KEMENTERIAN INDUSTRI UTAMA

DASAR KESELAMATAN ICT

KEMENTERIAN INDUSTRI UTAMA

Versi 3.0

DASAR KESELAMATAN ICT

Versi 3.0

2018 - 2020

KEMENTERIAN INDUSTRI UTAMA

BAHAGIAN PENGURUSAN MAKLUMAT (BPM)

SEJARAH DOKUMEN

Tarikh	Versi	Kelulusan	Tarikh Kuatkuasa
11 Mac 2010	1.0	JPICT Bil. 1/2010	11 Mac 2010
21 Oktober 2013	2.0	PENGURUSAN Bil. 11/2013	21 Oktober 2013
6 Ogos 2018	3.0	JPICT Bil.2/2018	6 Ogos 2018

JADUAL PINDAAN

Tarikh	Versi	Butiran Pindaan
3 Mac 2015	2.0	Pindaan terhadap perkara 020103 Pegawai Keselamatan ICT (ICTSO) bagi MPI ialah Ketua Penolong Setiausaha (KPSU), Bahagian Pengurusan Maklumat (BPM), MPI.
24 April 2018	3.0	Penambahan perkara 030203, 030204, 030205, 030206 dan 030207 iaitu Keselamatan Rahsia Rasmi Dalam Persekitaran Teknologi Maklumat dan Komunikasi (ICT).
3 Ogos 2018	3.0	Pindaan terhadap perkara 070301 c) "Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus".

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT (DKICT) MPI (*Ministry of Primary Industries)* mengandungi 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 MPI.

OBJEKTIF

Dasar Keselamatan ICT MPI diwujudkan untuk menjamin kesinambungan perkhidmatan MPI dengan meminimumkan kesan insiden keselamatan ICT.

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi MPI. Ia hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT MPI ialah seperti berikut:

a. Memastikan kelancaran operasi MPI dan meminimumkan kerosakan atau kemusnahan;
b. Melindungi kepentingan pihak-pihak yang terikat dengan sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
c. Mencegah salah guna atau kecurian aset ICT MPI.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Kawalan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin tahap ketersediaan keselamatan kerana cara ancaman dan pencerobohan 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 MPI dari capaian tanpa kuasa yang sah;
b. Menjamin setiap maklumat adalah tepat dan sahih;
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 MPI merangkumi perlindungan ke atas semua bentuk maklumat elektronik yang bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehcapaian 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 sentiasa dikemaskini. 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 yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Aset ICT terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT MPI 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 MPI, perkhidmatan dan pelanggan.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT MPI ini merangkumi perlindungan semua bentuk maklumat MPI yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan. 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. 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 ialah seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada MPI;

c. Perkhidmatan

Perkhidmatan atau sistem yang menyokong kepada 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 visi MPI. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod, 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 bagi mencapai misi dan objektif MPI.

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.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT MPI 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 untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Garis Panduan Keselamatan MPI.

b. Hak akses minimum

Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, 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. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu 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 ianya 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 dari diketahui umum.

d. Pengasingan

Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

e. Pengauditan

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*;

f. Pematuhan

Dasar Keselamatan ICT MPI hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

g. 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 aktiviti penduaan dan mewujudkan pelan pemulihan bencana/ kesinambungan perkhidmatan; dan

h. Saling Bergantungan

Setiap prinsip di atas adalah saling lengkap-melengkapi dan bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

BIDANG 01 - PEMBANGUNAN DAN PENYELENGGARAAN DASAR

0101 DASAR KESELAMATAN ICT

Objektif

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan fungsi-fungsi utama MPI dan perundangan yang berkaitan.

010101 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha (KSU) MPI dan dibantu oleh Timbalan Ketua Setiausaha, semua Setiausaha Bahagian dan Ketua Unit serta Pegawai Keselamatan ICT.

Tindakan: KSU

010102 Penyebaran Dasar

Dasar ini hendaklah disebarkan dan dipatuhi oleh semua pengguna aset ICT MPI termasuk kontraktor dan pihak ketiga yang berurusan atau memberikan perkhidmatan ICT kepada MPI.

Tindakan: ICTSO

010103 Penyelenggaraan Dasar

Dasar ini hendaklah disemak sekurang-kurangnya sekali (1) setahun dan dipinda mengikut keperluan selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial.

Tindakan: ICTSO

010104 Pengecualian Dasar

Dasar ini adalah terpakai kepada semua pengguna ICT MPI dan tiada pengecualian diberikan.

Tindakan: Semua

BIDANG 02 - ORGANISASI KESELAMATAN

0201 ORGANISASI KESELAMATAN MPI

Objektif

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

020101 Ketua Setiausaha (KSU) MPI

KSU MPI adalah berperanan dan bertanggung-jawab dalam perkara-perkara berikut:

a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MPI;
b. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MPI;
c. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; dan
d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT MPI.

020102 Ketua Pegawai Maklumat (CIO)

Ketua Pegawai Maklumat (CIO) bagi MPI ialah Timbalan Ketua Setiausaha Sektor Pengurusan dan Strategik (TKSUP), MPI.

Peranan dan tanggungjawab CIO adalah seperti berikut:

a. Membantu KSU dalam melaksanakan tugas-tugas yang melibatkan ICT dan keselamatan ICT;
b. Meluluskan semua prosedur, standard, dan garispanduan keselamatan ICT MPI;
c. Meluluskan perlaksanaan atau aktiviti keselamatan ICT MPI;
d. Menentukan keperluan keselamatan ICT;
e. Meluluskan pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT MPI serta pengurusan risiko dan pengauditan; dan
f. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MPI.

020103 Pegawai Keselamatan ICT (ICTSO)

Pegawai Keselamatan ICT (ICTSO) bagi MPI ialah Ketua Penolong Setiausaha (KPSU), Bahagian Pengurusan Maklumat, MPI.

Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

a. Mengurus keseluruhan program-program keselamatan ICT MPI;
b. Menguatkuasakan pelaksanaan Dasar Keselamatan ICT MPI;
c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MPI kepada semua pengguna;

d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MPI;
e. Menjalankan pengurusan risiko;
f. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MPI 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;
h. Melaporkan insiden keselamatan ICT kepada 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;
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; dan
l. Koordinator Pengurusan Kesinambungan Perkhidmatan (Koordinator PKP) MPI.

020104 Pengurus ICT

Pengurus ICT bagi MPI ialah Setiausaha Bahagian (SUB), Bahagian Pengurusan Maklumat MPI.

Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:

a. Mengkaji, menguji dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MPI;

b. Membuat penilaian keberkesanan kawalan keselamatan ICT;
c. Meluluskan prosedur teknikal perlaksanaan kawalan keselamatan;
d. Menentukan kawalan akses pengguna terhadap aset ICT MPI;
e. Memastikan semua dasar keselamatan ICT di patuhi;
f. Mengambil tindakan terhadap pencerobohan, ancaman atau penemuan mengenai kelemahan keselamatan ICT; dan
g. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MPI.

020105 Pentadbir Sistem ICT

Pentadbir Sistem ICT bagi MPI ialah Penolong Setiausaha (PSU) ICT yang dilantik untuk mentadbir dan menguruskan sistem-sistem ICT iaitu:

a. Pentadbir Rangkaian;
b. Pentadbir Rangkaian Wireless;
c. Pentadbir Pangkalan Data;
d. Pentadbir Laman Web (*Web Master*);
e. Pentadbir Pusat Data (*Server Farm*);
f. Semua Pentadbir Sistem Aplikasi;

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 MPI;

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, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.

020106 Pekhidmat MPI

Pekhidmat MPI adalah pegawai-pegawai yang dilantik oleh MPI secara tetap, kontrak dan sambilan.

Pekhidmat mempunyai peranan dan tanggung-jawab seperti berikut:

a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPI;
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 MPI dan menjaga kerahsiaan maklumat MPI;
e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;

f. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan
g. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MPI sebagaimana di **LAMPIRAN 1**.

020107 Jawatankuasa Keselamatan ICT (JKKICT) MPI

Jawatankuasa Keselamatan ICT (JKKICT) adalah jawatankuasa yang bertanggung-jawab ke atas segala perancangan, pelaksanaan, pemantauan dan strategi keselamatan ICT MPI. Mesyuarat perlu diadakan sekurang-kurangnya setahun (1) sekali.

Di MPI, Jawatankuasa Pemandu ICT (JPICT) atau Mesyuarat Pengurusan juga berperanan sebagai JKKICT MPI.

Keanggotaan JKKICT MPI adalah seperti berikut:

a. Pengerusi : KSU MPI
b. Ahli :
    i. Timbalan Ketua Setiausaha
    ii. Ketua Pegawai Maklumat (CIO)
    iii. Semua Setiausaha Bahagian dan Ketua Unit atau wakil
    iv. ICTSO

Urus Setia bagi JKKICT MPI ialah Urusetia JPICT/Jawatankuasa Kerja ISMS MPI atau ICTSO .

Bidang kuasa :

a. Memperakui/meluluskan dokumen DKICT MPI;
b. Meluluskan tahap pematuhan keselamatan ICT;

c. Meluluskan teknologi yang bersesuaian untuk dilaksanakan di dalam memperkukuhkan keselamatan ICT;
d. Meluluskan cadangan penyelesaian terhadap keperluan keselamatan ICT;
e. Memastikan DKICT MPI selaras dengan dasar-dasar ICT kerajaan semasa;
f. Meluluskan laporan dan membincangkan hal-hal keselamatan ICT semasa;
g. Meluluskan tindakan yang melibatkan pelanggaran DKICT MPI; dan
h. Meluluskan tindakan yang perlu diambil mengenai sebarang insiden.

020108 Pasukan Tindak Balas Insiden Keselamatan ICT MPI (CERT)

Pengguna wajib melaporkan sebarang insiden ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT MPI mengikut prosedur yang ditetapkan apabila berlaku insiden yang menjejaskan keselamatan ICT.

Pasukan Tindak Balas Insiden Keselamatan ICT MPI adalah pasukan yang akan bertindak semasa berlaku insiden keselamatan di MPI.

Peranan dan tanggungjawab CERT adalah seperti berikut :

a. Menerima dan mengesan aduan keselamatan ICT serta 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 baik pulih minimum;

d. Menasihati CIO untuk mengambil tindakan pemulihan dan pengukuhan;
e. Memberikan khidmat nasihat dan amaran awal insiden; dan
f. Menyebarkan maklumat berkaitan pengukuhan keselamatan ICT kepada pihak yang berkepentingan.

0202 PIHAK KETIGA

Objektif:

Menjamin keselamatan semua aset ICT yang digunakan oleh Pembekal, Kontraktor, Pakar Runding dan lain-lain adalah terkawal keselamatannya dan tidak disalahguna.

020201 Keperluan Keselamatan ICT di dalam Kontrak dengan Pihak Ketiga

Perjanjian kontrak dengan pihak ketiga yang berurusan dengan aset ICT perlu bagi memastikan penggunaan maklumat dan kemudahan prosesan maklumat dikawal.

Perkara yang perlu dipatuhi di dalam perjanjian adalah seperti berikut:

a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT MPI;
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 MPI perlu berlandaskan kepada perjanjian kontrak;

e. Memastikan semua syarat-syarat keselamatan dan prosedur dipatuhi dan dinyatakan dengan jelas kepada pihak ketiga;

Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai.

i. Dasar Keselamatan ICT MPI.
ii. Tapisan Keselamatan.
iii. Perakuan Akta Rahsia Rasmi 1972.
iv. Hak Harta Intelek.

Tindakan : Semua

BIDANG 03 - PENGURUSAN ASET

0301 TANGGUNGJAWAB TERHADAP ASET

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MPI.

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 dan dikemas kini;
b. Memastikan maklumat penyelenggaraan aset ICT direkod dan sentiasa dikemas kini;
c. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;
d. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MPI;

e. Semua pergerakan dan peminjaman aset ICT direkod dan dipantau;
f. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan;
g. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan
h. Peraturan bagi pengendalian pelupusan aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan.

Tindakan : PPK , BPM dan Semua

0302 PENGELASAN DAN PENGENDALIAN MAKLUMAT

Objektif:

Memastikan setiap maklumat diberikan tahap perlindungan yang bersesuaian.

030201 Pengelasan Maklumat

Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut Garis Panduan Keselamatan MPI.

Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan seperti berikut:

a. Rahsia Besar;
b. Rahsia;
c. Sulit; atau
d. Terhad.

Tindakan : PPK, Semua SUB dan Ketua Unit

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;
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.

Tindakan : PPK dan Semua

030203 Pengurusan Rahsia Rasmi Dalam Persekitaran ICT

Jabatan yang menguruskan rahsia rasmi dalam persekitaran ICT hendaklah mematuhi tatacara pengurusan rahsia rasmi dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.

Tindakan : Semua

030204 Pengelasan Rahsia Rasmi Dalam Persekitaran ICT

Rahsia rasmi perlu dikelaskan oleh Pegawai Pengelas yang dilantik dibawah Seksyen 2B Akta 88 berdasarkan kandungan, keutamaan dan tahap perlindungan keselamatan maklumat tersebut. Pengelasan rahsia rasmi dalam persekitaran ICT hendaklah mengikut tatacara pengelasan yang ditetapkan oleh Kerajaan.

Sistem aplikasi yang menyimpan maklumat rahsia rasmi perlulah berupaya untuk memberikan tanda keselamatan pada setiap antara muka (*interface*) dan juga pada semua janaan dengan ciri-ciri keselamatan yang bersesuaian dengan peringkat keselamatan dan penilaian risiko.

Tindakan : PPK dan Semua

030205 Pengelasan Semula Rahsia Rasmi Dalam Persekitaran ICT

Rahsia rasmi dalam persekitaran ICT perlulah dikaji dari semasa kesemasa bagi meringankan beban kepada sistem keselamatan secara keseluruhannya. MPI perlu mengambil tindakan untuk mengelaskan semula maklumat rahsia rasmi berdasarkan kepada peruntukan Seksyen 2C Akta 88 sekiranya maklumat berkenaan tidak lagi perlu menjadi rahsia rasmi.

Tindakan : PPK dan Semua

030206 Pengendalian Maklumat Dalam Persekitaran ICT

Penyimpanan rahsia rasmi dalam persekitaran ICT hendaklah dilindungi secara fizikal dan logikal mengikut perkembangan teknologi.

Pengguna kemudahan pengkomputeran bergerak (*mobile computing*) dalam memproses rahsia rasmi diluar pejabat hendaklah memastikan supaya ia sentiasa dilindungi daripada kehilangan dan kerosakan serta maklumat yang terkandung di dalamnya tidak dikrompomi.

Semua hubungan komunikasi MPI seperti e-mel rasmi, *instant messaging*, *web conferencing*, perkongsian sumber, rangkaian tanpa wayar dan seumpamanya perlu dilindungi daripada capaian yang tidak dibenarkan. Maklumat rahsia rasmi hendaklah disediakan dalam bentuk fail kepilan (*attachment*) dan disulitkan (*encrypted*) sebelum dihantar kepada semua.

E-mel yang mengandungi rahsia rasmi hendaklah berkeadaan disulitkan (*to be encrypted*) semasa dihantar dan disimpan serta dinyahsulitkan (*to be decrypted*) oleh penerima yang sah sahaja. Penggunaan e-mel peribadi untuk urusan rahsia rasmi adalah dilarang sama sekali.

Penggunaan pengkomputeran awan (*cloud computing*) seperti perkongsian maklumat, pemprosesan data dan sebagainya bagi tujuan rahsia rasmi tidak dibenarkan sama sekali kecuali pengkomputeran awan yang dibangunkan dan dibenarkan oleh pihak Kerajaan dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.

Tindakan : Semua

030207 Pemusnahan Rahsia Rasmi Dalam Persekitaran ICT

MPI hendaklah mendapatkan khidmat nasihat daripada Ketua Pengarah Keselamatan Kerajaan dan Ketua Pengarah Arkib Negara berhubung dengan pemusnahan maklumat rahsia rasmi sama ada

mempuntai nilai arkib atau tidak, kelulusan Ketua Arkib Negara hendaklah diperoleh terlebih dahulu sebelum rahsia rasmi tersebut dimusnahkan.

Tindakan : PPK

BIDANG 04 - KESELAMATAN SUMBER MANUSIA

0401 KESELAMATAN SUMBER MANUSIA

Objektif:

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

040101 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut:

a. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MPI yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan

b. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.

Tindakan : PSM

040102 Semasa Perkhidmatan

Objektif:

Memastikan semua pekhidmat, kontraktor dan pihak ketiga mempunyai kesedaran terhadap ancaman keselamatan dan sedar akan tanggungjawab bagi memastikan segala dasar keselamatan dilaksanakan di dalam kerja yang dilakukan untuk menurunkan risiko akibat kesilapan manusia.

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan MPI yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan;
b. Memastikan pegawai dan kakitangan MPI serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MPI;
c. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MPI secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa;

d. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan MPI sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MPI; dan

e. 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 merujuk kepada Bahagian Pengurusan Sumber Manusia (PSM).

Tindakan : PSM

040103 Tamat Perkhidmatan atau Pertukaran Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:

a. Memastikan semua aset ICT dikembalikan kepada MPI mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan

b. Membatalkan, mengantung atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MPI dan/atau terma perkhidmatan.

Tindakan : PSM

BIDANG 05 - KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 KESELAMATAN KAWASAN

Objektif:

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

050101 Keselamatan Kawasan Fizikal

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi.

Perkara-perkara yang perlu dipatuhi bergantung kepada hasil penilaian risiko termasuk yang berikut :

a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset;
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. 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. Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan;
j. Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau dan bencana;
k. Menyediakan garis panduan untuk kakitangan yang bekerja di kawasan terhad; dan
l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.

Tindakan : PPK, ICTSO dan CIO

050102 Kawalan Masuk Fizikal

Kawalan Masuk Fizikal perlu dikenal pasti dan dilaksanakan ke atas kawasan yang menempatkan infrastruktur rangkaian dan komunikasi, fasiliti pemprosesan atau tempat penyimpanan maklumat terperingkat.

Keselamatan fizikal termasuk keselamatan perimeter seperti pembinaan dinding, pagar kawalan dan menghadkan jalan keluar masuk ke kawasan berkenaan.

Akses ke kawasan pejabat dan kawasan larangan perlu dikawal bagi memastikan hanya kakitangan atau pihak yang diberi tanggungjawab sahaja dibenarkan masuk.

Tindakan : PPK dan Semua

050103 Kawasan Larangan ICT

Kawasan larangan ditakrifkan sebagai kawasan dimana terdapat aset ICT kritikal yang boleh menjejaskan operasi dan keselamatan maklumat secara keseluruhan jika tidak dikawal.

Kawasan larangan ICT di MPI ialah Bilik Server dan bilik/ruang yang terdapat peralatan ICT kritikal/kabel telekomunikasi (*MDF room/riser*).

Akses kepada kawasan larangan hendaklah dikawal dan kebenaran hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan pihak ketiga adalah dilarang sama 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.

Tindakan : BPM, PPK dan Semua

050104 Perlindungan Kawasan ICT Dari Ancaman Luar Dan Bencana Alam

Kawalan dan perlindungan keselamatan ke atas kawasan ICT perlu mengambilkira ancaman dari perbuatan manusia ataupun bencana alam seperti kebakaran, banjir, gempa bumi dan lain-lain.

Tindakan : BPM, PPK dan Semua

050105 Kawalan Kawasan Penghantaran Barangan dan *Loading Area*

Kawasan penghantaran barangan dan *loading area* hendaklah dikawal dan perlu dipisahkan dari akses terus ke kawasan larangan.

Tindakan : PPK

0502 KESELAMATAN ASET ICT

Objektif:

Melindungi aset ICT dari kehilangan, kerosakan, kecurian aset serta gangguan kepada aset tersebut.

050201 Peralatan dan Perkakasan ICT

Semua aset ICT perlu dijaga dan dikawal dengan baik supaya ianya boleh digunakan sepanjang masa, perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a. Pengguna hendaklah menyemak dan memastikan semua aset ICT di bawah kawalannya berfungsi dengan sempurna;
b. Pengguna bertanggungjawab spenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;
c. Pengguna dilarang sama sekali menambah, memanggil atau mengganti sebarang pekakasan ICT yang telah ditetapkan;
d. Pengguna dilarang 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 disamping melakukan imbasan ke atas media storan yang digunakan;

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

h. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;

i. Peralatan-peralatan kritikal perlu disokong oleh *Uninterrutable 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;

l. Peralatan ICT yang hendak dibawa keluar dari permis MPI perlulah mendapat kelulusan oleh pegawai yang diberikan kuasa dan direkodkan bagi tujuan pemantauan;

m. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera dan laporan polis hendaklah disertakan;

n. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT dan Pegawai Aset MPI;

p. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk dibaik pulih;

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

r. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;

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

t. Pengguna bertanggungjawab terhadap perkakasan, perisisan dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

u. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila meninggalkan pejabat;

v. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan

w. Memastikan suis ditutup bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.

Tindakan : Semua

050202 Media Storan Digital

Media storan digital merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cekera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain.

Media storan digital perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut :

a. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
b. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;
c. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan;
d. Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet;
e. Akses dan pergerakan media storan hendaklah direkodkan;
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.

Tindakan : Semua

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 selanjutnya.

Tindakan : Semua

050204 Media Perisian dan Aplikasi

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MPI;
b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran CIO;
c. Lesen perisian 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 pindaaan mestilah mengikut prosedur yang ditetapkan.

Tindakan : Semua

050205 Utiliti Sokongan

Semua utiliti sokongan perlu berada dalam keadaan terbaik dan mencukupi bagi menyokong sistem beroperasi. Utiliti sokongan ini termasuk bekalan elektrik, air, penghawa dingin, generator, alat komunikasi dan lain-lain.

Tindakan : Semua

050206 Penyelenggaraan Perkakasan

Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti adalah terkawal.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a. Semua perkakasan perlu diselenggara mengikut spesifikasi yang telah 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 pegawai yang diberikan tanggungjawab menjaganya.

Tindakan : Semua

050207 Aset ICT di Luar Premis

Aset ICT seperti storan penyimpanan maklumat, komputer peribadi, *computer tablet*, telefon mudah alih, *smart card*, dokumen atau lain-lain perkakasan yang dibawa keluar premis MPI perlu dilindungi dari risiko keselamatan seperti kecurian, kerosakan dan lain-lain.

Antara perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Aset yang hendak dibawa keluar dari premis perlu mendapat kebenaran;
b. Pegawai adalah bertanggungjawab sepenuhnya ke atas aset yang dibawa keluar;
c. Aset perlu dilindungi dan dikawal sepanjang masa;
d. Maklumat pada aset hendaklah sentiasa dilindungi dengan katakunci; dan
e. Penyimpanan atau penempatan aset mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.

Tindakan : Semua

050208 Pelupusan dan Guna Semula Perkakasan

Pelupusan melibatkan semua aset ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MPI dan ditempatkan di MPI.

Aset ICT yang akan dilupuskan atau diguna semula, terutama yang mengandungi maklumat terperingkat atau perisian yang dilesenkan, perlu diuruskan dengan teratur dan selamat mengikut prosedur pelupusan semasa atau guna semula peralatan yang telah

ditetapkan. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MPI.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Semua kandungan perkakasan khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan atau diguna semula;
b. Pelupusan Aset ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa;
c. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;
d. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;
e. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;
f. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;
g. Peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;
h. Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Inventori; dan
i. 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 MPI;

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

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

Tindakan : PPK dan Semua

0503 KESELAMATAN PERSEKITARAN

Objektif:

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

050301 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa atau mengubahsuai, pembelian hendaklah

dirujuk terlebih dahulu kepada Pegawai Keselamatan Kerajaan dan ICTSO.

Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi :

a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik pencetakan, 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 pencegahan 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 bersesuaian dan berjauhan dari aset ICT;
e. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer;
f. Semua cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;
g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini pelu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan
h. Akses kepada saluran riser hendaklah sentiasa dikunci.

Tindakan : PPK dan Semua

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 kritikal hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;
b. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan/atau penjana (*generator*) hendaklah digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan ; dan
c. Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.

Tindakan : PPK dan BPM

050303 Kabel

Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat terdedah.

Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

a. Menggunakan kabel yang mengikuti 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.

Tindakan : PPK dan BPM

050304 Prosedur Kecemasan Persekitaran

Prosedur kecemasan persekitaran seperti kebakaran, banjir, bencana alam dan lain-lain yang melibatkan persekitaran kawasan ICT terjejas hendaklah di kaji dari masa ke masa.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut :

a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MPI; dan

b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras.

Tindakan : PPK

0504 KESELAMATAN DOKUMEN

Objektif:

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

050401 Dokumen

Perkara-perkara yang perlu dipatuhi adalah seperti yang 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 sepertimana 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.

Tindakan : Semua

BIDANG 06 - PENGURUSAN OPERASI DAN KOMUNIKASI

0601 PENGURUSAN PROSEDUR OPERASI DAN TANGGUNGJAWAB

Objektif:

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

060101 Pengendalian Prosedur Operasi ICT

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a. Semua prosedur pengurusan operasi yang diwujudkan, 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 sekiranya pemprosesan tergendala atau terhenti; dan
c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan, diberikan nombor versi pindaan dan diluluskan oleh Pengurus ICT.

Tindakan : Semua

060102 Kawalan Perubahan

Perubahan yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah dikemukakan oleh pemilik sistem atau pentadbir rangkaian dan komunikasi serta mendapat kebenaran daripada pegawai yang diberi kuasa.

Sebarang perubahan komponen sistem ICT hendaklah mematuhi keperluan yang ditetapkan.

Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a. Pengubahsuaian yang melibatkan perkakasan rangkaian dan komunikasi, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;
b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;
c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan
d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.

Tindakan : Semua

060103 Pengasingan Tugas dan Tanggungjawab

Tugas dan tanggungjawab setiap pegawai perlu ditetapkan dan jelas bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT.

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 membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.

Tindakan : Pengurus ICT dan ICTSO

0602 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK KETIGA

Objektif:

Memastikan penyampaian perkhidmatan pihak ketiga mematuhi tahap keselamatan yang ditetapkan selaras dengan perjanjian perkhidmatan.

060201 Perkhidmatan

Pihak ketiga perlu mematuhi terma dan syarat-syarat berkaitan kawalan keselamatan yang telah ditetapkan dalam perjanjian

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. Pegurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.

Tindakan : Pengurus ICT dan Semua

060202 Pemantauan Perkhidmatan Pihak Ketiga

Perkhidmatan, laporan dan rekod pihak ketiga perlu dipantau, disemak dan diaudit.

Tindakan : Pengurus ICT

0603 PERANCANGAN DAN PENERIMAAN SISTEM

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

060301 Pengurusan Kapasiti

Pengurusan kapasiti perlu dilaksanakan sebelum sistem dibangun dan dilaksanakan dengan mengambilkira keperluan selama 3 tahun.

Tindakan : Pentadbir Sistem ICT

060302 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.

060303 Penerimaan Sistem

Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.

Sijil penerimaan sistem hanya akan dikeluarkan setelah segala ujian penerimaan yang ditetapkan berjaya dilaksanakan sepenuhnya.

Tindakan : Pentadbir Sistem ICT

0604 KAWALAN TERHADAP PERISIAN BERBAHAYA

Objektif:

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya.

060401 Perlindungan Dari Perisian Berbahaya

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Instrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat;
b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa;
c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya;
d. Mengemaskini antivirus dengan *pattern* antivirus 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.

Tindakan : Semua

060402 Kawalan terhadap kod berbahaya (*Malicious Code)*

Perisian atau sistem yang digunakan mesti bebas daripada kod berbahaya (*malicious code)*.

Tindakan : Pentadbir Sistem

060403 Kawalan terhadap *Mobile Code*

Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.

Tindakan : Semua Pentadbir Sistem

0605 *HOUSEKEEPING (BACKUP)*

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 mengikut prosedur yang telah ditetapkan.

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 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.

Tindakan : Pengurus ICT dan Semua Pentadbir Sistem

0606 PENGURUSAN KESELAMATAN RANGKAIAN

Objektif:

Memastikan maklumat dan infrastruktur rangkaian dilindungi.

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 yang 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 Pentadbir Sistem ICT;
f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MPI;
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 MPI;

i. Memasang *Web Content Filtering* pada *Internet Gateway* utuk menyekat aktiviti yang dilarang;

j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan MPI adalah tidak dibenarkan;

k. Semua pengguna hanya dibenarkan menggunakan rangkaian MPI sahaja dan penggunaan modem adalah dilarang sama sekali;

l. Semua peralatan yang hendak disambung kepada rangkaian perlu bebas daripada virus dan mempunyai *antivirus* yang sah;

m. Capaian kepada rangkaian perlu dilaksanakan mengikut kategori yang telah ditetapkan iaitu Intranet, Internet dan DMZ;

n. Peralatan persendirian adalah dilarang untuk capaian kepada rangkaian Intranet MPI;

o. Sistem yang terdapat didalam rangkaian Intranet tidak dibenarkan dicapai dari Internet;

p. Pihak ketiga adalah tidak dibenarkan untuk mencapai rangkaian Intranet kecuali untuk kerja-kerja pembangunan atau penyelenggaraan sistem dengan kebenaran pemilik sistem; dan

q. Capaian kepada *wireless* hendaklah dikawal mengikut kategori pengguna.

Tindakan : Pengurus ICT, ICTSO dan Pentadbir Rangkaian

0607 PENGENDALIAN MEDIA

Objektif:

Melindungi media mudah alih dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan perkhidmatan.

060701 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu dan perlu mematuhi prosedur yang ditetapkan.

Tindakan : Semua

060702 Prosedur Pengendalian Dan Pelupusan Media

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti yang berikut:

a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat ;
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

f. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.

Tindakan : Semua

060703 Keselamatan Sistem Dokumentasi

Sistem dokumentasi perlu disimpan dengan selamat dan dilindungi daripada capaian yang tidak dibenarkan.

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.

Tindakan : Semua

0608 PENGURUSAN PERTUKARAN MAKLUMAT

Objektif:

Memastikan keselamatan pertukaran maklumat dan perisian antara MPI dan agensi luar terjamin.

060801 Pertukaran Maklumat

Pertukaran maklumat mesti mendapat kelulusan dari pihak pengurusan.

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 MPI dengan agensi luar;
c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MPI; dan
d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.

Tindakan : Semua

060802 Pengurusan Mel Elektronik (E-Mel)

Penggunaan e-mel hendaklah mematuhi etika dan peraturan yang ditetapkan oleh MPI.

Pengguna e-mel perlu mematuhi perkara berikut:

a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MPI sahaja boleh digunakan semasa membuat urusan rasmi;
b. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;

c. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

d. Pengguna perlu memastikan saiz e-mel yang dihantar tidak melebihi saiz yang ditetapkan oleh penerima;

e. Pengguna tidak dibenarkan menghantar lampiran (*attachment*) melebihi had yang ditetapkan;

f. Pengguna bertanggungjawab membuat salinan atau *backup* e-mel;

g. Pengguna hendaklah menyemak dan menentukan tarikh dan masa sistem komputer adalah sentiasa tepat;

h. Pengguna perlu memastikan semua e-mel dibaca dan diambil tindakan segera;

i. Pengguna perlu memastikan *mailbox* mempunyai ruangan storan yang cukup terutama untuk transaksi dihujung minggu atau cuti; dan

j. Pengguna bertanggungjawab untuk mengemaskini *mailbox* masing-masing.

Tindakan : Semua

060803 *Business Information System*

Maklumat yang terlibat dalam perkongsian data di antara sistem aplikasi perlu dilindungi.

Tindakan : Semua

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

Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan.

Perkhidmatan E-Dagang melalui kemudahan Internet adalah dibenarkan dengan kawalan bagi menjamin keselamatan maklumat.

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.

Tindakan : Pengurus ICT, Pemilik Sistem dan Semua

060902 Transaksi atas talian

Maklumat yang terlibat dalam transaksi atas talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian dan pendedahan yang tidak dibenarkan.

Tindakan : Pemilik Sistem dan Pentadbir Sistem

060903 Maklumat Capaian Umum

Maklumat yang dipaparkan perlu mempunyai tahap integriti yang tinggi dan dilindungi dari pindaan yang tidak dibenarkan.

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti yang 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.

Tindakan : Pentadbir Laman Web dan Semua

0610 PEMANTAUAN

Objektif:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

061001 Pengauditan dan Forensik ICT

Pentadbir Sistem mestilah bertanggungjawab mengesan, merekod dan menganalisis perkara-perkara berikut :

a. Sebarang percubaan pencerobohan kepada sistem ICT MPI;
b. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery phising*), pencerobohan (*instrusion*), 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 (*bandwitdth*) 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.

Tindakan : ICTSO dan Pentadbir Sistem

061002 Jejak Audit

Sistem kritikal 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 yang ditetapkan oleh pihak pengurusan atau peraturan semasa.

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.

Tindakan : Pentadbir Sistem

061003 Sistem Log

Bagi memastikan aktiviti sistem kritikal dipantau, Pentadbir Sistem ICT perlu 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 yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.

Tindakan : Pentadbir Sistem

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 diwujudkan 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 MPI atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.

Tindakan : Pentadbir Sistem

061005 Perlindungan Log

Maklumat dan fasiliti log perlu dilindungi daripada capaian yang tidak dibenarkan.

Tindakan : Pentadbir Sistem

061006 Log untuk Pentadbir Sistem

Segala aktiviti pentadbir dan operator sistem perlu direkod.

Tindakan : Pentadbir Sistem

061007 Log Kerosakan

Segala kerosakan perlu direkod, dianalisa dan diambil tindakan.

Tindakan : Pentadbir Sistem

061008 Penyeragaman Waktu

Semua sistem ICT MPI perlu mempunyai waktu yang seragam dengan *Network Time Protokol* (NTP) MPI atau waktu yang dinyatakan oleh SIRIM.

Tindakan : Pentadbir Sistem

BIDANG 07 - KAWALAN CAPAIAN

0701 KAWALAN CAPAIAN

Objektif:

Memastikan capaian kepada maklumat adalah berdasarkan kepada keperluan organisasi dan keselamatan 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.

Tindakan : Pentadbir Sistem

0702 PENGURUSAN CAPAIAN PENGGUNA

Objektif:

Mengawal capaian pengguna ke atas aset ICT MPI.

070201 Pendaftaran Akaun Pengguna

Pendaftaran, pengemaskinian dan penamatan akaun penguna mestilah dilaksanakan mengikut prosedur yang ditetapkan. 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 pengguna hanya diwujudkan setelah mendapat pengesahan Bahagian Pengurusan Sumber Manusia dan pengguna telah mengesahkan memahami Dasar Keselamatan ICT (DKICT);
b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti 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 MPI. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;

f. Penggunaan akaun milik orang lain adalah dilarang;

g. Penggunaan akaun tidak boleh dikongsi; dan

h. Akaun pengguna boleh dibeku atau ditamatkan apabila menerima arahan daripada Bahagian Pengurusan Sumber Manusia atas sebab-sebab berikut :

   i. Pengguna bercuti panjang dalam tempoh waktu melebihi tiga (3) minggu;

   ii. Bertukar bidang tugas kerja;

   iii. Bertukar ke agensi lain;

   iv. Bersara;

   v. Bagi menjalankan siasatan; atau

   vi. Ditamatkan perkhidmatan.

Tindakan : Semua

070202 Hak Capaian *(Privilege)*

Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.

Tindakan : Pemilik Sistem dan Pentadbir Sistem ICT

070203 Semakan Hak Capaian Pengguna

Pemilik sistem perlu menyemak semula hak capaian pengguna dari masa ke semasa.

Tindakan : Pentadbir Sistem ICT

070204 Pengurusan Kata Laluan Pengguna

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta garispanduan yang ditetapkan oleh MPI.

Penggunaan *default administrator* dan *guest* adalah tidak dibenarkan.

Tindakan : Semua

0703 TANGGUNGJAWAB PENGGUNA

Objektif:

Menghalang capaian yang tidak dibenarkan terhadap maklumat dan fasiliti pemprosesan.

070301 Penggunaan Akaun dan Kata Laluan

Perkara-perkara yang perlu dipatuhi adalah 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 aksara, angka dan aksara khusus;
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 identiti pengguna;
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.

Tindakan : Semua

070302 *Unattended User Equipment*

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a. Komputer yang *idle* dalam tempoh 15 minit perlu di *lock screen*;
b. Semua peralatan komputer perlu di *log off* setelah tugasan selesai; dan
c. Kawalan yang bersesuaian perlu dilaksanakan bagi peralatan tanpa pengawasan.

Tindakan : Semua

070303 *Clear Desk* dan *Clear Screen*

Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada di atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya

a. Pengguna perlu *lock screen* apabila meninggalkan komputer pada bila-bila masa;
b. Semua fail atau dokumen terperingkat perlu disimpan di tempat yang berkunci apabila meninggalkan meja kerja;
c. Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan; dan
d. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

    i. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;
    ii. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan
    iii. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.

Tindakan : Semua

070304 Penggunaan Komputer/*Notebook*

Penggunaan aset komputer MPI termasuk desktop dan *notebook* perlu dikawal supaya tiada pencerobohan, penyalahgunaan, kecurian, kehilangan dan pengubahsuaian kepada maklumat.

Semua pengguna komputer MPI perlu mematuhi perkara berikut:

a. Semua komputer MPI hendaklah digunakan untuk tugas rasmi sahaja;
b. Pengguna bertanggungjawab memastikan bahawa komputer perlu sentiasa mempunyai *antivirus* yang aktif dan terkini;
c. Semua komputer perlu didaftar pemiliknya dan pemilik berkenaan adalah bertanggungjawab menjaga keselamatan komputer tersebut sehingga komputer tersebut dilupuskan;
d. Setiausaha Bahagian adalah bertanggungjawab terhadap komputer gunasama, dan setiap pergerakan komputer tersebut perlu direkodkan;
e. Komputer (*notebook*) yang dibekalkan kepada pegawai yang layak, dibenarkan untuk dibawa pulang atau dibawa ke mana-mana dan pegawai adalah bertanggungjawab menjaga keselamatan aset berkenaan sepanjang masa;
f. Pentadbir Sistem berhak untuk menyiasat kandungan komputer apabila menerima arahan daripada CIO atau ICTSO;
g. Komputer milik MPI saja yang dibenarkan untuk mencapai maklumat-maklumat yang terdapat di dalam Intranet;
h. Komputer milik MPI perlu menggunakan domain MPI bagi mencapai ke rangkaian dan sistem-sistem MPI;
i. Komputer milik MPI adalah dilarang digunakan oleh pihak ketiga tanpa kawalan dan pengawasan pegawai MPI; dan
j. Pegawai perlu melaporkan dengan segera sekiranya berlaku kehilangan komputer atau notebook kepada MPI dengan menyertakan salinan laporan Polis.

Tindakan : Semua

0704 KAWALAN CAPAIAN RANGKAIAN

Objektif:

Menghalang capaian yang tidak sah dan tanpa kebenaran ke atas perkhidmatan Rangkaian (wayar dan tanpa wayar) MPI.

070401 Capaian Rangkaian

Penggunaan perkhidmatan rangkaian diberikan kepada pengguna berasaskan kepada tugas dan skop kerja. Semua sistem/aplikasi atau pengguna perlu mematuhi kawalan capaian perkhidmatan rangkaian yang ditetapkan seperti berikut;

a. Semua capaian akan berasaskan kepada tiga (3) *zone* rangkaian iaitu Intranet, *Demilitarized Zone* (DMZ) dan Internet ;
b. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MPI, rangkaian agensi lain dan rangkaian awam;
c. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunanya;
d. Menghalang mana-mana pengguna awam memasuki ke rangkaian intranet tanpa pengawasan;
e. Kontraktor atau pihak ketiga adalah dilarang membawa keluar peralatan yang digunakan untuk mencapai rangkaian intranet kecuali telah mendapat pengesahan pemilik sistem; dan
f. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.

Tindakan : Pentadbir Rangkaian, Pengurus ICT dan Semua

070402 Capaian Internet

Capaian melalui Internet (Rangkaian Awam) kepada rangkaian dan maklumat MPI hendaklah dikawal bagi memastikan tiada berlaku kecurian, pencerobohan, kerosakan dan pengubahsuaian.

Pengguna MPI yang berdaftar adalah dibenarkan untuk mencapai Internet dengan kawalan berasaskan tugas-tugas rasmi dan skop kerja.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :

a. Capaian ke Intranet MPI menggunakan Internet atau rangkaian awam adalah tidak dibenarkan;
b. Penggunaan Internet di MPI hendaklah dipantau secara berterusan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja seperti yang terdapat di dalam tatacara penggunaan Internet;
c. Penggunaan *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;
d. Semua aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu disekat bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan;
e. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja, CIO berhak menentukan penggunaan yang dibenarkan atau sebaliknya;
f. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh ICTSO atau CIO;

g. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Setiausaha 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 MPI;

j. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board* atau sebagainya. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

k. Penggunaan *modem/broadband* pada mana-mana peralatan atau aset yang berada atau bersambung dengan rangkaian MPI adalah 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.

Tindakan : Pentadbir Rangkaian, Pengurus ICT dan Semua

070403 Peralatan Dalam Rangkaian

Bagi memastikan bahawa peralatan yang disambungkan kepada Rangkaian MPI tidak menjejaskan keselamatan maklumat dan capaian, maka perkara-perkara berikut hendaklah dipatuhi:

a. Setiap peralatan yang hendak disambung kepada rangkaian MPI perlu didaftarkan;
b. Semua peralatan perlu disahkan bebas daripada virus dan perisian *antivirus* hendaklah dipasang dan masih aktif sepanjang masa;
c. Hanya peralatan yang telah berdaftar dibenarkan untuk sambungan (*join*) kepada rangkaian;
d. Setiap peralatan yang hendak disambung ke rangkaian perlu menggunakan protokol TCP/IP dan akan menggunakan IP *address* dan *domain name* yang ditetapkan oleh pentadbir rangkaian; dan
e. Semua konfigurasi peralatan dalam rangkaian selepas *switches* adalah menjadi tanggungjawab penggguna.

Tindakan : Pentadbir Rangkaian

070404 Capaian Ke *Port* Untuk Tujuan Diagnostik

Bagi memastikan bahawa *port* rangkaian tidak dicapai tanpa pengawasan, perkara berikut perlu dipatuhi oleh semua pengguna;

a. Semua *port* yang tak digunakan perlu *disable*;
b. Capaian fizikal dan logikal ke atas *port* untuk tujuan diagnostik perlu mendapat kebenaran pegawai yang diberikan kuasa;

c. Capaian oleh pegawai MPI hanya dibenarkan berasaskan kepada tugas dan skop kerja; dan
d. Capaian oleh pihak ketiga perlu mendapat kelulusan dari pegawai yang diberikan kuasa.

Tindakan : Pentadbir Rangkaian

070405 Pengasingan Dalam Rangkaian

Rangkaian MPI perlu dibuat pengasingan menggunakan VLAN, Zon (Intranet, DMZ, Internet) dan VPN mengikut jenis perkhidmatan, pengguna, sensitiviti maklumat dan sistem.

Tindakan : Pentadbir Rangkaian

070406 Kawalan Penghalaan *(Routing)* Rangkaian

Penghalaan (*routing*) perlu dikawal supaya ianya tidak disalah guna dengan memastikan perkara berikut:

a. Konfigurasi (*routing*) perlu disemak dan disahkan sebelum dilaksanakan;
b. Semakan *routing table* perlu dibuat dari masa ke semasa; dan
c. Penghalaan (*routing*) di dalam sistem rangkaian perlu dilaksanakan dengan betul dan terkawal.

Tindakan : Pentadbir Rangkaian

0705 KAWALAN CAPAIAN SISTEM PENGOPERASIAN

Objektif:

Menghalang capaian yang tidak sah dan tanpa dibenarkan ke atas sistem pengoperasian.

070501 Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu diaktifkan 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; dan
b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*.

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. Menghadkan dan mengawal penggunaan program; dan

d. Menghadkan tempoh sambungan ke aplikasi berisiko tinggi.

Tindakan : Pentadbir Sistem

070502 *Secure Log-on*

Log-on ke atas sistem pengoperasian perlu melalui satu kaedah yang selamat bagi mengurangkan akses yang tidak dibenarkan.

Tindakan : Pentadbir Sistem

070503 Pengenalan dan Pengesahan pengguna

Capaian masuk sistem perlu mempunyai kaedah bagi mengenal dan mengesahkan pengguna adalah sah.

Tindakan : Pentadbir Sistem

070504 Penggunaan Sistem Utiliti

Penggunaan sistem utiliti perlulah dikawal dan dihadkan kepada pegawai yang dibenarkan saja.

Tindakan : Pentadbir Sistem

070505 *Session Time-Out*

Sesi yang tidak aktif perlu ditamatkan mengikut tempoh masa yang ditetapkan.

Tindakan : Pentadbir Sistem dan Pentadbir Rangkaian

070506 Had Masa Capaian

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Had masa capaian kepada maklumat dan sistem aplikasi hendaklah berasaskan kepada keperluan dan fungsi pengguna; dan
b. Masa capaian bagi aplikasi berisiko tinggi perlu dihadkan semasa waktu pejabat sahaja.

Tindakan : Pentadbir Sistem

0706 KAWALAN CAPAIAN APLIKASI DAN MAKLUMAT

Objektif

Menghalang capaian yang tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.

070601 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 diberikan mengikut tahap capaian dan keselamatan maklunat yang telah ditentukan;

b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log);
c. Menghadkan capaian sistem dan aplikasi kepada tiga (5) 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
e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaanya terhad kepada perkhidmatan yang dibenarkan sahaja dan di dalam zon yang ditetapkan.

Tindakan : Semua

070602 Larangan Capaian Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Capaian kepada maklumat dan sistem aplikasi hendaklah berasaskan kepada keperluan dan fungsi pengguna;
b. Capaian kepada maklumat yang tidak rasmi , berunsur lucah, iklan dan yang menjejaskan prestasi kerja; dan
c. Capaian kepada maklumat dan sistem aplikasi perlu dinyatakan dengan jelas kepada pengguna.

Tindakan : Semua

070603 Pengasingan Sistem Kritikal

Pengasingan sistem kritikal perlu dilaksana dengan menggunakan VLAN/ VPN dan zon rangkaian (intranet, DMZ, Internet).

Tindakan : Pentadbir Sistem

0707 PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH

Objektif:

Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.

070701 Peralatan Mudah Alih

Perkara yang perlu dipatuhi adalah seperti berikut :

a. Peralatan mudah alih yang dikhaskan untuk pegawai yang berkelayakan dibenarkan dibawa keluar bagi melaksanakan tugas-tugas rasmi;
b. Peralatan mudah alih gunasama perlu direkod dan mendapat kelulusan pegawai yang bertanggungjawab apabila hendak dibawa keluar dari pejabat;
c. Semua peralatan mudah alih hendaklah dilindungi dan dikawal dengan selamat; dan
d. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.

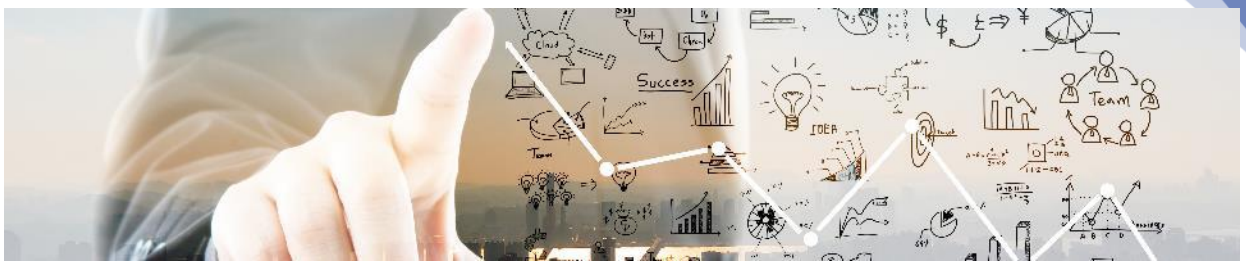
Tindakan : Semua

070702 Kemudahan Kerja Jarak Jauh

Kerja jarak jauh hanya boleh dilaksanakan setelah mendapat kelulusan pegawai yang diberi kuasa dan pemilik sistem yang berkaitan.

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

Tindakan : 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

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 menggangu pemprosesan dan ketetapan 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, serta sistem output untuk memastikan data yang telah diproses adalah tepat;
c. Aplikasi perlu mengandungi semakan pengesahan (*vadilation*) 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 digunapakai.

Tindakan : Pentadbir Sistem, Pemilik Sistem dan ICTSO

080102 Analisa Dan Spesifikasi Keperluan Keselamatan

Spesifikasi reka bentuk perlu memasukkan keperluan keselamatan sistem maklumat. Sekiranya sesuatu *off-the-shelf* produk diperolehi, pembekal perlu dimaklumkan berkenaan keperluan keselamatan.

Tindakan : Pentadbir Sistem

0802 KEBOLEHPERCAYAAN PEMPROSESAN DALAM APLIKASI

Objektif

Untuk mengelak kesalahan, kecacatan, kerugian, pengubahsuaian yang tidak dibenarkan, penyalahgunaan maklumat dalam aplikasi atau kehilangan kepercayaan terhadap sistem.

080201 Pengesahan Data *Input*

Data yang dimasukkan ke dalam aplikasi perlu disahkan untuk memastikan data adalah tepat dan betul.

Tindakan : Pemilik Sistem

080202 Kawalan Bagi Pemprosesan Dalaman

Satu prosedur semakan perlu diadakan di dalam aplikasi bagi mengesan sebarang kerosakan maklumat yang terhasil dari kesilapan dan kecacatan pemprosesan ataupun kesalahan yang disengajakan. Senarai semak yang bersesuaian perlu disediakan, aktiviti-aktiviti hendaklah didokumenkan dan hasil keputusan perlu disimpan dengan selamat.

Tindakan : Pentadbir Sistem

080203 Integriti Maklumat

Satu penilaian terhadap risiko keselamatan perlu dijalankan untuk menentukan keperluan integriti maklumat dan bagi mengenal pasti kaedah yang paling bersesuaian untuk dilaksanakan.

Tindakan : Pemilik Sistem dan Pentadbir Sistem

080204 Pengesahan Data *Output*

Data yang dikeluarkan daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.

Tindakan : Pemilik Sistem

0803 KAWALAN KRIPTOGRAFI

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi mengikut keperluan.

080301 Enkripsi

Proses enkripsi (*encryption*) perlu dilaksanakan bagi melindungi kerahsiaan maklumat kritikal atau sensitif berdasarkan keperluan, penilaian risiko dan selaras dengan Akta-akta MPI.

Tindakan : Semua

080302 Tandatangan Digital

Penggunaan tandatangan digital (sekiran berkaitan) adalah dimestikan kepada semua pengguna khususnya yang berurusan dengan transaksi maklumat kritikal atau sensitif atau maklumat rahsia rasmi secara elektronik.

Tindakan : Semua

080303 Pengurusan Kunci Kriptografi

Pengurusan ke atas kunci kriptografi yang dilaksanakan ke atas maklumat kritikal atau sensitif hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

Tindakan : Semua

0804 KESELAMATAN FAIL SISTEM

Objektif:

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

080401 Kawalan Perisian (*Operational Software*)

Kawalan perubahan kepada perisian perlu dilaksanakan bagi mengurangkan risiko kerosakan pada perisian. Perkara-perkara yang perlu dipatuhi adalah seperti yang berikut:

a. Proses pengemaskinian perisian hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang diberi tanggungjawab dan mengikut prosedur yang telah ditetapkan;
b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh digunakan selepas diuji dan diluluskan;
c. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan;
d. Mengawal capaian ke atas kod atau cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan
e. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal.

Semua sistem konfigurasi perlu didokumenkan/daftarkan.

Tindakan : Pentadbir Sistem

080402 Kawalan Data Pengujian Sistem

Data pengujian sistem perlu dipilih dengan teliti, dilindungi dan terkawal. Penggunaan data sebenar (*operational data*) yang melibatkan data personel atau data sensitif pada persekitaran pengujian perlu dielakkan. Jika data personel atau data sensitif digunakan untuk tujuan pengujian, kandungan sensitif perlu ditapis atau diubahsuai sebelum digunakan.

Tindakan : Pemilik Sistem

080403 Kawalan Capaian kepada Kod Sumber (*Source Code*)

Kawalan capaian kepada kod atau atur cara program perlu dilaksanakan bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian.

Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik MPI.

Tindakan : Pentadbir Sistem

0805 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN PROSESAN SOKONGAN

Objektif

Menjaga dan menjamin keselamatan sistem perisian aplikasi dan maklumat.

080501 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a. Perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat perlu dikawal, diuji, direkodkan dan disahkan melalui prosedur yang ditetapkan sebelum diguna pakai;
b. Pengujian terhadap perubahan dan pengubahsuaian ke atas sistem perisian aplikasi dan maklumat hendaklah dilaksanakan dalam persekitaran yang berasingan sama ada daripada produksi atau pembangunan;
c. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan

tiada kesan yang buruk terhadap operasi dan keselamatan agensi.

d. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor;

e. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja;

f. Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan

g. Menghalang sebarang peluang untuk membocorkan maklumat.

Tindakan : Pentadbir Sistem dan Pemilik Sistem

080502 Keperluan Kajian Teknikal Terhadap Aplikasi Selepas Perubahan Sistem Pengoperasian

Semua aplikasi perlu dikaji dan diuji apabila berlaku perubahan sistem pengoperasian bagi memastikan tiada sebarang kesan buruk yang merugikan kepada operasi dan keselamatan organisasi.

Tindakan : Pentadbir Sistem

080503 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 MPI.

Tindakan: Pemilik Sistem dan Pentadbir Sistem

0806 PENGURUSAN KELEMAHAN TEKNIKAL

Objektif:

Mengurangkan Risiko Akibat Dari Eksploitasi Kelemahan Teknikal.

080601 Kawalan Kelemahan Teknikal

Kelemahan teknikal terhadap sistem maklumat perlu dilapor dan dibuat penilaian dengan segera untuk tindakan pembetulan.

Tindakan : Pemilik Sistem dan Pentadbir Sistem

0807 KAWALAN TEKNIKAL KETERDEDAHAN (*VULNERABILITY*)

Objektif:

Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.

080701 Kawalan dari Ancaman Teknikal

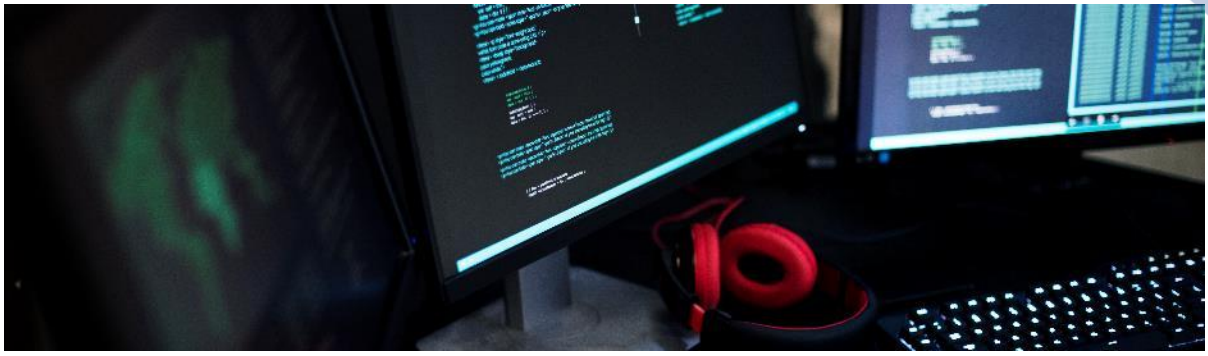
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan.

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.

Tindakan : Pentadbir Sistem



BIDANG 09 - PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 MEKANISME PELAPORAN INSIDEN KESELAMATAN ICT

Objektif:

Memastikan insiden keselamatan ICT dan kelemahan dilapor dan disalurkan dengan cepat dan berkesan bagi meminimumkan proses pembaikan dan mengurangkan 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 (DKICT) sama ada yang ditetapkan secara tersurat atau tersirat.

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CERT MPI dengan kadar segera:

a. Maklumat didapati hilang, didedahkan oleh pihak-pihak yang 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;
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.

Prosedur pelaporan insiden keselamatan ICT di MPI hendaklah berdasarkan:

a. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi.
b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.

Tindakan : Semua

090102 Pelaporan Kelemahan Keselamatan

Pengguna sistem dikehendaki melaporkan sebarang kelemahan sistem dengan segera bagi mengelak insiden keselamatan ICT.

Tindakan : Semua

0902 PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT

Objektif:

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

090201 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 MPI.

Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan 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;
b. Menyalin bahan bukti dan merekodkan semua maklumat dan aktiviti penyalinan;
c. Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;
d. Menyediakan tindakan pemulihan segera; dan

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

Tindakan : CIO dan Pengurus ICT

090202 Pembelajaran Dari Insiden Kelemahan Maklumat

Mewujudkan mekanisma bagi menentukan semua insiden keselamatan maklumat direkod untuk dianalisa dan dipantau.

Tindakan : ICTSO dan Pentadbir Sistem

090203 Pengumpulan Bukti

Bukti-bukti insiden keselamatan maklumat perlu dikumpul dan dikekalkan untuk tindakan perundangan.

Tindakan : ICTSO dan Pentadbir Sistem

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 Plan (BCP)*) 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 pihak pengurusan MPI atau mana-mana jawatankuasa yang ditubuhkan. 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 (1) sekali.

BCP mempunyai empat komponen utama iaitu:-

a. Pelan Pemulihan Bencana;
b. Pelan Tindakbalas Kecemasan;
c. Pelan Tindakbalas Insiden; dan
d. Pelan Komunikasi.

DAN hendaklah mengandungi perkara-perkara berikut:

a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
b. Senarai personel MPI dan vendor berserta nombor yang boleh dihubungi (faks, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel yang 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 yang mana perlu.

Salinan BCP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. BCP hendaklah diuji sekurang-kurangnya sekali (1) 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 objektif pembangunan.

Ujian BCP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. MPI hendaklah memastikan salinan BCP sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

Tindakan : Pengurus ICT dan Pemilik Sistem

BIDANG 11 - PEMATUHAN

1101 PEMATUHAN DAN KEPERLUAN PERUNDANGAN

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT (DKICT) MPI.

110101 Pematuhan Dasar

Setiap pengguna di MPI hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT (DKICT) MPI dan undang-undang atau peraturan-peraturan lain yang berkuat kuasa.

Semua aset ICT di MPI termasuk maklumat yang disimpan di dalamnya adalah hak milik MPI. KSU atau pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna bagi mengesan penggunaan selain dari tujuan yang telah ditetapkan.

Sebarang penggunaan aset ICT MPI selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber MPI.

Tindakan : Semua

110102 Pematuhan Dasar dan Keperluan Teknikal

ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar dan keperluan teknikal.

Tindakan : 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.

Tindakan : Semua

110104 Keperluan Perundangan

Semua pengguna aset ICT MPI perlu mematuhi segala keperluan perundangan, akta atau peraturan-peraturan lain yang berkaitan yang terpakai oleh MPI.

Senarai Perundangan dan Peraturan adalah seperti berikut:

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) 2002;

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 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 Bil. 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. Garis Panduan Keselamatan MPI;
w. *Standard Operating Procedure* (SOP) ICT MPI;
x. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
y. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.

Tindakan : Semua

110105 Pelanggaran Dasar

Pelanggaran Dasar Keselamatan ICT MPI boleh dikenakan tindakan tatatertib menurut polisi yang diluluskan.

Tindakan: Semua

Lampiran 1

Surat Akuan Pematuhan Dasar Keselamatan ICT MPI

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT MPI

Nama (Huruf Besar) :
No. Kad Pengenalan :
Jawatan :
Bahagian :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

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

Tandatangan : _____

Tarikh : _____

Pengesahan Pegawai Keselamatan ICT

_____

(Nama Pegawai Keselamatan ICT/ICTSO)
b.p. Ketua Setiausaha MPI
Tarikh : _____