Dasar Keselamatan ICT

Majlis Perbandaran Pekan

1 NOVEMBER 2023

Versi 3.0

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MPP	3.0	01/11/2023	3/82

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT MPP mengandungi peraturan-peraturan mengenai penggunaan perkakasan dan perisian (aset) teknologi maklumat dan komunikasi (ICT) MPP. Peraturan-peraturan ini perlu difahami dan dipatuhi oleh semua pengguna di MPP. Dasar ini juga menerangkan mengenai tanggungjawab dan peranan pengguna dalam melindungi aset ICT MPP.

OBJEKTIF

Dasar Keselamatan ICT MPP diwujudkan untuk mencapai tahap keselamatan ICT yang meneluruh bagi memastikan kesinambungan serta perkongsian maklumat dalam semua urusan di MPP dengan melindungi kepentingan Majlis dan meminimumkan insiden keselamatan ICT serta kesannya seperti berikut;

a. Memastikan kelancaran operasi MPP dan meminimumkan kerosakan atau kemusnahan;
b. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;
c. Mencegah salah guna atau kecurian aset ICT Kerajaan;
d. Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;
e. Meningkatkan tahap keselamatan ICT kepada para kakitangan, pengguna dan pembekal;
f. Memperkemaskan pengurusan risiko; dan
g. Melindungi aset ICT daripada penyelewengan oleh kakitangan, pengguna dan pembekal.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang melibatkan kerosakan atau kejadian yang tidak diingini. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah. Keselamatan ICT adalah bermaksud 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. 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 ketersediaan maklumat apabila diperlukan oleh pengguna; dan
d. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT MPP 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 kemas kini. 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.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Dasar ini meliputi semua aset ICT MPP yang terdiri daripada perkakasan, perisian, data/maklumat dan manusia. Dasar Keselamatan ICT MPP menetapkan keperluan-keperluan asas berikut:

a. Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
b. Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Memandangkan sistem ICT sangat kompleks dan terdedah kepada kelemahan, ancaman dan risiko, adalah tidak mudah untuk memenuhi keperluan ini. Sistem ICT dan komponennya yang saling berhubungan dan bergantungan antara satu dengan lain kerap kali mewujudkan pelbagai kelemahan. Sesetengah risiko hanya menjadi kenyataan setelah masa berlalu manakala sesetengahnya timbul apabila berlaku perubahan. Walau bagaimanapun risiko seperti ini hendaklah dikenal pasti dan ditangani sewajarnya.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT MPP ini 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 MPP. 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. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada MPP;

c. Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; 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 MPP. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod MPP, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

e. Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian MPP bagi mencapai misi dan objektif agensi. Individu

berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

f. Premis Komputer Dan Komunikasi

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

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah- langkah keselamatan.

Dasar Keselamatan ICT MPP ini juga adalah saling lengkap melengkapi dan perlu dilaksanakan secara konsisten dengan undang-undang dan peraturan yang sedia ada.

Dasar ini adalah terpakai kepada semua pengguna di Majlis Perbandaran Pekan termasuk kakitangan, pembekal dan pakar runding yang mencapai, mengurus, menyelenggara, memproses, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT Majlis Perbandaran Pekan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT MPP dan perlu dipatuhi adalah seperti berikut:-

a. **Akses Atas Dasar Perlu Mengetahui**

Akses 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 akses di bawah prinsip ini adalah berasaskan kepada klasifikasi maklumat dan tapisan keselamatan pengguna seperti berikut (Sumber: Arahan Keselamatan perenggan 53, muka surat 15):-

i. Klasifikasi Maklumat

Keselamatan ICT Kerajaan hendaklah mematuhi "Arahan Keselamatan" perenggan 53, muka surat 15, di mana maklumat dikategorikan kepada Rahsia Besar, Rahsia, Sulit dan Terhad. Data, bahan atau maklumat rasmi yang sensitif atau bersifat terperingkat perlu dilindungi dari pendedahan, di manipulasi atau diubah semasa dalam penghantaran. Penggunaan kod dan tandatangan digital mesti dipertimbangkan bagi melindungi data yang dikirim secara elektronik. Dasar kawalan akses ke atas aplikasi atau sistem juga hendaklah mengikut klasifikasi maklumat yang sama, iaitu sama ada rahsia besar, rahsia, sulit atau terhad; dan

ii. Tapisan Keselamatan Pengguna

Dasar Keselamatan ICT Kerajaan adalah mematuhi prinsip bahawa pengguna boleh diberi kebenaran mengakses kategori maklumat tertentu setelah siasatan latar belakang menunjukkan tiada sebab atau faktor untuk menghalang pengguna daripada berbuat demikian.

b. **Hak Akses Minimum**

Hak akses kepada pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu data atau maklumat. Hak akses adalah 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. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah MPP menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:-

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

d. **Pengasingan**

i. Prinsip pengasingan bermaksud bahawa semua tugas-tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data diasingkan. Ia bertujuan untuk mengelak akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat, di manipulasi dan seterusnya, mengenalkan integriti dan kebolehsediaan; dan

ii. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. Ia bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail program, kemudahan sistem dan komunikasi, manakala pemisahan antara domain pula adalah untuk mengawal dan mengurus perubahan pada konfigurasi dan keperluan sistem.

Pada tahap minimum, semua sistem ICT perlu mengekalkan persekitaran operasi yang berasingan seperti berikut:-

i. Persekitaran pembangunan di mana sesuatu aplikasi dalam proses pembangunan;

ii. Persekitaran penerimaan di mana sesuatu aplikasi diuji; dan

iii. Persekitaran sebenar di mana aplikasi sedia untuk beroperasi.

e. **Pengauditan**

i. Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall*, dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*. Pentingnya *audit trail* ini menjadi semakin ketara apabila wujud keperluan untuk mengenal pasti punca masalah atau ancaman kepada keselamatan ICT. Oleh itu, rekod audit hendaklah dilindungi dan tersedia untuk penilaian atau tindakan serta merta;

ii. Pengauditan juga perlu dibuat ke atas rekod-rekod manual seperti dokumen operasi, nota serah tugas, kelulusan keluar pejabat, memorandum, borang kebenaran, surat kuasa, senarai inventori dan kemudahan akses log. Ini adalah kerana dalam kes-kes tertentu, dokumen ini diperlukan untuk menyokong *audit trail* sistem komputer; dan

iii. Keseluruhannya, sistem pengauditan ini adalah penting dalam menjamin akauntabiliti.

Antara lain, sistem ini dapat dirujuk bagi menentukan perkara-perkara berikut:

i. Mengesan pematuhan atau perlanggaran keselamatan;
ii. Menyediakan catatan peristiwa mengikut urutan masa yang boleh digunakan untuk mengesan punca berlakunya perlanggaran keselamatan; dan
iii. Menyediakan bahan bukti bagi menentukan sama ada berlakunya perlanggaran keselamatan.

f. Pematuhan

Dasar Keselamatan ICT MPP hendaklah dibaca, difahami dan dipatuhi. Pematuhan adalah merupakan prinsip penting dalam menghindar dan mengesan sebarang perlanggaran Dasar yang boleh membawa ancaman kepada keselamatan ICT. Pematuhan kepada Dasar Keselamatan ICT MPP boleh dicapai melalui tindakan berikut:

i. Mewujudkan proses yang sistematik khususnya dalam menjamin keselamatan ICT untuk memantau dan menilai tahap pematuhan langkah-langkah keselamatan yang telah dikuatkuasakan;

ii. Merumuskan pelan pematuhan untuk menangani sebarang kelemahan atau kekurangan langkah-langkah keselamatan ICT yang dikenal pasti;

iii. Melaksanakan program pemantauan keselamatan secara berterusan untuk memastikan standard, prosedur dan garis panduan keselamatan dipatuhi; dan

iv. Menguatkuasakan amalan melaporkan sebarang peristiwa yang mengancam keselamatan ICT dan seterusnya mengambil tindakan pembetulan.

g. Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Antara lain, pemulihan boleh dilakukan melalui tindakan-tindakan berikut:-

i. Mewujudkan, merumuskan dan menguji Pelan Pemulihan Bencana/ kesinambungan perkhidmatan– (*Disaster Recovery Plan/ Business Continuity Plan*); dan

ii. Mengamalkan langkah-langkah membuat salinan data dan lain-lain amalan terbaik dalam penggunaan ICT seperti menghapuskan virus, langkah-langkah pencegahan kebakaran dan amalan *clear desk*.

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 mekanisme keselamatan, dapat menjamin keselamatan yang maksimum. Prinsip saling bergantung meliputi beberapa peringkat di mana di tahap minimum, mengandungi langkah-langkah berikut:-

i. Sambungan kepada Internet – Semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui mekanisme pusat untuk mengurus, menguatkuasa dan mengawas sebarang bahaya keselamatan. Melalui sistem ini, semua trafik dalaman hendaklah melalui *gateway firewall* yang diurus secara berpusat. Semua trafik dari luar ke dalam hendaklah juga melalui laluan ini atau melalui kumpulan modem yang dikawal secara berpusat. Dengan itu, penggunaan modem dalaman tidak dibenarkan;

ii. *Backbone* Rangkaian – *Backbone* rangkaian akan hanya mengendalikan trafik yang telah dikod untuk meminimumkan intipan;

iii. Rangkaian Jabatan – Semua rangkaian jabatan akan dihubungkan ke *backbone* melalui *firewall* yang mana akan pula mengekod semua trafik di antara rangkaian jabatan dengan rangkaian di peringkat yang seterusnya atau pusat data; dan

iv. Pelayan Jabatan – Semua data dan maklumat yang kritikal atau sensitif akan hanya disimpan di pelayan jabatan atau di pelayan yang diurus

secara berpusat. Ini akan meminimumkan pendedahan, pengubahan atau kecurian. Semua data dan maklumat sensitif akan dikodkan.

Perkara 1 - Pembangunan dan Penyelenggaraan Dasar Keselamatan ICT

1.1. Dasar Keselamatan ICT

Menerangkan hala tuju, sokongan pengurusan dan peraturan-peraturan bagi mengguna dan melindungi aset ICT selaras dengan keperluan Majlis Perbandaran Pekan dan perundangan yang berkaitan.

1.1.1. Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Yang DiPertua MPP dibantu oleh ahli dari Mesyuarat Pengurusan yang terdiri daripada Ketua Pegawai Maklumat (CIO), semua Ketua Jabatan dan Ketua Bahagian.	**Yang DiPertua**

1.1.2. Penyebaran Dasar

Dasar ini disebarkan kepada semua pengguna MPP iaitu kakitangan, pembekal, pakar runding dan lain-lain.	**Ketua Bahagian ICT, ICTSO**

1.1.3. Penyelenggaraan Dasar

Dasar ini akan disemak dan dipinda dari semasa ke semasa selaras dengan kemajuan teknologi dan perubahan pada prosedur, perundangan dan perkembangan social. Prosedur berhubung penyelenggaraan Dasar Keselamatan ICT MPP adalah: a. kenal pasti dan tentukan perubahan yang diperlukan; b. kemuka cadangan pindaan untuk mendapatkan persetujuan Mesyuarat Pengurusan; c. perubahan yang telah dipersetujui oleh mesyuarat akan dimaklumkan	**Ketua Bahagian ICT, ICTSO**

kepada semua pengguna; d. dasar ini hendaklah dikaji dari masa ke masa.	

1.1.4. Pengecualian Dasar

Dasar Keselamatan ICT MPP digunapakai oleh semua pengguna ICT MPP dan tiada pengecualian diberikan.	**Semua**

Perkara 2 - Organisasi Keselamatan

2.1. Struktur Organisasi Dalaman

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT MPP.

2.1.1. Yang DiPertua

Peranan dan tanggungjawab Yang DiPertua adalah seperti berikut : a. memastikan semua pengguna memahami peruntukan-peruntukan yang telah digariskan di bawah Dasar Keselamatan ICT MPP; b. memastikan semua pengguna mematuhi Dasar Keselamatan ICT MPP; c. memastikan perlindungan keselamatan adalah mencukupi dari setiap aspek; d. memastikan program keselamatan ICT dilaksanakan	**Yang DiPertua**

2.1.2. Ketua Pegawai Maklumat (CIO)

Ketua Pegawai Maklumat (CIO) bagi MPP ialah Timbalan Yang DiPertua (ICT) MPP. Peranan dan tanggungjawab CIO adalah seperti berikut: a. Membantu Datuk Bandar dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Menentukan keperluan keselamatan ICT; c. Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT MPP serta pengurusan risiko dan pengauditan; dan	**CIO**

d. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MPP.	
2.1.3. Ketua Bahagian ICT	
Peranan dan tanggungjawab Ketua Bahagian ICT adalah seperti berikut: a. membantu Datuk Bandar dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MPP; c. Menentukan kawalan akses pengguna terhadap aset ICT MPP; d. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO; dan e. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MPP. f. Membangun dan menyelaras pelaksanaan program mengenai keselamatan ICT. g. Koordinator Pengurusan Kesinambungan Perkhidmatan (Koordinator PKP) MPP.	**Pengarah Jabatan ICT**
2.1.4. Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) bagi MPP ialah Pegawai Teknologi Maklumat dari Jabatan Teknologi Maklumat dan Komunikasi MPP. Peranan dan tanggungjawab ICTSO adalah a. Membantu mengurus keseluruhan program-program keselamatan ICT MPP; b. Membantu menguatkuasakan pelaksanaan Dasar Keselamatan ICT MPP;	**ICTSO**

c. Membantu memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MPP kepada semua pengguna; d. Menjalankan pengurusan risiko; e. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPP berdasarkan hasil penemuan dan menyediakan laporan mengenainya; f. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; g. Melaporkan insiden keselamatan ICT kepada Ketua Bahagian ICT MPP dan memaklumkannya kepada CIO; h. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan i. Membantu menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT. j. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
2.1.5 Pentadbir Sistem ICT	
Pentadbir Sistem bagi MPP ialah Ketua Bahagian dan PPTM di 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,	**Pentadbir Sistem ICT, PPTM**

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 MPP; c. Memantau aktiviti capaian harian sistem aplikasi pengguna; d. Menjaga kerahsiaan konfigurasi sistem aplikasi dan aset ICT MPP e. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; f. Menganalisis dan menyimpan rekod jejak audit; g. Menyediakan laporan mengenai aktiviti capaian secara berkala; dan h. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	
2.1.6. Pengguna	
Peranan dan tanggungjawab pengguna adalah: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPP; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat MPP; d. Melaksanakan langkah-langkah perlindungan seperti berikut :- menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; memeriksa maklumat dan menentukan ia tepat dan lengkap dar	**Semua**

semasa ke semasa; menjaga kerahsiaan kata laluan; mematuhi prosedur, langkah dan garis panduan keselamatan yang ditetapkan; memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; e. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; f. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MPP sebagaimana **Lampiran 1**.	
2.1.7. Mesyuarat Pengurusan MPP	
Mesyuarat Pengurusan bertanggungjawab dalam keselamatan ICT. Keanggotaan adalah seperti berikut: Pengerusi : Yang DiPertua MPP Ahli : Semua Ketua Jabatan Semua Ketua Bahagian	**Mesyuarat Pengurusan**

Peranan : a. Memperakukan/meluluskan dokumen DKICT MPP; b. Memantau tahap pematuhan keselamatan ICT; c. Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam MPP yang mematuhi keperluan DKICT MPP; d. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; e. Memastikan DKICT MPP selaras dengan dasar-dasar ICT kerajaan semasa; f. Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; g. Membincang tindakan yang melibatkan pelanggaran DKICT MPP; dan h. Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	

2.1.8. Pihak Ketiga

Perkara yang perlu dipatuhi oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain) bagi memastikan penggunaan maklumat dan kemudahan proses maklumat termasuk yang berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPP; 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. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah	**CIO, Ketua Bahagian ICT,** **ICTSO,** **Pentadbir Sistem ICT** **dan** **Pihak Ketiga**

dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT MPP; ii. Tapisan Keselamatan iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. e. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MPP sebagaimana **Lampiran 1**.	

Perkara 3 - Pengurusan Aset

3.1 Akauntabiliti Aset

Untuk memberi perlindungan keselamatan yang bersesuaian ke atas semua aset ICT Majlis Perbandaran Pekan.

3.1.1. Inventori Aset

Memastikan semua aset ICT MPP 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 MPP; 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.	**Pemegang Inventori, Semua**

3.2. Pengelasan dan Pengendalian Maklumat

Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

3.2.1. Pengelasan Maklumat

Maklumat hendaklah dikelaskan dan mempunyai peringkat keselamatan	

sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan iaitu a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	**Semua**
3.2.2 Pengendalian Maklumat	
Langkah-langkah keselamatan perlu diambil kira ketika mengendalikan maklumat seperti mengumpul, menghantar, menyimpan, memproses, menyampai, menukar dan ketika memusnah maklumat. Langkah-langkah keselamatan yang perlu diambil adalah: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menjaga kerahsiaan kata laluan; d. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; e. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; f. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; dan g. Menentukan maklumat sedia untuk digunakan	**Semua**

Perkara 4 - Keselamatan Sumber Manusia

4.1. Keselamatan Sumber Manusia Dalam Tugas Harian

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

4.1.1. Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan MPP serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MPP 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 dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	**Semua**

4.1.2. Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan MPP serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan	**Semua**

perundangan dan peraturan yang ditetapkan oleh MPP; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MPP 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 undangundang ke atas pegawai dan kakitangan MPP serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MPP; dan d. Memantapkan pengetahuan berkaitan dengan penggunaan asset 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 merujuk kepada Bahagian Sumber Manusia, Jabatan Khidmat Pengurusan MPP.	
4.1.3 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan semua aset ICT dikembalikan kepada MPP 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 MPP dan/atau terma perkhidmatan.	**Semua**

4.1.4. Perakuan Akta Rahsia Rasmi

Kakitangan MPP yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	**Semua**

.

Perkara 5 - Keselamatan Fizikal Dan Persekitaran

5.1. Keselamatan Kawasan

Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan.

5.1.1. Kawalan Kawasan

Kawalan fizikal kawasan adalah bertujuan untuk menghalang akses, mengesan dan mencegah cubaan menceroboh. Antara langkah-langkah keselamatan fizikal adalah; a. Lokasi hendaklah di kenal pasti dengan jelas. b. Lokasi hendaklah diprkukuhkan seperti dinding, siling, tingkap dan pintu serta dikunci untuk mengawal kemasukan; c. Memasang alat penggera atau kamera tertutup; d. Menghadkan 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; i. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan tempat-tempat yang memerlukan kawalan. j. Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana;	**Yang** **DiPertua, CIO,** **Pengarah Jabatan ICT,** **ICTSO**

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.	
5.1.2. Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Setiap pengguna MPP hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Setiap pelawat hendaklah mendaftar dan mendapatkan Pas Keselamatan di lobi dan Pas dikembalikan semula selepas tamat lawatan; c. Semua pas keselamatan hendaklah diserahkan balik kepada Bahagian Sumber Manusia, Jabatan Khidmat Pengurusan apabila kakitangan berhenti atau bersara; d. Kehilangan pas mestilah dilaporkan dengan segera;	**Semua,** **Pelawat**
5.1.3. Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang aksesnya dihadkan kepada pegawai-pegawai yang diberi kuasa sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di MPP adalah bilik Yang DiPertua, Bilik Timbalan Yang DiPertua, bilik-bilik Pengarah dan Pegawai, Bilik Fail, Bilik Komputer dan Pusat Data. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja : Secara umumnya;	**Semua**

a. Peralatan ICT di dalam kawasn larangan hendaklah dijaga dan dikawal supaya sentiasa dalam keadaan selamat, baik dan boleh digunakan. b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai. c. Semua penggunaan peralatan yang melibatkan penghantaran, pengemaskinian dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Pengarah Jabatan.	

5.2. Keselamatan Peralatan

Melindungi peralatan ICT MPP dari kehilangan dan perkara-perkara yang boleh membahayakan.

5.2.1 Peralatan ICT

Dalam memastikan peralatan ICT dikawal dan dijaga dengan baik, perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Pengguna hendaklah bertanggungjawa menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; b. Pengguna hendaklah memastikan semua perkakasan disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; c. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa	**Semua**

kebenaran;

d. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan serta membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;

e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

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

g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

h. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT atau Juruteknik untuk di baik pulih;

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

j. 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;

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

k. Peralatan ICT yang hendak dibawa keluar dari premis MPP, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan;

l. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan

Pegawai Aset dengan segera; m. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; n. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT; o. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; p. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; q. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT / Juruteknik; r. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; s. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; t. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan u. Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
5.2.2. Media Storan	
Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah	**Semua**

terjamin dan selamat : a. penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; c. penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu dan dihapuskan dengan teratur dan selamat; d. Pergerakan media storan hendaklah direkodkan; e. Pengguna bertanggungjawab terhadap keselamatan maklumat dalam storan mudah alih seperti *thumbdrive* atau *external harddisk* . f. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; 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.	
5.2.3. 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	**Semua**

c. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	
5.2.4. Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan di MPP; b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Ketua Bahagian ICT; c. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-rom*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	**Semua**
5.2.5. Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan agar tidak bermasalah bagi kebolehsediaan, kerahsiaan dan integrity. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; d. Semua penyelenggaraan mestilah mendapat kebenaran daripada pegawai.	**Pegawai Aset, Jabatan ICT**

5.2.6. Perkakasan Untuk Kegunaan Di Luar Pejabat	
Langkah-langkah yang perlu dipatuhi bagi perkakasan yang dibawa keluar dari permis MPP adalah seperti dibawah; a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan. c. Peralatan perlu dilindungi dan dikawal sepanjang masa;	**Semua**
5.2.7 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MPP dan ditempatkan di MPP. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MPP. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan dilakukan; 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. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; e. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang	**Semua**

telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

f. Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan;

g. Pelupusan peralatan ICT hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa.

Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:

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 komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MPP;

iii. Memindah keluar dari MPP mana-mana peralatan ICT yang hendak dilupuskan;

iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab MPP; 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.

5.3 Keselamatan Persekitaran

Melindungi aset ICT MPP dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

5.3.1. Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada CIO. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g. 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; dan h. Akses kepada saluran *riser* hendaklah sentiasa dikunci.	**Semua**

5.3.2. 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; 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.	**Jabatan ICT dan ICTSO**

5.3.3 Kabel

Kabel komputer hendaklah di lindung kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; dan c. Melindung laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*. d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	**Jabatan ICT, ICTSO**

5.3.4. Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Manual Keselamatan Dan Kesihatan Pekerja MPP; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras.	**Semua pegawai Keselamatan Jabatan**

5.4 Keselamatan Dokumen

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

5.4.1. Dokumen

Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat hendaklah dipatuhi. 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	**Semua**

e. Menggunakan enkripsi (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. f. Kawalan terhadap percetakkan dokumen yang mengandungi maklumat sensitive.	

Perkara 6 - Pengurusan Operasi dan Komunikasi

6.1. Pengurusan Prosedur Operasi

Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

6.1.1. 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. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	**Semua**

6.1.2. Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, perisian dan sistem untuk pemprosesan maklumat serta prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Kerja-kerja memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen dan sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan dengan aset ICT berkenaan serta mematuhi spesifikasi perubahan yang telah ditetapkan; c. Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat.	**Semua**

6.1.3. 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, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	**Pengarah Jabatan ICT dan ICTSO**

6.2. Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

6.2.1. 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 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**

6.3. Perancangan dan Penerimaan Sistem	
6.3.1. Perancangan Kapasiti	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. 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. b. 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**
6.3.2. 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**
6.4. Perisian Berbahaya	
6.4.1. Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) untuk mengesan perisian atau program berbahaya serta mengesan aktiviti yang tidak diingini; b. Menggunakan perisian yang berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Mengimbas semua perisian atau sistem dengan anti virus;	**Semua**

d. Mengemas kini *pattern* anti virus yang terkini; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. 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; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
6.4.2 Perlindungan dari Mobile Code	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	**Semua**
6.5 *Housekeeping*	
6.5.1 *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	**Semua**

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 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.	
6.6. Pengurusan Rangkaian	
6.6.1. 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. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh	**Jabatan ICT**

Pentadbir Sistem ICT; f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MPP; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MPP; i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan MPP adalah tidak dibenarkan; k. Semua pengguna hanya dibenarkan menggunakan rangkaian MPP sahaja dan penggunaan modem adalah dilarang sama sekali; dan l. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.	
6.7. Pengurusan Media	
6.7.1. Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	**Semua**
6.7.2. Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;	**Semua**

b. Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; c. Menghadkan 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 b. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	
6.7.3. Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	**Semua**
6.8. Pengurusan Maklumat	
6.8.1. 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	**Semua**

di antara MPP dengan agensi luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MPP; dan d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	
6.8.2. Mel Elektronik (E-mel)	
Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MPP sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Sebarang penghantaran dokumen rasmi hendaklah menggunakan e-mail rasmi Majlis. c. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; d. Semua e-mail hendaklah melalui prosess scan untuk memastikan e-mail yang diterima atau dihantar tidak mempunyai virus. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; e. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan serta mengemaskini *mailbox* masing-masing; f. Pengguna dinasihatkan tidak membuka e-mail yang mencurigakan. g. Pengguna hendaklah menentukan tarikh dan masa sistem komputer	**Semua**

adalah tepat; h. Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".	
6.9. Perkhidmatan E-Dagang (Electeronic Commerce Services)	
6.9.1. E-Dagang	
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.	**Semua**
6.9.2. 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	**Semua**

terlebih dahulu; dan c. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	
6.10. Pemantauan	
6.10.1. Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT MPP; 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**
6.10.2. Jejak Audit	
Jejak audit hendaklah mengandungi maklumat-maklumat berikut:	**Semua**

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 b. 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 danpengubahsuaian yang tidak dibenarkan.	
6.10.3. Sistem Log	
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: a. Mengadakan sistem log untuk merekod semua aktiviti harian pengguna; b. Menyemak dan meneliti sistem log untuk 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**

6.10.4. 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 MPP atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

Perkara 7- Kawalan Capaian

7.1. Dasar Kawalan Capaian

Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan Aset ICT MPP.

7.1.1. 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.	**Pentadbir Sistem ICT,** **Semua**

7.2. Capaian Pengguna

7.2.1. Akaun Pengguna

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Akaun yang diperuntukkan oleh MPP sahaja boleh digunakan b. Akaun pengguna mestilah unik;	**Semua**

c. Pemilik akaun pengguna bukanlah hak mutlak pengguna dan ia tertakluk kepada peraturan MPP. Akaun boleh ditarik balik jika pengguna melanggar peraturan. d. Tidak semua pengguna boleh capai semua peringkat maklumat. Terdapat peringkat dalam capaian maklumat dengan dikawal menggunakan akaun. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; e. Penggunaan akaun milik orang lain tidak dibenarkan. f. Akaun pengguna boleh dibekukan dan ditamatkan 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; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
7.2.2 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 MPP 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 ditetapkan sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksana khusus;	**Semua dan Pentadbir Sistem ICT**

d. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. Kata laluan *windows* dan *screen saver* disyorkan 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; i. Disyorkan 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 lama digunakan.	
7.2.3. *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* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja atau di paparan skrin apabila kakitangan tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Gunakan kemudahan *password* b. Log keluar apabila meninggalkan komputer;	**Semua**

c. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci; d. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	
7.3. Kawalan Capaian Rangkaian	
7.3.1. Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MPP, rangkaian agensi lain dan rangkaian awam; b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	**Pentadbir Sistem ICT dan ICTSO**
7.3.2. Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan Internet di MPP hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MPP; b. Kaedah *Content Filtering* boleh digunakan bagi mengawal akses	**Pentadbir Rangkaian**

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;

d. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;

e. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengarah/ pegawai yang diberi kuasa;

f. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;

g. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet;

h. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;

i. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MPP;

j. 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;

k. Penggunaan modem atau 'broadband' untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan

l. 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 ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah. Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".	
7.4. Kawalan Capaian Sistem Pengoperasian	
7.4.1. 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 MPP menyokong perkara-perkara berikut: a. Mengesahkan pengguna yang dibenarkan; b. Mewujudkan jejak audit ke atas semua capaian sistem	**Pentadbir Sistem ICT dan ICTSO**

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;
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. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.

7.4.2. Kad Pintar

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan;
b. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain;
c. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan disyorkan untuk disekat; dan
b. (d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Jabatan ICT, MPP.

7.5. Kawalan Capaian Aplikasi dan Maklumat	
7.5.1. Capaian Maklumat dan Sistem Aplikasi	
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. Mengehadkan capaian sistem dan aplikasi kepada minima tiga (3) kali percubaan adalah disyorkan. Sekiranya gagal, akaun atau kata laluan pengguna boleh disekat; d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	**Pentadbir Sistem ICT,** **ICTSO**
7.6. Peralatan Mudah Alih dan Kerja Jarak Jauh	
7.6.1. Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	**Semua**

7.6.2. Kerja Jarak Jauh

Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	**Semua**

Perkara 8 – Perolehan, Pembangunan dan Penyelenggaraan Aplikasi

8.1. Keselamatan Dalam Membangunkan Sistem dan Aplikasi

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

8.1.1. Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: 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 sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	**Pemilik Sistem, Pegawai ICT, ICTSO**

8.1.2. Pengesahan Data Input dan Output

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	**Sistem ICT**

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.	
8.2. Kawalan Kriptografi	
8.2.1 Enkripsi	
Pengguna disyorkan membuat enkripsi (encryption) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	**Semua**
8.2.2. Tandatangan Digital	
Penggunaan tandatangan digital adalah perlu dalam menguruskan transaksi maklumat rahsia rasmi secara elektronik.	**Semua**
8.2.3. 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**
8.3. Keselamatan Fail Sistem	
8.3.1. Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti 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	**Pemilik Sistem dan Pentadbir Sistem ICT**

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 b. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	
8.4. Keselamatan Dalam Proses Pembangunan dan Sokongan	
8.4.1. 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. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e. Menghalang sebarang peluang untuk membocorkan maklumat.	**Pemilik Sistem dan Pentadbir Sistem ICT**

8.4.2. 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 MPP.	**Jabatan ICT dan Pentadbir Sistem ICT**

8.5 Kawalan Teknikal Keterdedahan (*Vulnerability*)

8.5.1. Kawalan dari Ancaman Teknikal

Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem 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.	

Perkara 9 – Pengurusan Pengendalian Insiden Keselamatan

9.1. Mekanisme Pelaporan Insiden Keselamatan ICT

Memastikan semua insiden dikendalikan dengan cepat dan berkesan serta memastikan sistem ICT MPP dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej Majlis dan sistem penyampaian perkhidmatan awam.

9.1.1. 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 dengan kadar segera. Disyorkan juga insiden keselamatan ICT dilaporkan kepada pihak GCERT MAMPU: a. Maklumat didapati hilang, 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; 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 yang tidak dijangka. Prosedur pelaporan insiden keselamatan ICT berdasarkan:	**Semua**

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.	
9.2. Pengurusan Maklumat Insiden Keselamatan ICT	
9.2.1. 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 MPP. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Tindakan menangani insiden keselamatan ICT perlu dilakukan dengan cepat, teratur dan berkesan; prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a. Mengenal pasti jenis insiden keselamatan ICT b. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; c. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; d. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; e. Menyediakan tindakan pemulihan segera; dan	**ICTSO**

f. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	

Perkara 10 - Pengurusan Kesinambungan Perkhidmatan

10.1. Dasar Kesinambungan Perkhidmatan

Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

10.1.1. 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 JKICT MPP. 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; f. Membuat *backup*; dan g. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	**Semua**

Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkaraberikut:

a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
b. Senarai personel MPP 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 diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran 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 mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. MPP hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

Perkara 11 – Pematuhan

11.1. Pematuhan dan Keperluan Perundangan

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT MPP

11.1.1. Pematuhan Dasar

Setiap kakitangan MPP perlu membaca, memahami dan mematuhi Dasar Keselamatan ICT MPP dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa; Semua aset ICT di MPP termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT MPP selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber MPP.	**Semua**

11.1.2. Pematuhan dengan Dasar, Piawaian dan Keperluan Kawalan Teknikal Keterdedahan

Semua prosedur keselamatan dalam bidang tugas masing-masing perlu mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT. Kawalan ancaman teknikal keterdedahan perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi	

11.1.3. 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.	
11.1.4. Keperluan Perundangan	
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MPP: a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan; c. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook*(MyMIS); d. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi- Agensi Kerajaan; f. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; g. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; h. 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; i. Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan	**Semua**

yang bertarikh 1 Jun 2007; j. Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-agensi Kerajaan yang bertarikh 23 November 2007; k. Surat Pekeliling Am Bilangan 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK); l. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan pertama)- Tatacara Penyediaan, Penilaian dan Penerimaan Tender; m. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan; n. Akta Tandatangan Digital 1997; o. Akta Rahsia Rasmi 1972; p. Akta Jenayah Komputer 1997; q. Akta Hak cipta (Pindaan) Tahun 1997; r. Akta Komunikasi dan Multimedia 1998; s. Perintah-Perintah Am; t. Arahan Perbendaharaan; u. Arahan Teknologi Maklumat 2007; v. Akta Perlindungan Data Peribadi	
11.1.5. Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT MPP boleh dikenakan tindakan tatatertib.	

Lampiran 1

MAJLIS PERBANDARAN PEKAN

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT MPP

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Jabatan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT MPP; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

(**JAMAIAH AHMAD**)
b.p Yang DiPertua
Majlis Perbandaran Pekan

Tarikh:

Majlis Perbandaran Pekan

DASAR KESELAMATAN ICT MPP

SETIAP WARGA KERJA MPP MESTI
MEMAHAMI DAN MEMATUHI SEMUA
PERATURAN MENGENAI
PENGGUNAAN PERKAKASAN DAN PERISIAN (ASET)
TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT) MPP

BAGI

MEMASTIKAN KESINAMBUNGAN DALAM SEMUA URUSAN DI MPP

UNTUK

MENGHASILKAN PERKHIDMATAN YANG TERBAIK

DISAHKAN OLEH :

YANG DIPERTUA
MAJLIS PERBANDARAN PEKAN
01/11/2023

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MPP	3.0	01/11/2023	82/82