MAJLIS DAERAH TANJONG MALIM

MDTM.(IT) 01/10/05/13/PPICT

DASAR KESELAMATAN ICT MDTM

(Versi 1.1)

Disediakan oleh :

Bahagian Teknologi Maklumat

Majlis Daerah Tanjong Malim

Disemak Oleh	Diperakui Oleh
……..	. ……
Pegawai Keselamatan Jabatan (PKJ) Majlis Daerah Tanjong Malim	Yang Dipertua Majlis Daerah Tanjong Malim

Pekeliling Perkhidmatan ICT — 2 Febuari 2017

MAJLIS DAERAH TANJONG MALIM

DASAR KESELAMATAN ICT MDTM

(Versi 1.1)

MAJLIS DAERAH TANJONG MALIM

2 FEBUARI 2017

Pekeliling Perkhidmatan ICT 2 Febuari 2017

JADUAL PINDAAN DASAR KESELAMATAN ICT MDTM

TARIKH	VERSI	PINDAAN	TARIKH KUATKUASA
10 Disember 2013	1.0	TIADA	11 Disember 2013
2 Febuari 2017	1.1	Pengesahan DKICT bagi PKJ dan Yang Dipertua MDTM	6 Febuari 2017

JADUAL PINDAAN DASAR KESELAMATAN ICT MDTM

TARIKH	VERSI	BUTIRAN PINDAAN
2 Febuari 2017	1.1	

ISI KANDUNGAN

PERKARA 06 - PENGURUSAN OPERASI DAN KOMUNIKASI

PENGENALAN

Tuntutan perkhidmatan yang semakin mencabar menuntut Majlis Daerah Tanjong Malim (MDTM) menyediakan sistem perkhidmatan yang lebih efisien dan berkualiti. Antara teras yang dilihat mampu merealisasikan usaha ini adalah menerusi keunggulan perkhidmatan ICT dalam setiap perkhidmatan yang diberikan. Justeru, satu dasar telah dibentuk sebagai usaha untuk membantu dan membimbing kakitangan yang bertanggungjawab dalam melaksanakan tugas mahupun program yang melibatkan ICT. Perkara ini dlihat sebagai satu keperluan yang akan melancarkan pengurusan kerja harian serta mampu mengelakkan insiden-insiden ICT yang boleh menyebabkan kerosakan mahupun kehilangan maklumat serta perkakasan.

MDTM berusaha untuk mencapai visi dan misinya melalui sistem peyampaian perkhidmatan yang berteraskan serta memenuhi kehendak dan keperluan pihak pengurusan perkhidmatan dan juga para pelanggan. Berdasarkan kepada kepentingan ini maka pihak pengurusan perkhidmatan MDTM telah mengeluarkan dokumen ini sebagai usaha untuk memastikan objektif perkomputeran yang telah ditetapkan dapat dicapai. Dokumen ini juga merangkumi beberapa pernyataan dasar mengikut kepada aspek penting dalam melindungi aset ICT di MDTM.

Tujuan dasar ini adalah untuk memaklumkan peraturan-peraturan yang perlu dipatuhi oleh semua kakitangan MDTM demi untuk menjaga keselamatan dan aset teknologi maklumat serta komunikasi ICT. Berdasarkan kepada peraturan ini, diharapkan agar semua pengguna yang akan berurusan dengan perkhidmatan MDTM sedar akan tanggungjawab dan peranan mereka dalam melindungi aset ICT MDTM. Oleh itu. tahap keselamatan ICT dan langkah-langkah mengurangkan risiko ancaman dari dalam dan luar ke atas sistem dan infrastruktur ICT MDTM dapat dipertingkatkan.

OBJEKTIF

Dasar Keselamatan ICT MDTM secara umumnya diwujudkan untuk menjamin kesinambungan urusan perkhidmatan MDTM dengan meminimumkan kesan insiden keselamatan ICT. Objektif utama Dasar Keselamatan ICT MDTM adalah seperti berikut :-

(a) Memastikan kelancaran operasi MDTM yang menggunakan teknologi ICT dan meminimumkan kerosakan dan kemusnahan.
(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem ICT dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan makumat dan komunikasi; dan
(c) Mencegah salahguna atau kecurian Aset ICT MDTM.

SKOP

Dasar ini meliputi semua sumber atau aset ICT yang digunakan seperti :-

(a) **Perkakasan**
Aset ICT yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan MDTM (contoh seperti komputer, pelayan, peralatan komunikasi dan sebagainya);

(b) **Perisian**
Program perisian atau aplikasi yang menyediakan kemudahan pemerosesan maklumat seperti sistem pengoperasian, sistem pangkalan data, aplikasi pejabat, perisian sistem rangkaian dan sebagainya;

(c) **Premis Komputer dan Komunikasi**
Semua kemudahan serta lokasi yang digunakan untuk menempatkan aset-aset di atas.

(d) **Perkhidmatan**
Perkhidmatan atau sistem yang menyokong aset lain seperti perkhidmatan rangkaian, perkhidmatan keselamatan dan lain-lain lagi;

(e) **Data dan Maklumat**
Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik;

(f) **Manusia**

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja MDTM yang mana merupakan aset berdasarkan kepada tugas dan fungsi yang dilaksanakan;

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

PRINSIP-PRINSIP

Prinsip-prinsip asas yang menjadi dasar kepada pelaksanaan Dasar Keselamatan ICT MDTM yang perlu dipatuhi adalah seperti berikut :

(a) **Akses Atas Dasar Perlu Mengetahui**

Akses terhadap penggunaan aset ICT hanya diberi untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

(b) **Hak Akses Minimum**

Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat.

(c) **Akauntabiliti**

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT MDTM

(d) **Pengasingan**

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat berperingkat atau dimanipulasi.

(e) **Pengauditan**

Pengauditan adalah 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 MDTM hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk perlanggaran 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.

(h) **Saling bergantung**

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.

PERKARA 01 – PEMBANGUNAN DAN PENYELENGGARAAN DASAR

P01(01) – Dasar Keselamatan ICT	
P01(01) 01 – Pelaksanaan Dasar	**Tindakan**
Pelaksanaan dasar ini akan dijalankan oleh Yang DiPertua selaku Pengerusi Jawatankuasa Keselamatan Perlindungan Penuh (JKKPP) MDTM.JKKPP ini terdiri daripada Pegawai Keselamatan Jabatan(PKJ) dengan dibantu oleh Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Ketua Jabatan/bahagian.	Yang DiPertua,Ketua Jabatan/Bahagian,PKJ
P01(01) 02 –Penyebaran Dasar	**Tindakan**
Dasar ini perlu disebarkan kepada semua pelanggan MDTM (termasuk kakitangan, pembekal, pakar runding dan lain-lain yang berkaitan).	CIO/ICTSO
P01(01) 03 – Penyelenggaraan Dasar	**Tindakan**
Dasar Keselamatan ICT MDTM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur berhubung penyelenggaraan dasar keselamatan ICT MDTM : a) Kenal pasti dan tentukan perubahan yang diperlukan; b) Kemukakan cadangan pindaan secara bertulis kepada CIO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Keselamatan Perlindungan Penuh (JKKPP) MDTM; c) perubahan yang telah dipersetujui oleh JKKPP dimaklumkan kepada semua pengguna; d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	CIO / ICTSO
P01(01) 04 – Pengecualian Dasar	**Tindakan**
Dasar Keselamatan ICT MDTM adalah terpakai kepada semua pengguna ICT MDTM dan tiada pengecualian diberikan	Semua

PERKARA 02 – ORGANISASI KESELAMATAN

P02(01) – Infrastruktur Organisasi Keselamatan

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

P02(01) 01 – Yang Dipertua / Pegawai Keselamatan Jabatan	**Tindakan**
Yang DiPertua adalah merupakan Pegawai Pengawal.Manakala Setiausaha MDTM adalah merupakan Pegawai Keselamatan Jabatan (PKJ).Peranan dan tanggungjawab Yang Dipertua/PKJ adalah seperti berikut: (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MDTM; (b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MDTM; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi dan memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT MDTM; dan (d) Memepengerusikan Mesyuarat Jawatankuasa Keselamatan Perlindungan Penuh (JKKPP), MDTM.	Yang Dipertua/PKJ
P02(01) 02 – Ketua Pegawai Maklumat (CIO)	**Tindakan**
Ketua Bahagian Teknologi Maklumat adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut : (a) Membantu Yang Dipertua / PKJ dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Menentukan keperluan Keselamatan ICT; (c) Membangun dan menyelaras perlaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; (d) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Majlis;	CIO

(e) Menentukan kawalan akses pengguna terhadap aset ICT Majlis; (f) Mengurus keseluruhan program-program keselamatan ICT MDTM; (g) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Majlis; (h) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT MDTM; (i) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT MDTM dan menjaga kerahsiaan maklumat MDTM; (j) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MDTM sebagaimana **Lampiran 1**; dan (k) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MDTM.	
P02(01) 03 – Pegawai Keselamatan ICT (ICTSO)	**Tindakan**
Juruteknik Bahagian Teknologi Maklumat merupakan pegawai yang dilantik sebagai Pegawai Keselamatan ICT (ICTSO) MDTM. Peranan dan tanggungjawab Pegawai Keselamatan ICT (ICTSO) yang dilantik adalah seperti berikut:- (a) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MDTM kepada semua pengguna; (b) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MDTM; (c) Menjalankan pengurusan risiko; (d) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MDTM berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (e) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (f) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO; (g) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT Kerajaan (GCERT), MAMPU dan memaklumkannya kepada CIO;	ICTSO

(h) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan (i) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT. (j) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (k) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT MDTM; (l) Memantau aktiviti capaian harian sistem aplikasi pengguna; (m) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (n) Menganalisis dan menyimpan rekod jejak audit; dan (o) Menyediakan laporan mengenai aktiviti capaian secara berkala.	
P02(01) 04 – Pengguna	**Tindakan**
Pengguna mempunyai peranan dan tanggungjawab seperti berikut:- (d) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MDTM (e) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (f) Lulus tapisan keselamatan; (g) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT MDTM dan menjaga kerahsiaan maklumat MDTM; (h) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (i) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan (j) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MDTM sebagaimana **Lampiran 1**.	

P02(01) 05 – Jawatankuasa Keselamatan Perlindungan Penuh (JKKPP) , MDTM.	Tindakan
Jawatankuasa Keselamatan ICT (JKICT) adalah Jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT MDTM. Di MDTM, Mesyuarat Jawatankuasa Keselamatan MDTM juga berperanan sebagai JKICT MDTM. Keanggotaan ahli Jawatankuasa adalah seperti berikut :- **Pengerusi** : Yang Dipertua / Pegawai Keselamatan Jabatan (PKJ) **Ahli** : (1) Ketua Pegawai Maklumat (CIO), MDTM (2) Semua Ketua Jabatan/Bahagian (3) Pegawai Keselamatan MDTM (4) ICTSO MDTM **Urus Setia** bagi jawatankuasa ini adalah Jabatan Khidmat Pengurusan. Bidang kuasa: (a) Memperakukan/meluluskan dokumen DKICT MDTM; (b) Memantau tahap pematuhan keselamatan ICT; (c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam MDTM yang mematuhi keperluan DKICT MDTM; (d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (e) Memastikan DKICT MDTM selaras dengan dasar-dasar ICT kerajaan semasa; (f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; (g) Membincangkan tindakan yang melibatkan pelanggaran DKICT MDTM; dan (h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	JKKPP MDTM

P02(02) Pihak Ketiga

Objektif:
Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).

P02(02) 01 – Keperluan Keselamatan Kontrak dengan Pihak Ketiga	Tindakan
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MDTM; (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 MDTM perlu berlandaskan kepada perjanjian kontrak; (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT MDTM; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. v. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MDTM sebagaimana di **Lampiran 1**.	CIO, ICTSO, dan Pihak Ketiga

PERKARA 03 – PENGURUSAN ASET

P03(01) Akauntabiliti Aset ICT

Objektif:

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

P03(01) 01 – Inventori Aset ICT	**Tindakan**
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemaskini; (b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MDTM; (d) Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, didokumen dan dilaksanakan; dan **(e)** Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Semua yang terlibat didalam pengurusan aset

P03(02) Pengelasan dan Pengendalian Aset ICT	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
P03(02) 01 – Pengelasan Maklumat	**Tindakan**
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau Terhad.	semua
P03(02) 02 – Pengendalian Maklumat	**Tindakan**
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.	Semua

PERKARA 04 - KESELAMATAN SUMBER MANUSIA

P04 (01) Keselamatan Sumber Manusia Dalam Tugas Harian

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

P04(01) 01 – Sebelum Perkhidmatan	**Tindakan**
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menjelaskan peranan dan tanggungjawab pegawai dan kakitangan MDTM serta pihak ketiga yang terlibat dengan lengkap dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan MDTM serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	Semua

P04(01) 02 – Dalam Perkhidmatan	**Tindakan**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan pegawai dan kakitangan MDTM serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh MDTM;	Semua

(b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MDTM secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan MDTM serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MDTM; dan (d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Latihan, Jabatan Khidmat Pengurusan, MDTM.	
P04(01) 03 – Bertukar Alamat atau Tamat Perkhidmatan	**Tindakan**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Semua aset ICT mestilah dikembalikan kepada MDTM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MDTM dan/atau terma perkhidmatan adalah terbatal atau perlu ditarik balik.	Semua

P04(02) Program Pembudayaan Keselamatan ICT	
Objektif: Memastikan semua sumber manusia yang terlibat termasuk pegawai, kakitangan MDTM dan pihak-pihak yang berkepentingan memperolehi latihan yang mencukupi dan melibatkan mereka dalam program kesedaran dan pembudayaan ICT.	
P04(02) 01 – Kursus Keselamatan ICT	**Tindakan**
Melaksanakan kursus serta latihan kepada kakitangan dan memastikan mereka menerima latihan keselamatan ICT yang mencukupi secara berterusan untuk dilaksanakan di dalam tugas harian mereka.	Semua
P04(02) 02 - Program Kesedaran Dan Pembudayaan	**Tindakan**
Program kesedaran dan pembudayaan keselamatan ICT seperti taklimat dan seminar mengenai pentingnya keselamatan ICT dititikberatkan serta kesan-kesannya sekiranya diabaikan hendaklah diadakan secara kerap dan menyeluruh di kalangan kakitangan. Program menangani insiden keselamatan ICT juga penting untuk memastikan kakitangan dapat bertindak segera dan sewajarnya sekiranya ia berlaku.	Semua

PERKARA 05 - KESELAMATAN FIZIKAL DAN PERSEKITARAN

P05(01) Keselamatan Kawasan

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

P05(01) 01 – Kawalan kawasan	Tindakan
Ia bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenalpasti dengan jelas.Lokasi dan kekuatan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Penggunaan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Pemasangan alat penggera atau kamera keselamatan; (d) Menghadkan laluan jalan keluar masuk; (e) Mewujudkan 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 lain; (j) Merekabentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau-bilau dan bencana;	Pegawai Keselamatan Jabatan, Ketua Jabatan, CIO, ICTSO

(k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
P05(01) 02 – Kawalan Masuk Fizikal	**Tindakan**
Perkara-perkara yang perlu dipatuhi termasuk yang berikut:- (a) Setiap pengguna MDTM hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan semula kepada MDTM apabila kakitangan berhenti atau bersara; (c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter khidmat pelanggan dan dikembalikan semula selepas tamat urusan/lawatan; (d) Setiap pelawat hendaklah mendaftar di Kaunter Khidmat Pelanggan di Lobi Pejabat Majlis Daerah Tanjong Malim terlebih dahulu; dan (e) Kehilangan pas mestilah dilaporkan dengan segera;	Semua
P05(01) 03 – Kawasan Larangan	**Tindakan**
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di kawasan tersebut. Kawasan larangan di MDTM adalah Bilik Yang Dipertua, Bilik Setiausaha, Bilik Server / Pusat Data dan Bilik Operasi Penguatkuasa. (a) Pegawai yang terlibat dan telah diberi kuasa sahaja yang dibenarkan untuk mengakses bilik-bilik tersebut;	Semua

(b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai dan mestilah mendapat kebenaran daripada Ketua Jabatan/Bahagian.	

P05(02) Keselamatan Peralatan

Objektif:
Melindungi peralatan ICT MDTM dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

P05(02) 01 – Peralatan ICT	**Tindakan**
Perkara-perkara yang perlu dipatuhi bagi menjaminkan keselamatan peralatan ICT adalah seperti berikut: (a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) Pengguna bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang peralatan ICT yang telah ditetapkan; (d) Pengguna dilarang memuatnaik atau menambah sebarang perisian tambahan tanpa kebenaran CIO / ICTSO; (e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;	Semua

(f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemaskini di samping 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 *Uninterruptable Power Supply* (UPS)/*Automatic Voltage Regulator* (AVR);

(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 premis MDTM, perlulah mendapat kelulusan Ketua Bahagian Teknologi Maklumat selaku CIO dan hendaklah direkodkan bagi tujuan pemantauan;

(m)Peralatan ICT yang hilang hendaklah dilaporkan kepada CIO/ICTSO dan Pegawai Aset dengan segera;

(n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa;

(o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran CIO;

(p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan ke Bahagian Teknologi Maklumat untuk tindakan selanjutnya;

(q) Sebarang pelekat selain bagi 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 CIO/ICTSO; (t) Pengguna bertanggungjawab terhadap perkakasan, perisian 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; dan (w) Memastikan plug dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya. (v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada CIO/ICTSO.	
P05(02) 02 – Media Storan	**Tindakan**
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti 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;	Semua

(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.	
P05(02) 03 – Media Tandatangan Digital	**Tindakan**
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 tandatangan digital ini tidak boleh dipindah milik atau dipinjamkan; dan (c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Semua

P05(02) 04 – Media Perisian dan Aplikasi	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MDTM; (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran CIO; (c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-rom*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan (d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua

P05(02) 05 – Penyelenggaraan Peralatan ICT	Tindakan
Peralatan ICT hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan;	Pegawai Aset ICT, Bahagian Teknologi Maklumat

(e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran daripada CIO/ICTSO.	
P05(02) 06 – Peralatan ICT di Luar Premis	**Tindakan**
Peralatan yang dibawa keluar dari premis MDTM adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
P05(02) 07 – Pelupusan Peralatan ICT	**Tindakan**
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MDTM dan ditempatkan di MDTM. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MDTM. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; (b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;	Semua, Pegawai Aset ICT, Bahagian Teknologi Maklumat

(c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (d) ICTSO/Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (f) Pegawai Aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori Aset ICT; (g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuatkuasa; dan (h) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di MDTM; iii. Memindah keluar dari MDTM mana-mana peralatan ICT yang hendak dilupuskan; dan iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan adalah di bawah tanggungjawab MDTM.	Semua, Pegawai Aset ICT, Bahagian Teknologi Maklumat

P05(03) Keselamatan Persekitaran	
Objektif: Melindungi aset ICT MDTM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
P05(03) 01 – Kawalan Persekitaran	**Tindakan**
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: (a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; (b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; (c) Peralatan perlindungan keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; (d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; (e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; (f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; (g) Akses kepada saluran *riser* hendaklah sentiasa dikunci; dan	Semua

(h) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	
P05(03) 03 – Kabel	**Tindakan**
Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan. (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Bahagian Teknologi Maklumat, ICTSO
P05(03) 04 – Prosedur Kecemasan	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MDTM; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ).	Bahagian Teknologi Maklumat, ICTSO

P05(04) Keselamatan Dokumen	
Objektif: Melindungi maklumat MDTM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
P05(04) 01 – Dokumen	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua

PERKARA 06 – PENGURUSAN OPERASI DAN KOMUNIKASI

P06(01) Pengurusan Prosedur Operasi

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

P06(01) 01 – Pengendalian Prosedur	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur pengurusan operasi yang diwujud, dikenalpasti 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.	Semua

P06(01) 02 – Kawalan Perubahan	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;	Semua

(c) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (d) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (e) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua
P06(01) 03 – Pengasingan Tugas dan Tanggungjawab	**Tindakan**
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 dimanipulasi; dan	CIO, ICTSO

P06(02) Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
P06(02) 01 – Perkhidmatan Penyampaian	**Tindakan**
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan (c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	CIO, ICTSO
P06(03) Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
P06(03) 01 – Perancangan Keupayaan	**Tindakan**
Keupayaan/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.	CIO, ICTSO

Keperluan keupayaan/kapasiti ini juga perlu mengambilkira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	
P06(03) 02 – Penerimaan Sistem	**Tindakan**
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	CIO,ICTSO
P06(04) Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya.	
P06(04) 01 – Perlindungan daripada Perisian Berbahaya	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) 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 berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; (d) Mengemaskini anti virus dengan *pattern* antivirus yang terkini;	Semua

(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.	Semua
P06(04) 02 – Perlindungan dari *Mobile Code*	**Tindakan**
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
P06(05) *Housekeeping*	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
P06(05) 01 – *Backup*	**Tindakan**
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua

(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.	Semua

P06(06) Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
P06(06) 01 – Kawalan Infrastruktur Rangkaian	**Tindakan**
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; *(d)* Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh CIO/ICTSO; (f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan rangkaian MDTM; (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran CIO; (h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MDTM; (i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;	Bahagian Teknologi Maklumat

(j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan MDTM adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian MDTM sahaja dan penggunaan modem luaran/mudahalih adalah dilarang samasekali; dan (l) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.	

P06(07) Pengurusan Media

Objektif:
Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

P06(07) 01 – Penghantaran dan Pemindahan	**Tindakan**
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua

P06(07) 02 – Prosedur Pengedalian Media	**Tindakan**
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti 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;	Semua

(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.	Semua
P06(07) 03 – Keselamatan Sistem Dokumentasi	**Tindakan**
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Semua
P06(08) Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara MAMPU dan agensi luar terjamin.	
P06(08) 01 – Pertukaran maklumat	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Semua

(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 MDTM dengan agensi luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MDTM; dan (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
P06(08) 02 – Pengurusan Mel Elektronik (E-Mel)	**Tindakan**
Penggunaan e-Mel di MDTM hendaklah dipantau secara berterusan oleh Pentadbir e-Mel untuk memenuhi keperluan etika penggunaan e-Mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"* dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: (a) Akaun atau alamat mel elektronik (e-Mel) yang diperuntukkan oleh MDTM sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (b) Setiap e-Mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh MDTM; (c) Memastikan subjek dan kandungan e-Mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;	Semua

(d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-Mel rasmi dan pastikan alamat e-Mel penerima adalah betul; (e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10MB) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; (f) Pengguna hendaklah mengelak dari membuka e-Mel daripada penghantar yang tidak diketahui atau diragui; (g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-Mel; (h) Setiap e-Mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; (i) e-Mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; (j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; (k) Mengambil tindakan dan memberi maklum balas terhadap e-Mel dengan cepat dan mengambil tindakan segera; (l) Pengguna hendaklah memastikan alamat e-Mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan (m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbo*x* masing-masing.	Semua

P06(09) Perkhidmatan Elektronik	
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
P06(09) 01 – e-Perkhidmatan	**Tindakan**
Bagi menggalakkan pertumbuhan e-Perkhidmatan serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat yang terlibat dalam e-Perkhidmatan perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Semua

P06(09) 02 – Maklumat Umum	Tindakan
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; (b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua

P06(10) Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
P06(10) 01 – Pengauditan dan Semakan ICT	**Tindakan**
CIO dan ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT MDTM; (b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery,phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*);	CIO,ICTSO

(c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; (g) Aktiviti penyalahgunaan akaun e-Mel; dan (h) Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Rangkaian ICT/CIO/ICTSO.	CIO,ICTSO
P06(10) 02 – Jejak Audit	**Tindakan**
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.	CIO/ICTSO

Pengendalian Jejak audit hendaklah memastikan perkara-perkara berikut:- (a) Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. (b) CIO/ICTSO 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. (c) Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	CIO/ICTSO
P06(10) 03 – Sistem Log	**Tindakan**
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, ICTSO hendaklah melaporkan kepada CIO.	CIO/ICTSO

P06(10) 04 – Pemantauan Log	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; (c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; (e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan (f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MDTM atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	CIO/ICTSO , Pentadbir Rangkaian ICT

PERKARA 7 – KAWALAN CAPAIAN

P07(01) Dasar Kawalan Capaian

Objektif:

Mengawal capaian ke atas maklumat yang menggunakan aset ICT MDTM.

P07(01) 01- Keperluan Kawalan Capaian	Tindakan
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.	BTM, ICTSO

P07(02) Pengurusan Capaian Pengguna

Objektif:

Mengawal capaian pengguna ke atas aset ICT MDTM.

P07(02) 01- Akaun Pengguna	Tindakan
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh MDTM sahaja boleh digunakan; (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan tertakluk kepada peraturan MDTM. Akaun boleh ditarik balik jika penggunanya melanggar peraturan. (d) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (e) Bahagian Teknologi Maklumat boleh membeku dan menamatkan akaun pengguna atas sebab-sebab tertentu: i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	Semua, ICTSO

P07(02) 02 - Hak Capaian	Tindakan
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	CIO/ICTSO
P07(02) 03 - Pengurusan Kata Laluan	**Tindakan**
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MDTM 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 dua belas (12) 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;	Semua,ICTSO

(j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan (k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
P07(02) 04 - *Clear Desk* dan *Clear S*creen	**Tindakan**
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 bagi mengelakkan kerosakan, kecurian atau kehilangan.Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan katalaluan bagi *screen saver* atau log keluar apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Semua
P07(03) Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
P07(03) 01 - Capaian Rangkaian	**Tindakan**
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MDTM, rangkaian agensi lain dan rangkaian awam;, (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Semua, CIO, ICTSO

P07(03) 02 - Capaian Internet	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di MDTM hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja untuk melindungi daripada kemasukan malicious code, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MDTM; (b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (video conferencing, video streaming, chat, downloading) adalah perlu bagi menguruskan penggunaan jalur lebar (bandwidth) yang maksimum dan lebih berkesan; (d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. CIO /ICTSO berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; (e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Pengarah/ pegawai yang diberi kuasa; (f) Bahan yang diperoleh daripada Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; (g) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan/Ketua Bahagian sebelum dimuat naik ke Internet; (h) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MDTM; (i) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan penuh talian internet. Walau bagaimanapun, penggunaan talian internet masih dipantau oleh CIO / ICTSO; (j) Penggunaan sebarang modem/modem mudahalih bukan milik MDTM bagi tujuan sambungan ke Internet adalah tidak dibenarkan sama sekali; dan	Semua,CIO, ICTSO

(k) 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.	

P07(04) Kawalan Capaian Sistem Pengoperasian

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

P07(04) 01 - Capaian Sistem Pengoperasian	**Tindakan**
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: (a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan (b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (a) Mengesahkan pengguna yang dibenarkan; (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf super user; dan (c) Menjana amaran (alert) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem.	Semua, CIO, ICTSO

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log masuk yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	

P07(05) Kawalan Capaian Aplikasi dan Maklumat

Objektif:

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

P07(05) 01 - Capaian Aplikasi dan Maklumat	**Tindakan**
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; (b) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan (c) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	CIO, ICTSO

P07(06) Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
P07(06) 01 - Peralatan Mudah Alih	**Tindakan**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
P07(06) 02 - Kerja Jarak Jauh (*Remote Access*)	**Tindakan**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salahguna kemudahan.	Semua

PERKARA 8 – PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

P08(01) Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif:

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

P08(01) 01 - Keperluan Keselamatan Sistem Maklumat	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem oleh CIO hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; (c) Aplikasi perlu mengandungi semakan pengesahan (validation) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik Sistem, CIO, ICTSO

P08(01) 02 - Pengesahan Data Input dan Output	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan adalah betul dan bersesuaian; dan (b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem, CIO, ICTSO

P08(02) Kawalan Kriptografi

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

P08(02) 01 - Penyulitan/Enkripsi	Tindakan
Pengguna hendaklah membuat penyulitan/enkripsi (encryption) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua

P08(02) 02 - Tandatangan Digital	Tindakan
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua

P08(02) 03 - Pengurusan Infrastruktur Kunci Awam (PKI)	Tindakan
Pengurusan Kunci Awam hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua

P08(03) Keselamatan Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
P08(03) 01 - Kawalan Fail Sistem	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh CIO/ICTSO atau pegawai yang dibenarkan mengikut prosedur yang telah ditetapkan; (b) Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; (c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan (e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem, CIO,ICTSO

P08(04) Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
P08(04) 01 - Prosedur Kawalan Perubahan	**Tindakan**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pemilik Sistem,

(a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (d) Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan (e) Menghalang sebarang peluang untuk membocorkan maklumat.	CIO,ICTSO
P08(04) 02 - Pembangunan Perisian Secara *Outsource*	**Tindakan**
Pembangunan perisian secara outsource perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (source code) bagi semua aplikasi dan perisian adalah menjadi hak milik MDTM.	Pemilik Sistem, BTM, CIO,ICTSO

P08(05) Kawalan Teknikal Keterdedahan (Vulnerability)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
P08(05) 01 - Kawalan dari Ancaman Teknikal	**Tindakan**
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.	CIO

PERKARA 9 – PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

P09(01) Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

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

P09(01) 01 - Mekanisme Pelaporan	Tindakan
Insiden keselamatan ICT bermaksud musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada CIO dan ICTSO dengan kadar segera: (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	Semua

Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	

P09(02) Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:

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

P09(02) 01 - Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	**Tindakan**
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 MDTM. 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 aktiviti penyalinan; (c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO

PERKARA 10 – PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

P10(01) Dasar Kesinambungan Perkhidmatan	
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
P10(01) 01 – Pelan Kesinambungan Perkhidmatan	**Tindakan**
Pelan Kesinambungan Perkhidmatan (Business Continuity Management -BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JKPP MDTM. Perkara-perkara berikut perlu diberi perhatian: (a) Mengenalpasti 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 serta mengemaskini pelan sekurang-kurangnya setahun sekali.	CIO/ICTSO

Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel MDTM dan pembekal berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; dan (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh. BCM yang telah dibangunkan hendaklah melalui proses berikut: (a) Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. (b) Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. (c) Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. (d) Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. (e) Salinan pelan BCM hendaklah sentiasa dikemaskini dan dilindungi seperti di lokasi utama.	

PERKARA 11 – PEMATUHAN

P11(01) Mekanisme Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT MDTM.	
P11(01) 01 - Pematuhan Dasar	**Tindakan**
Pematuhan Dasar merangkumi perkara berikut: (a) Setiap pengguna di MDTM hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MDTM juga undang-undang atau peraturan-peraturan lain yang berkaitan yang telah dikuatkuasakan. (b) Semua aset ICT di MDTM termasuk maklumat yang disimpan didalamnya adalah hak milik Kerajaan. Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. (c) Sebarang penggunaan aset ICT MDTM selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber MDTM.	Semua
P11(01) 02 - Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	**Tindakan**
Untuk memenuhi perkara di atas, perkara berikut hendaklah dilaksanakan: (a) ICTSO hendaklah memastikan semua prosedur keselamatan	ICTSO

dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. (b) Sistem maklumat perlu diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.	
P11(01) 03 - Pematuhan Keperluan Audit	**Tindakan**
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Perkara yang perlu dilaksanakan adalah seperti berikut: (a) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. (b) Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
P11(01) 04 – Pematuhan Perundangan	**Tindakan**
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MDTM: (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;	Semua

(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 Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
(m) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
(n) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
(o) Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
(p) Akta Rahsia Rasmi 1972;
(q) Akta Tandatangan Digital 1997;
(r) Akta Hak Cipta (Pindaan) Tahun 1997;
(s) Akta Komunikasi dan Multimedia 1998;
(t) Akta Jenayah Komputer 1997;
(u) Akta Aktiviti Kerajaan Elektronik 2007;
(v) Perintah-Perintah Am;
(w) Arahan Perbendaharaan;

(x) Arahan Teknologi Maklumat 2007; (y) Garis Panduan IT Outsourcing Agensi-agensi Sektor Awam Tahun 2006 yang dikeluarkan oleh Jabatan Perdana Menteri; (z) Polisi Panduan Penggunaan Internet dan Emel Kakitangan Majlis Perbandaran Klang pada 26 Januari 2004; (aa) Surat Aku Janji; (bb) Manual Prosedur; (cc) Fail Meja Kakitangan.	
P11(01) 05 - Pelanggaran Dasar	**Tindakan**
Pelanggaran Dasar Keselamatan ICT MDTM boleh dikenakan tindakan tatatertib.	Semua

Lampiran 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT MAJLIS DAERAH TANJONG MALIM

Nama (Huruf Besar) : ……

No. Kad Pengenalan : …….

Jawatan : **.....**……...

Jabatan/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 MDTM; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : ..... Tarikh : .....

.....	.....
Pengesahan	Pengesahan
Ketua Pegawai Keselamatan	Ketua Pegawai Maklumat
Teknologi Maklumat	(CIO)
(ICTSO)	