CD ROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.

Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage), penipuan (hoaxes).
GCERT	Government Computer Emergency Response Team atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	Information and Communication Technology (Teknologi Maklumat dan Komunikasi).
ICTSO	ICT Security Officer Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.

	Merupakan suatu titik yang berperanan sebagai pintu masuk ke Internet rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari Gateway satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaianrangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer
Logout	Log-out komputer Keluar daripada sesuatu sistem atau aplikasi komputer
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. ia meibatkan serangan virus, trojan horse, worm, spyware, dan sebagainya
Modem	MOdulator DEModulator Perantiyang boleh menukar strim bit digital ke isyarat analog dan sebaiknya . Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen dibangunkan oleh sesebuah organisasi atau pejabat.

Perisian Aplikasi	Ia merujuk kepada peisian atau pakej yang selalu digunakan seperti spreadsheet dan word processing ataupun sstem aplikasi yang dibangunkan oleh sesebuah organisasi atau pejabat.
Public-Key Infrastructure	Infrastruktur Kunci Awam merupakan satu kombinasi perisian teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan trasaksi melalui internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan .Contohnya, pencapaian internet
Skrin Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan Komputer
Switch	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense Multiple Access / Collision Detection (CSMA/CD) yang merupakaln satu protokol penghantaran degan mengurangkan perlanggaran yang berlaku.
TREAT	Gangguandan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakanbagi membekalkan bekalan kuasa yang berterusan dari sunber berlainan ketika ketiadaan bekalan kuasa ke peralatayang bersambung
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar
Video Streaing	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak

Virus	Atur cara yang bertujuan merosakan data atau sistem aplikasi
Wireless LAN	Jaringan komputer yang berhubung tanpa melalui kabel

Lampiran A

CARTA ORGANISASI STRUKTUR KESELAMATAN ICT MPAJ

Lampiran B

BAHAGIAN TEKNOLOGI MAKLUMAT & KOMUNIKASI
JABATAN PERANCANGAN KORPORAT
MAJLIS PERBANDARAN AMPANG JAYA

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT
MAJLIS PERBANDARAN AMPANG JAYA

Keselamatan ICT adalah merangkumi peralatan, perisian, semua data dan maklumat serta rangkaian yang menjadi **HAKMILIK kepada Majlis Perbandaran Ampang Jaya**. Kakitangan MPAJ/kontraktor **tidak mempunyai hak untuk menyalinalih, menerbitkan semula , menggunapakai, mengedar dan memindahmilik** kepada mana-mana pihak ketiga dalam keadaan apa jua sekalipun **KECUALI** mendapat kebenaran bertulis dari Pengarah Majlis Perbandaran Ampang Jaya.

Tandakan ✓ pada kotak yang disediakan

Nama : ……....

No. Kad Pengenalan : …….

Jawatan : ……..

Status : Kakitangan MPAJ ☐ Kontraktor ☐

☐ Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-
Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yan terkandung seperti perkara di atas.
Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka **pihak MPAJ** boleh mengambil tindakan di bawah **Akta Rahsia Rasmi 1972.**

.....
(Tandatangan Kakitangan MPAJ/Kontraktor) Tarikh:.....

Pengesahan Oleh:

.....
(ROSLIZA BINTI MOHD)
Pengarah/
Ketua Keselamatan Maklumat Jabatan Perancangan Korporat
b.p Yang Dipertua
Majlis Perbandaran Ampang Jaya Tarikh:.....

SENARAI PERUNDANGAN DAN PERATURAN

Arahan Keselamatan;

a) Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

b) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;

c) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

d) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;

e) Surat Pekeliling Am Bilangan 6 Tahun 2005 –Garis Panduan Penilaian Risiko Keselamatan Maklumat SektorAwam;

f) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

g) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi- Agensi Kerajaan yang bertarikh 20 Oktober 2006;

h) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

i) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

j) Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

k) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

l) Surat Pekeliling Perbendaharaan Bil. 3/1995 – Peraturan Perolehan Perkhidmatan Perundingan;

m) Akta Tandatangan Digital 1997;

n) Akta Rahsia Rasmi 1972;

o) Akta Jenayah Komputer 1997;

p) Akta Hak Cipta (Pindaan) Tahun 1997;

q) Akta Komunikasi dan Multimedia 1998;

r) Perintah-Perintah Am;

s) Arahan Perbendaharaan;

t) Arahan Teknologi Maklumat 2007;

u) Garis Panduan Keselamatan MAMPU 2004;

v) Standard Operating Procedure (SOP) ICT MAMPU;

w) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

x) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.