KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

DASAR KESELAMATAN ICT

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI

Dasar Keselamatan ICT MOSTI
Diterbitkan Pada April 2017 (Versi 3.0)

ISI KANDUNGAN

SEJARAH DASAR KESELAMATAN ICT

TARIKH	EDISI	KELULUSAN	TARIKH KUATKUASA
1 Jun 2008	1.0	JPICT	1 Jun 2008
1 Mac 2012	2.0	JPICT	1 Mac 2012
1 Feb 2015	2.1	JPICT	1 Mei 2015
1 Feb 2017	3.0	JPICT	1 April 2017

JADUAL PINDAAN DASAR KESELAMATAN ICT

TARIKH	Edisi	BUTIRAN PINDAAN
1 Jun 2010	**1.1**	
Feb 2015	**2.1**	Telah diluluskan melalui Mesyuarat JPICT bertarikh 16 Februari 2015
Feb 2017	**3.0**	Telah diluluskan melalui Mesyuarat JPICT bertarikh 20 Februari 2017

TERMA DAN DEFINISI

Bahagian ini menerangkan istilah-istilah utama yang digunakan di dalam dasar ini:

Akaun pengguna	Akaun e-mel.
Aset ICT	Data, maklumat, perkakasan, perisian, aplikasi, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab MOSTI.
BPTM	Bahagian Pengurusan Teknologi Maklumat, MOSTI.
Dokumen	Semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut (*soft copy*), elektronik, dalam talian, kertas lutsinar, risalah atau slaid.
Insiden	Musibah (*adverse event*) yang berlaku ke atas sistem aplikasi dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Kawasan Larangan	Kawasan yang dihadkan kemasukan oleh pegawai-pegawai yang tertentu sahaja atau kawasan-kawasan premis atau sebahagian dari premis di mana perkara-perkara terperingkat disimpan atau diuruskan atau di mana kerja terperingkat dijalankan.
Maklumat Terperingkat	Dokumen/Maklumat Rasmi yang dikategorikan sebagai Rahsia Besar dan Rahsia.
Malware	Merujuk kepada virus, *worms, trojan horses*, *bots* dan lain-lain kod jahat.

Bahagian ini menerangkan istilah-istilah utama yang digunakan di dalam dasar ini:

Media storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti telefon bimbit, kad memori, disket, kartrij, cakera padat, cakera mudah alih, pita, cakera keras dan pemacu pena.
Peralatan mudah alih	Perkakasan seperti telefon bimbit, komputer peribadi, komputer tablet, projektor, *pendrive*, *external* HDD, gajet ICT dan alat-alat rangkaian komunikasi.
Penggodam	Penceroboh sistem PC dengan melakukan aktiviti seperti pencurian maklumat, mengubahsuai laman web, penyebaran virus, menyesakkan rangkaian, merosakkan PC dan pelbagai lagi aktiviti negatif dalam dunia ICT.
Pengguna	Warga MOSTI yang menggunakan aset ICT.
Pihak Ketiga	Pihak atau pembekal yang membekalkan perkhidmatan kepada MOSTI.
Rahsia Besar	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia, hendaklah diperingkatkan Rahsia Besar.
Sulit	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan kerajaan atau orang perseorangan atau akan menyebabkan keadaan

Bahagian ini menerangkan istilah-istilah utama yang digunakan di dalam dasar ini:

	memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing hendaklah diperingkatkan sulit.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakan juga diberi satu tahap perlindungan keselamatan hendaklah diperingkatkan Terhad.
DKICT	Dasar Keselamatan ICT MOSTI.
JPICT	Jawatankuasa Pemandu ICT MOSTI.
ICT	*Information and Communication Technology* atau Teknologi Maklumat dan Komunikasi.
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindakbalas Kecemasan Kerajaan – Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden ICT di agensi masing-masing dan agensi di bawah kawalannya.
Vulnerability	Kelemahan pada sistem dan aplikasi yang membenarkan serangan berlaku dan menjejaskan tahap keselamatan maklumat.
Stress Test	Ujian ke atas sistem, aplikasi dan perkakasan yang memberi penekanan kepada prestasi, ketersediaan dan kawalan ralat semasa beban puncak.
Load Test	Ujian capaian sistem aplikasi *online* bagi menguji tahap ketahanan ke sistem daripada capaian yang banyak.

Bahagian ini menerangkan istilah-istilah utama yang digunakan di dalam dasar ini:

Penetration Test	Kaedah menilai tahap keselamatan sistem komputer atau rangkaian dengan melakukan simulasi serangan daripada dalaman dan luaran.
Outsource	Perolehan kementerian bagi mendapatkan perkhidmatan dan pembekalan daripada pihak luar.
Inhouse	Perkhidmatan yang dilaksanakan secara dalaman kementerian menggunakan sumber manusia yang sedia ada.
Jabatan/Agensi di bawah MOSTI	Agensi kerajaan dibawah MOSTI iaitu Jabatan Kimia Malaysia, Jabatan Meteorologi Malaysia, Jabatan Standard Malaysia, Agensi Remote Sensing Malaysia, Agensi Angkasa Malaysia, Agensi Nuklear Malaysia dan Lembaga Perlesenan Tenaga Atom.
Kawasan Terhad	Kawasan yang dikawal diberikan kebenaran hanya kepada pegawai-pegawai tertentu yang dipertanggungjawabkan untuk melaksanakan tugas. Contoh adalah seperti bilik-bilik ketua bahagian, bilik-bilik fail, bilik Sistem PABX dan Pusat Data MOSTI.
Pegawai yang diberikan kuasa	Pegawai yang diberikan kebenaran serta tanggungjawab bagi melaksanakan tugas atau memasuki kawasan-kawasan terhad.
Pengguna yang bertanggungjawab	Pengguna yang dikhususkan untuk mengurus, memantau, mengendali dan melaksanakan sesuatu tugas.

Bahagian ini menerangkan istilah-istilah utama yang digunakan di dalam dasar ini:

Pegawai Keselamatan MOSTI	Pegawai yang menjalankan tugas menyedia dan memastikan keselamatan personel dan fizikal di Ibu Pejabat MOSTI.
Pegawai Aset	Pegawai yang dilantik untuk menjaga dan menguruskan aset di Ibu Pejabat MOSTI.
Agensi luar	Individu atau organisasi kerajaan/swasta yang berurusan dengan MOSTI.
Pejabat Ketua Pegawai Keselamatan Kerajaan	Badan yang memberi khidmat nasihat keselamatan perlindungan kepada Kerajaan Negeri, Kementerian, Jabatan dan agensi kerajaan dengan tujuan untuk membantu mengekalkan tahap keselamatan fizikal, keselamatan dokumen dan keselamatan personel di semua agensi kerajaan yang ditetapkan oleh kerajaan dari semasa ke semasa bagi melindungi terhadap espionaj dan sabotaj serta daripada kebocoran maklumat tanpa kebenaran daripada semua jabatan dan agensi kerajaan.
Bahagian Pentadbiran MOSTI	Bahagian yang bertanggungjawab menyediakan perkhidmatan infrastruktur kerja, keselamatan, penyelenggaraan persekitaran kerja dan perkhidmatan-perkhidmatan lain yang berkaitan di MOSTI.
Penyelenggara Bangunan	Pihak ketiga atau kontraktor yang dilantik dan diberi tanggungjawab untuk menyelenggara bangunan dan infrastruktur komunikasi dan teknikal di MOSTI.

Bahagian ini menerangkan istilah-istilah utama yang digunakan di dalam dasar ini:

Ketua Agensi	Ketua Pengarah dan Ketua Pegawai Eksekutif jabatan-jabatan di bawah MOSTI.
Pengguna Kad EG	Pengguna yang diberikan Kad EG dan bertanggungjawab bagi menjalankan transaksi kewangan menggunakan aplikasi kerajaan EG NET.
Public Key Infrastructure (PKI)	PKI adalah komunikasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi untuk melindungi keselamatan komunikasi dan transaksi di Internet.
Pelawat	Individu / Kumpulan yang datang berurusan di MOSTI secara rasmi atau tidak rasmi
Pegawai Yang Bertanggungjawab	Pegawai yang diberikan tanggungjawab melaksanakan sesuatu tugas.
PKP	Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan*)
Koordinator PKP	Pegawai bertanggungjawab menguruskan dan melaksanakan Pelan Kesinambungan Perkhidmatan (PKP) MOSTI

PENDAHULUAN

1. PENGENALAN

Tujuan dokumen ini adalah untuk memaklumkan peraturan-peraturan yang perlu dipatuhi oleh semua pengguna Teknologi Maklumat dan Komunikasi (ICT) untuk menjaga keselamatan aset. Dengan adanya peraturan ini adalah diharapkan tahap keselamatan ICT dan langkah-langkah mengurangkan risiko ancaman dari dalam dan luar ke atas sistem dan infrastruktur ICT MOSTI dapat ditingkatkan. DKICT MOSTI dibangunkan untuk mematuhi Pekeliling Am Bilangan 3 Tahun 2000: Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan dan selari dengan kehendak MS ISO/IEC 27001:2013 serta arahan-arahan lain yang terkini dan berkuatkuasa.

2. OBJEKTIF

Objektif DKICT MOSTI adalah seperti berikut:

a. Memastikan kelancaran operasi kerajaan amnya dan MOSTI khasnya berterusan, meminimakan kerosakan atau kemusnahan melalui usaha pencegahan atau usaha mengurangkan kesan insiden yang tidak diingini;
b. Melindungi kepentingan pengguna sistem aplikasi daripada menghadapi kegagalan dan/atau kelemahan kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;
c. Memastikan aset ICT terlindung daripada ancaman pencerobohan/penggodaman, kecurian data, serangan *malware* dan penafian perkhidmatan; dan
d. Mencegah kes-kes penyalahgunaan serta kehilangan aset ICT kerajaan.

3. SKOP

Dasar ini meliputi semua aset ICT yang digunakan seperti maklumat (contoh: fail, dokumen, data elektronik), perisian (contoh: aplikasi dan pangkalan data) dan fizikal (contoh: Pusat Data, PC, server, peralatan komunikasi, media magnet dan lain-lain). Dasar ini adalah terpakai oleh semua pengguna di MOSTI termasuk pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, memuat naik, menyedia, berkongsi, menyimpan dan menggunakan aset ICT MOSTI.

4. PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT MOSTI 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 Arahan Keselamatan.

b. **Hak akses minimum**

Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan daripada pegawai yang dipertanggungjawabkan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah, membatalkan atau mencetak sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas atau perubahan dasar MOSTI.

c. **Akauntabiliti**

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT MOSTI.

d. **Pengasingan**

Tugas mewujud, memadam, menambah, mengubah dan mengesahkan data/maklumat perlu diasingkan. Ini adalah untuk mengelakkan akses yang tidak dibenarkan dan melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi.

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 PC, server, peralatan rangkaian/keselamatan dan sebagainya hendaklah dipastikan dapat menjana dan menyimpan log untuk tujuan *audit trail*.

f. **Pematuhan**

DKICT MOSTI hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk ketidakpatuhan ke atasnya yang boleh membawa ancaman kepada keselamatan ICT.

g. **Pemulihan**

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimakan sebarang gangguan atau kerugian perkhidmatan akibat daripada *unavailability* sistem. Pemulihan boleh dilakukan melalui kaedah *redundancy* dan mewujudkan Pelan Kesinambungan Perkhidmatan (PKP) dan Pelan Pemulihan Bencana (DRP).

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 ICT adalah perlu bagi menjamin keselamatan ICT yang maksimum.

BAB 1

PEMBANGUNAN DAN PENYELENGGARAAN DASAR KESELAMATAN ICT

Dasar Keselamatan ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat ICT selaras dengan keperluan MOSTI dan perundangan yang berkaitan.	
1.1 Pelaksanaan Dasar Keselamatan ICT	**Tanggungjawab**
Ketua Setiausaha adalah bertanggungjawab ke atas pelaksanaan arahan dengan dibantu oleh Jawatankuasa Pemandu ICT yang terdiri daripada Ketua Agensi, Ketua Bahagian, Ketua Pegawai Maklumat (CIO) dan Pegawai Keselamatan ICT (ICTSO).	Ketua Setiausaha, CIO dan ICTSO
1.2 Penyebaran Dasar Keselamatan ICT	
DKICT perlu disebarkan kepada semua pengguna ICT yang berkaitan melalui medium penyampaian yang bersesuaian.	ICTSO
1.3 Penyelenggaraan Dasar Keselamatan ICT	
DKICT adalah tertakluk kepada semakan dan pindaan selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan DKICT MOSTI: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan secara bertulis kepada CIO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT); c. Perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna; dan d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	ICTSO
1.4 Pengecualian Dasar Keselamatan ICT	
DKICT adalah terpakai kepada semua pengguna ICT MOSTI dan tiada pengecualian diberikan.	Pengguna dan Pihak Ketiga

BAB 2

KESELAMATAN ORGANISASI

Infrastruktur Organisasi Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif **DKICT MOSTI**.	
2.1 Ketua Setiausaha	**Tanggungjawab**
Peranan dan tanggungjawab Ketua Setiausaha adalah seperti berikut: a. Memastikan pelaksanaan Jawatankuasa Pemandu ICT (JPICT) MOSTI merangkumi perkara mengenai keselamatan ICT MOSTI; b. Memastikan semua pengguna mematuhi DKICT MOSTI terkini; c. Merancang semua keperluan berkaitan keselamatan ICT untuk organisasi (sumber kewangan, sumber pengguna dan perlindungan keselamatan) adalah mencukupi; dan d. Memastikan penilaian risiko dan program keselamatan ICT di dalam DKICT MOSTI mengikut peraturan-peraturan yang sedang berkuatkuasa.	Ketua Setiausaha
2.2 Ketua Pegawai Maklumat (CIO)	
Setiausaha Bahagian Kanan (Pengurusan) dilantik sebagai CIO MOSTI. Peranan dan tanggungjawab beliau adalah seperti berikut: a. Mewujud dan mengetuai pasukan kerja keselamatan ICT MOSTI; b. Membantu Ketua Setiausaha dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; c. Menjadi penasihat keselamatan ICT; d. Menyelaras pembangunan dan pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; e. Memastikan semua pengguna memahami dan mematuhi DKICT MOSTI;	SUBK(P)

f. Memastikan semua keperluan organisasi (sumber kewangan, sumber pengguna dan perlindungan keselamatan) adalah mencukupi; dan g. Merancang penilaian risiko dan program keselamatan ICT di dalam DKICT MOSTI mengikut peraturan-peraturan yang sedang berkuatkuasa	
2.3 Pegawai Keselamatan ICT (ICTSO)	
Setiausaha Bahagian Pengurusan Teknologi Maklumat dilantik sebagai ICTSO MOSTI. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Mengurus pelaksanaan keseluruhan program keselamatan ICT MOSTI; b. Memberi penerangan dan pendedahan serta menguatkuasakan DKICT MOSTI kepada semua pengguna; c. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT MOSTI; d. Menjalankan pengurusan risiko; e. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; f. Menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. Memberi amaran terhadap kemungkinan berlakunya ancaman siber seperti virus, spam dan lain-lain; h. Memberi khidmat nasihat dan menyediakan langkah-langkah perlindungan yang bersesuaian; i. Melaporkan insiden keselamatan ICT kepada CERT MOSTI dan memaklumkannya kepada CIO serta GCERT MAMPU; j. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;	SUB(PTM)

k. Melaporkan insiden keselamatan ICT kepada CIO bagi insiden yang memerlukan pelaksanaan Pelan Kesinambungan Perkhidmatan (PKP); dan l. Mengesyor dan menyokong proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar DKICT MOSTI.	
2.4 Pengurus ICT	
Pengurus-pengurus ICT bagi MOSTI ialah Ketua Penolong Setiausaha Bahagian PTM dan MASTIC. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MOSTI; b. Menentukan kawalan akses semua pengguna terhadap aset ICT MOSTI; c. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; d. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MOSTI; dan e. Memastikan pelaksanaan DKICT dipatuhi dalam operasi seperti berikut: i. Pelaksanaan sistem atau aplikasi baru samada dibangunkan secara dalaman atau luaran yang melibatkan teknologi baru; dan ii. Perolehan perkakasan dan perisian ICT yang diperlukan.	KPSU(PTM)OP KPSU(PTM)AK KPSU(PTM)AP KPSU (MASTIC) Seksyen ICT
2.5 Pentadbir Sistem ICT	
Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap akses berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT MOSTI;	Pentadbir Sistem ICT MOSTI

c. Memantau dan menyediakan laporan mengenai aktiviti akses kepada pemilik maklumat berkenaan secara berkala. d. Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan/penggodaman dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. Memastikan pembangunan sistem aplikasi mengambil kira dan mematuhi ciri-ciri keselamatan yang termaktub di dalam DKICT MOSTI; dan f. Menyimpan dan menganalisis rekod audit trail.	
2.6 Pengguna	
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: a. Membaca, memahami dan mematuhi DKICT MOSTI; b. Menandatangani Surat Akuan Pematuhan DKICT MOSTI; c. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; d. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; e. Melaksanakan prinsip-prinsip DKICT MOSTI dan menjaga kerahsiaan maklumat MOSTI; f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan g. Menghadiri program-program kesedaran mengenai keselamatan ICT.	Pengguna
2.7 Jawatankuasa Pemandu ICT (JPICT) MOSTI	
JPICT adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam MOSTI. Bidang kuasa: a. Memperakukan/meluluskan dokumen DKICT MOSTI; b. Memantau tahap pematuhan keselamatan ICT;	JPICT MOSTI

c. Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam MOSTI yang mematuhi keperluan DKICT MOSTI; d. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; e. Memastikan DKICT MOSTI selaras dengan dasar-dasar ICT kerajaan semasa; f. Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; g. Membincang tindakan yang melibatkan pelanggaran DKICT MOSTI; dan h. Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	
2.8 Pasukan Tindak Balas Insiden Keselamatan ICT MOSTI (CERT MOSTI)	
Keanggotaan CERT MOSTI adalah seperti berikut: Pengarah : Setiausaha Bahagian Kanan (Pengurusan) Pengurus : Setiausaha Bahagian Pengurusan Teknologi Maklumat Ahli : (1) Pegawai Teknologi Maklumat di Ibu Pejabat MOSTI dan Jabatan dibawah MOSTI; dan (2) Penolong Pegawai Teknologi Maklumat di Ibu Pejabat MOSTI dan Jabatan dibawah MOSTI. Peranan dan tanggungjawab CERT MOSTI adalah seperti berikut: a. Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; b. Merekod dan menjalankan siasatan awal insiden yang diterima;	CERT MOSTI

c. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minima; d. Menghubungi dan melapor insiden yang berlaku kepada GCERT MAMPU samada sebagai input atau untuk tindakan seterusnya; e. Menasihat Jabatan di bawah MOSTI mengambil tindakan pemulihan dan pengukuhan; f. Menyebarkan makluman berkaitan dengan agensi di bawah kawalannya; dan g. Menjalankan penilaian dalaman untuk mempastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
2.9 Jawatankuasa Keselamatan ICT (JKICT) MOSTI	
Keanggotaan Jawatankuasa Keselamatan ICT adalah seperti berikut: Pengerusi : Pegawai Keselamatan ICT (ICTSO) Ahli : Pegawai Teknologi Maklumat atau Penolong Pegawai Teknologi Maklumat Dalam Bidang-Bidang Berikut : (1) Sistem Aplikasi; (2) Sistem Pengoperasian; dan (3) Rangkaian dan Keselamatan. Urus Setia : Seksyen Operasi, Rangkaian dan Keselamatan, BPTM Peranan dan tanggungjawab JKICT MOSTI adalah seperti berikut: a. Merancang, melaksana, menyemak dan memantau dasar, strategi dan pelan tindakan keselamatan ICT MOSTI;	JKICT MOSTI

b. Merancang, melaksana, menyelaras dan memantau pengurusan keselamatan ICT MOSTI; c. Mengkaji dan menilai teknologi yang bersesuaian terhadap keperluan keselamatan ICT; d. Menjalankan penilaian ke atas tahap keselamatan ICT MOSTI dan mengambil tindakan pengukuhan atau pemulihan; dan e. Mengambil tindakan terhadap sebarang insiden yang dilaporkan.	
Pihak Ketiga/Luar	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Perunding dan lain-lain).	
2.10 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	**Tanggungjawab**
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 DKICT MOSTI; b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d. Memastikan akses kepada infrastruktur ICT MOSTI perlu berlandaskan pada kontrak perjanjian; e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam kontrak perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. DKICT MOSTI; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek;	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

f. Menandatangani *Non-Disclosure Agreement* (NDA) sebagaimana **Lampiran 1.**	

BAB 3

KAWALAN DAN PENGELASAN ASET

Akauntabiliti Aset	
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MOSTI.	
3.1 Inventori Aset ICT	**Tanggungjawab**
Semua aset ICT MOSTI hendaklah direkodkan. Ini termasuklah mengenalpasti aset, mengkategorikan aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya. Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal, sistem pengurusan aset MOSTI dan inventori 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 MOSTI; d. Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, di dokumen dan dilaksanakan; dan e. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT dibawah kawalannya. f. Memastikan penggunaan aset gunasama direkodkan dalam buku daftar pengguna (*logbook*) dan pegawai aset / pegawai yang dipertanggungjawabkan mesti memastikan aset tersebut berada di dalam keadaan yang baik selepas penggunaan.	Pentadbir Sistem ICT dan Pengguna

Kategori dan Pengendalian Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
3.2 Kategori Maklumat	
Setiap maklumat yang dikategori mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	Pengguna
3.3 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira perkara-perkara 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 dan mengikut pekeliling yang berkuatkuasa; **f.** Memberi perhatian khususnya kepada maklumat terperingkat; dan **g.** Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Pengguna
3.4 Perlindungan Ketirisan Data	
Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran.	Pengguna

Teknologi yang bersesuaian dengan keadaan semasa dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.	

BAB 4

KESELAMATAN SUMBER MANUSIA

Keselamatan Sumber Manusia Dalam Tugas Harian	
Objektif: Memastikan semua pengguna dan pihak ketiga : i. Memahami tanggungjawab dan peranan; ii. Meningkatkan pengetahuan dan kesedaran; dan iii. Menguruskan aspek keselamatan secara teratur dalam mengurangkan risiko penyalahgunaan keselamatan aset ICT. Semua pengguna dan pihak ketiga hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.	
4.1 Tanggungjawab Keselamatan Sebelum Dalam Perkhidmatan	**Tanggungjawab**
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Menjelaskan peranan dan tanggungjawab pengguna serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pegawai dan pengguna berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan dan ditandatangani.	ICTSO, Pengguna dan Pihak Ketiga
4.2 Tanggungjawab Keselamatan Semasa Dalam Perkhidmatan	
Memastikan semua pengguna dan pihak ketiga sedar akan ancaman keselamatan maklumat dan perkakasan serta memahami peranan dan tanggungjawab masing-masing untuk mematuhi DKICT MOSTI. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	ICTSO, Pengguna dan Pihak Ketiga

a. Memastikan pengguna serta pihak ketiga mematuhi keselamatan aset ICT berdasarkan kepada dasar dan peraturan yang ditetapkan oleh MOSTI; b. Memastikan pengguna menjalani latihan kesedaran dan perubahan yang berkaitan dengan dasar dan peraturan keselamatan aset ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; c. Mempertimbangkan tindakan tatatertib dan/atau undang-undang ke atas pengguna dan pihak ketiga sekiranya berlaku pelanggaran dengan dasar dan peraturan yang telah ditetapkan; dan d. Memastikan pengguna menjalani latihan yang berkaitan supaya setiap kemudahan ICT hendaklah digunakan dengan cara dan kaedah yang telah ditetapkan.	
4.3 Bertukar/Tamat Perkhidmatan/Cuti Belajar	
Memastikan semua pengguna yang bertukar/tamat perkhidmatan/cuti belajar mematuhi perkara-perkara berikut: a. Memulangkan semua aset ICT Kerajaan yang diterima semasa perkhidmatan dikembalikan mengikut peraturan yang berkuatkuasa; dan b. Membatal atau menangguhkan semua kebenaran akses ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan.	ICTSO, Pentadbir Sistem ICT, Pengguna dan Pihak Ketiga
4.4 Program Kesedaran Keselamatan ICT	
Setiap pengguna di MOSTI perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program kesedaran menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT.	ICTSO dan Pengguna

BAB 5

KESELAMATAN FIZIKAL DAN PERSEKITARAN

Keselamatan Kawasan	
Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
5.1 Keselamatan Fizikal	**Tanggungjawab**
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh premis. Langkah-langkah keselamatan fizikal adalah seperti berikut: a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan dan kunci harus disimpan oleh pegawai bertanggungjawab; c. Memperkukuhkan dinding dan siling; d. Memasang alat penggera dan sistem CCTV; e. Menghadkan jalan keluar masuk; f. Mengadakan kaunter kawalan; g. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; h. Mewujudkan perkhidmatan kawalan keselamatan; i. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang mendapat kebenaran sahaja untuk masuk; j. Merekabentuk dan melaksanakan perlindungan fizikal daripada bencana seperti kebakaran, banjir, letupan atau huru hara; k. Menyediakan garis panduan keselamatan untuk kakitangan yang bekerja di dalam kawasan terhad;	Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO), Pegawai Keselamatan MOSTI, CIO, ICTSO dan Pegawai Bertanggung-jawab

l. Sistem kawalan kunci; Terdapat pegawai yang bertanggungjawab untuk menyimpan kunci dengan baik dan mempunyai rekod; dan m. Mewujudkan kawalan di kawasan penghantaran, pemunggahan dan kawasan larangan.	
5.2 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pengguna hendaklah memakai Pas Keselamatan sepanjang waktu bertugas; b. Setiap pelawat mestilah mendaftar dan mendapatkan Pas Pelawat di pintu masuk utama MOSTI untuk ke kawasan/tempat berurusan dan hendaklah dikembalikan semula selepas tamat urusan; c. Semua Pas Keselamatan hendaklah diserahkan semula kepada MOSTI apabila pengguna bertukar, berhenti atau bersara; dan d. Kehilangan Pas Keselamatan mestilah dilaporkan dengan segera kepada Pegawai Keselamatan MOSTI.	Pengguna dan Pelawat.
5.3 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di MOSTI adalah Blok C4 dan C5. a. Akses kepada kawasan tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja; b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan mendapat kebenaran untuk temujanji. Mereka hendaklah diiringi sepanjang masa sehingga tugas atau temujanji di kawasan berkenaan selesai; dan	Pengguna, Jabatan dibawah MOSTI, Pihak Ketiga, Agensi luar dan Pelawat.

c. Semua aktiviti Pihak ketiga di kawasan larangan perlu mendapat kebenaran daripada pegawai yang diberi kuasa dan dipantau serta dikawal oleh pegawai bertanggungjawab.	
Keselamatan Peralatan ICT Dan Maklumat	
Objektif: Melindungi peralatan ICT dan maklumat dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
5.4 Peralatan ICT	
Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan dengan mengambil tindakan berikut: a. Setiap pengguna hendaklah memeriksa dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna dan melaporkan sebarang kerosakan kepada Pegawai Aset ICT MOSTI; b. Setiap pengguna adalah bertanggungjawab ke atas kerosakan dan kehilangan peralatan ICT di bawah kawalannya; c. Semua peralatan ICT hendaklah disimpan atau diletakkan ditempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; d. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; e. Pengguna bertanggungjawab sepenuhnya ke atas peralatan ICT dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; f. Pengguna mesti mendapat kebenaran daripada ICTSO atau atau pegawai yang diberikan kuasa untuk membuat instalasi perisian tambahan; g. Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemaskini disamping melakukan imbasan ke atas media storan yang digunakan; h. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;	Pengguna, Pentabir Sistem ICT dan Pihak Ketiga

i. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); j. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; k. Peralatan ICT yang hendak dibawa keluar dari premis MOSTI untuk tujuan rasmi, perlu mendapat kelulusan pegawai yang diberikan kuasa dan direkodkan bagi tujuan pemantauan; l. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; m. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa; n. Pengguna mesti mendapat kebenaran daripada ICTSO atau atau pegawai yang diberikan kuasa untuk mengubah kedudukan komputer dari tempat asal; o. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada pegawai yang bertanggungjawab untuk dibaik pulih; p. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; q. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; r. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem ICT; s. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; t. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; dan u. Memastikan plug dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum	

meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
5.5 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk, flash disk*, *thumb drive, external drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan Tindakan berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan adalah terjamin dan selamat: a. Sediakan ruang penyimpanan yang kondusif dan selamat serta bersesuaian dengan kandungan maklumat; b. Mendapatkan kebenaran terlebih dahulu sebelum memasuki kawasan penyimpanan media storan. Kawasan ini adalah terhad kepada mereka yang dibenarkan sahaja; c. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; d. Merekodkan pergerakan media storan untuk tujuan pinjaman; e. Mendapat kelulusan pemilik maklumat terlebih dahulu sebelum menghapuskan maklumat atau kandungan media storan dengan teratur dan selamat; f. 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; g. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; dan	Pengguna dan Pentabir Sistem ICT

h. Perkakasan backup hendaklah diletakkan di tempat yang terkawal.	
5.6 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 pegawai yang bertanggungjawab untuk tindakan seterusnya.	Pengguna dan Pentabir Sistem ICT
5.7 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan MOSTI; b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c. Lesen perisian (*registration code*, *CD-keys* dan nombor siri) 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.	Pengguna dan Pentabir Sistem ICT
5.8 Penyelenggaraan Perkakasan	
Peralatan ICT hendaklah diselenggarakan dengan baik bagi memastikan kerahsiaan, integriti dan kebolehsediaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar;	Pengguna, Pentabir Sistem ICT dan Pihak Ketiga

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; dan e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	
5.9 Pinjaman Peralatan ICT	
Peralatan ICT yang dipinjam adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mendapatkan kelulusan mengikut peraturan dibawah Pekeliling Perbendaharaan Tatacara Pengurusan Aset atau peraturan MOSTI bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan; b. Pengguna hendaklah memohon peminjaman peralatan ICT melalui sistem yang berkuatkuasa; c. Pengguna perlu melindungi dan mengawal peralatan sepanjang tempoh pinjaman; d. Memastikan aktiviti pinjaman dan pemulangan peralatan ICT direkodkan; dan e. Memastikan peralatan ICT yang dipulangkan dalam keadaan baik dan lengkap.	Pengguna
5.10 Peralatan ICT di Luar Premis MOSTI	
Bagi peralatan ICT yang dibawa keluar dari premis MOSTI, langkah-langkah keselamatan berikut hendaklah diambil: a. Peralatan ICT perlu dilindungi dan dikawal sepanjang masa; b. Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan c. Memeriksa dan memastikan peralatan ICT yang dibawa keluar tidak mengandungi maklumat Kerajaan. Ia perlu	Pengguna dan Pihak Ketiga

dihapuskan dari peralatan tersebut setelah disalin ke media storan sekunder.	
5.11 Pelupusan Peralatan Aset ICT	
Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa mengikut Tatacara Pengurusan Aset Alih Kerajaan. Pelupusan peralatan ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MOSTI. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan ICT khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan dilaksanakan; dan b. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;	Pengguna dan Pegawai Aset
Keselamatan Persekitaran	
Objektif: Melindungi aset ICT MOSTI dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
5.12 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa dan mengubahsuai hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (CGSO). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah dipatuhi : a. Merancang dan menyediakan pelan keseluruhan susun atur peralatan PC, 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 ditempat yang bersesuaian, mudah dicapai dan dikendalikan;	ICTSO dan Bahagian Pentadbiran

d. Bahan mudah terbakar DILARANG disimpan di dalam kawasan 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, ketuhar gelombang mikro dan lain-lain berhampiran peralatan PC; g. Semua peralatan perlindungan keselamatan hendaklah diperiksa sekurang-kurangnya dua (2) kali setahun dan diuji sekurang-kurangnya satu (1) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h. Akses kepada bilik sesalur telefon hendaklah sentiasa dikunci.	
5.13 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan hendaklah disalurkan mengikut *voltage* yang bersesuaian; b. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.	ICTSO dan Penyelenggara Bangunan
5.14 Kabel Peralatan ICT	
Kabel peralatan ICT hendaklah dilindungi kerana ia adalah salah satu punca maklumat. Langkah-langkah keselamatan kabel adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;	ICTSO, Pentabir Sistem ICT dan Penyelenggara Bangunan

b. Melindungi kabel dengan menggunakan konduit untuk mengelakkan 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.	
5.15 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan yang telah ditetapkan; b. Melaporkan insiden kecemasan persekitaran kepada Pegawai Keselamatan; dan c. Mengadakan, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa;	Pengguna dan Bahagian Pentadbiran MOSTI
Keselamatan Dokumen	
Objektif: Melindungi maklumat MOSTI dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
5.16 Dokumen	
Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi: a. Memastikan sistem dokumentasi atau penyimpanan dokumen adalah selamat dan kehilangan atau kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; b. Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; c. Pergerakan fail terperingkat dan dokumen rahsia rasmi hendaklah mengikut prosedur keselamatan;	Pengguna

d. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan dan tatacara Jabatan Arkib Negara; e. Dokumen terperingkat rasmi perlu dienkripsikan sebelum dihantar secara elektronik; dan f. Memastikan cetakan yang mengandungi maklumat terperingkat diambil segera dari pencetak.	

BAB 6

PENGURUSAN OPERASI DAN KOMUNIKASI

Pengurusan Prosedur Operasi	
Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan baik dan selamat daripada sebarang ancaman dan gangguan.	
6.1 Pengendalian Prosedur	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur keselamatan ICT hendaklah didokumenkan, diselenggarakan dan boleh digunapakai oleh pengguna bila diperlukan; 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 dikemaskini dari semasa ke semasa atau mengikut keperluan.	Pengguna
6.2 Kawalan Perubahan	
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; b. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai	ICTSO , Pengguna dan Pentabir Sistem ICT

yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan.	
6.3 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; dan b. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT
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.	
6.4 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Pengguna, Pengurus ICT, Pihak Ketiga dan Pentadbir Sistem ICT
Perancangan dan Penerimaan Sistem	
Objektif: Meminimakan risiko yang menyebabkan gangguan atau kegagalan sistem.	
6.5 Perancangan Kapasiti	

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b. Perancangan kapasiti setiap projek ICT hendaklah mengambil kira unjuran pertambahan kapasiti sesuatu komponen, sistem ICT dan teknologi ICT bagi tempoh 5 tahun; dan c. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimakan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO dan Pentadbir Sistem ICT
6.6 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a. Memantau pengurusan dan pengagihan kapasiti sesuatu komponen atau sistem ICT bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; b. Memantau dan menyelaras penalaan *(fine tuning)* penggunaan peralatan bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem sentiasa ditahap optimum; c. Menetapkan kriteria penerimaan sistem baru dan sistem yang ditingkatkan (versi terkini). Pengujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem; dan d. Mengambil kira ciri-ciri keselamatan ICT dalam perancangan keperluan kapasiti supaya dapat meminimakan risiko gangguan perkhidmatan.	ICTSO dan Pentadbir Sistem ICT

Perisian Keselamatan	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh malware serta perisian berbahaya seperti virus, trojan, mobile code dan sebagainya.	
6.7 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang perisian keselamatan untuk mengesan malware seperti anti virus dan *Intrusion Prevention System* (IPS); 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. Mengemas kini pattern perisian keselamatan mengikut keperluan; e. Menyemak kandungan sistem (tidak terhad kepada fail log, *time stamp*, fail-fail yang dimuat naik dan kod sumber) atau pertambahan maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang sedang berkuatkuasa dan akan datang bertujuan membolehkan tuntutan baik pulih sekiranya perisian tersebut dikesan mengandungi *malware*; g. Mengadakan program dan prosedur jaminan kualiti ke atas semua sistem yang dibangunkan; h. Memberi peringatan mengenai ancaman keselamatan ICT seperti serangan virus dan lain-lain kepada pengguna; dan i. Menganjurkan program kesedaran mengenai ancaman keselamatan ICT berkaitan dengan perisian berbahaya seperti malware, virus, trojan dan sebagainya.	ICTSO dan Pentadbir Sistem ICT

6.8 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	ICTSO dan Pentadbir Sistem ICT
Housekeeping	
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar sentiasa tepat dan terkini dan boleh diakses pada bila-bila masa dengan cepat.	
6.9 Backup	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* mestilah dilakukan setiap kali perubahan berlaku, contoh: konfigurasi, data/maklumat, *program coding* dan lain-lain. Melindungi integriti dan ketersediaan maklumat serta pengurusan proses maklumat agar boleh diakses pada bila-bila masa. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat *backup* secara berkala mengikut keperluan operasi sistem; b. Membuat *master copy* ke atas semua perisian dan sistem aplikasi sekurang-kurangnya sekali dan/atau sekiranya terdapat pengubahsuaian setelah mendapat versi terbaharu; c. Menguji *master copy* dan backup sedia ada bagi memastikan ianya dapat *restore* dan berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila diperlukan; d. Menyimpan sekurang-kurangnya tiga (3) generasi backup; dan e. Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.	Pentadbir Sistem ICT
Pengurusan Rangkaian Dan Keselamatan	
Objektif: Melindungi maklumat dalam infrastruktur dan rangkaian ICT.	
6.10 Kawalan Keselamatan Infrastruktur Rangkaian	
Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pengguna, Pentadbir Sistem ICT dan Pegawai

a. Kerja-kerja operasi yang melibatkan rangkaian perlu diasingkan daripada tugas dan tanggungjawab yang lain bagi mengurangkan akses, pengubahsuaian konfigurasi dan infrastruktur yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat, kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Akses kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pegawai bertanggungjawab sahaja; d. Sistem aplikasi yang melibatkan maklumat terperingkat kerajaan hendaklah dilindungi oleh firewall yang dipasang di antara rangkaian dalaman dan zon yang menempatkan sistem tersebut. Polisi firewall hendaklah dikawalselia oleh pentadbir sistem sepenuhnya; e. Semua trafik keluar dan masuk hendaklah melalui gateway yang dikawal oleh MOSTI; f. Semua sistem aplikasi berasaskan web hendaklah diletakkan di dalam *Demilitarized Zone* (DMZ), manakala pangkalan data ditempatkan di Secured Zone; g. Perisian *Intrusion Detection System* (IDS) dan *Intrusion Prevention System (IPS)* perlu diinstalasi dan dikonfigurasi bagi mengesan dan melindungi dari sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam sistem maklumat MOSTI; h. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan” dan/atau di dalam arahan/pekeliling kerajaan yang sedang berkuatkuasa; i. Memastikan keperluan keselamatan ICT adalah bersesuaian dan mencukupi bagi menyokong penyampaian perkhidmatan yang optimum; dan	Bertanggung-jawab

j. Semua pengguna komputer hanya dibenarkan menggunakan rangkaian MOSTI sahaja. Penggunaan modem, wireless adapter dan broadband adalah dilarang sama sekali kecuali dengan kebenaran ICTSO;	
Pengurusan Media Storan	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
6.11 Penghantaran dan Pemindahan	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Penghantaran atau pemindahan media storan yang mengandungi maklumat terperingkat ke luar pejabat hendaklah mendapat kebenaran daripada pemilik, Ketua Setiausaha atau Ketua Agensi terlebih dahulu.	Ketua Setiausaha, Ketua Agensi dan Pengguna
6.12 Prosedur Pengendalian Media Storan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media storan mengikut tahap sensitiviti sesuatu maklumat; b. Menghadkan dan menentukan akses media storan kepada pengguna yang sah sahaja; c. Menghadkan pengedaran data atau media storan untuk tujuan yang dibenarkan; d. Mengawal dan merekodkan aktiviti penyelenggaraan media storan bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media storan di tempat yang selamat; dan f. Maklumat terperingkat di dalam Media storan hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	CIO, ICTSO, Pengguna dan Pentadbir Sistem ICT

6.13 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menyedia dan memastikan keselamatan sistem dokumentasi mempunyai ciri-ciri keselamatan; b. Memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti akses sistem dokumentasi sedia ada.	ICTSO, Pengguna dan Pentadbir Sistem ICT
Pengurusan Pertukaran Maklumat	
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara MOSTI dan agensi luar terjamin.	
6.14 Pertukaran Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara MOSTI dengan agensi luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MOSTI; dan d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Pengguna, Jabatan dibawah MOSTI, Pihak Ketiga dan Agensi luar.
6.15 Mel Elektronik (E-mel)	
Penggunaan e-mel di MOSTI 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.	Pengguna

6.16 Maklumat Untuk Capaian Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme perlindungan keselamatan yang bersesuaian; b. Memastikan sistem untuk kegunaan orang awam diuji terlebih dahulu; dan c. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	ICTSO dan Pentadbir Sistem ICT
Pemantauan	
Objektif: Mengesan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
6.17 Pengauditan dan Forensik ICT	
Bagi memudahkan proses pengauditan dan forensik ICT dilaksanakan, perkara-perkara yang mesti direkod dan dianalisis adalah seperti berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT MOSTI; b. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery, phishing*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); c. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f. Aktiviti instalasi dan penggunaan perisian yang membebankan rangkaian; g. Aktiviti penyalahgunaan akaun e-mel; dan	ICTSO,Pengguna dan Pentadbir Sistem ICT

6.18 Jejak Audit	
a. Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti Jejak audit mengandungi: i. Setiap aktiviti transaksi direkodkan; ii. Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; iii. Aktiviti akses pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya;dan iv. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. b. Jejak audit hendaklah disimpan untuk tempoh masa yang dipersetujui iaitu tiga (3) bulan;dan c. 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.	Pengurus ICT dan Pentadbir Sistem ICT
6.19 Sistem Log	
Sistem log membantu untuk memudahkan pengesanan ke atas aktiviti sistem yang telah dijalankan. Perkara-perkara yang perlu dipatuhi adalah seperti 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. Melaporkan kepada ICTSO sekiranya wujud aktiviti-aktiviti tidak sah seperti kecurian maklumat dan pencerobohan.	Pentadbir Sistem ICT
6.20 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir

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 direkod, dianalisis dan diambil tindakan sewajarnya; dan f. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MOSTI atau domain keselamatan perlu diselaraskan dengan satu sumber waktu/julat yang dipersetujui iaitu sepuluh (10) minit.	Sistem ICT

BAB 7

KAWALAN AKSES

Dasar Kawalan Akses	
Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT MOSTI	
7.1 Keperluan Kawalan Akses	**Tanggungjawab**
Kawalan akses kepada proses dan maklumat hendaklah dilaksanakan mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan akses pengguna sedia ada. Peraturan kawalan akses hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Kawalan akses ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b. Kawalan akses 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.	ICTSO dan Pentadbir Sistem ICT
Pengurusan Akses Pengguna	
Objektif: Mengawal akses pengguna ke atas aset ICT MOSTI	
7.2 ID Pengguna Sistem Aplikasi	
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. ID pengguna yang diperuntukkan oleh MOSTI sahaja boleh digunakan; b. ID pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Pemilikan ID pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MOSTI;	Pengguna dan Pentadbir Sistem ICT

d. Akaun boleh disekat/ dipadam/ dibeku/ dibatal/ ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;dan f. Pentadbir Sistem aplikasi ICT hendaklah membeku dan membatalkan ID pengguna atas sebab-sebab berikut: i. Pengguna berkursus/bercuti panjang dalam tempoh waktu melebihi tiga (3) bulan; atau; ii. Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang dibenarkan oleh Ketua Setiausaha; iii. Bertukar ke agensi lain; iv. Bersara; v. Ditamatkan perkhidmatan; atau vi. Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang dibenarkan oleh Ketua Setiausaha. g. Pentadbir Sistem aplikasi ICT MESTI membeku atau membatalkan ID pengguna atas sebab-sebab berikut: i. Bertukar ke agensi lain; ii. Bersara; atau iii. Ditamatkan perkhidmatan;	
7.3 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
7.4 Pengurusan Kata laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh MOSTI dan mengikut pekeliling yang berkuatkuasa seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;	Pengguna dan Pentadbir Sistem ICT

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 hendaklah diaktifkan pada setiap komputer pengguna 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. Kata laluan hendaklah ditukar selepas sembilan puluh (90) hari atau selepas tempoh masa yang bersesuaian; j. Mengelakkan penggunaan semula kata laluan yang baru digunakan; dan k. Mengelakkan penggunaan semula kata laluan yang telah digunakan.	
7.5 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media storan hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif dan terperingkat terdedah sama ada atas meja atau di paparan skrin apabila pemilik tidak berada di tempatnya. Berikut adalah tindakan yang perlu diambil: a. Menggunakan kemudahan password screensaver, *lock PC* atau *log* keluar apabila meninggalkan PC;	Pengguna

b. Menyimpan bahan-bahan sensitif dan terperingkat dalam laci atau kabinet fail yang berkunci; dan *c.* Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faks dan mesin fotostat oleh pengguna yang bertanggungjawab.	
Kawalan Akses Rangkaian	
Objektif:Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
7.6 Akses Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Mewujudkan segmen rangkaian yang bersesuaian bagi membezakan di antara rangkaian MOSTI 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.	ICTSO dan Pentadbir Sistem ICT
7.7 Akses Internet	
Kawalan akses internet yang perlu dipatuhi adalah seperti perkara-perkara berikut: a. Penggunaan Internet di MOSTI hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kawalan ini akan dapat melindungi pengguna daripada ancaman *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian MOSTI; b. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;	Pengurus ICT, Pengguna dan Pentadbir Sistem ICT

c. Penggunaan teknologi (*packet shaper*) untuk mengawal dan menguruskan penggunaan jalur lebar (*bandwidth*) rangkaian dengan lebih berkesan; d. Penggunaan *Internet* termasuk aktiviti muat naik dan muat turun hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; e. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Setiausaha Bahagian sebelum dimuat naik ke Internet; f. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; g. Hanya pengguna yang mendapat kebenaran sahaja boleh menggunakan kemudahan laman media sosial dan online forum seperti newsgroup dan bulletin board. Walau bagaimanapun, kandungan perbincangan awam berkaitan MOSTI hendaklah mendapat kelulusan daripada Ketua Setiausaha terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; dan h. 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, perkauman, fitnah, hasutan dan ektremis.	
Kawalan Capaian Sistem Pengoperasian	
Objektif:Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
7.8 Capaian Sistem Pengoperasian	

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. a. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: i. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; ii. Merekodkan semua aktiviti log capaian; dan iii. Memastikan perisian keselamatan (seperti antivirus) adalah yang terkini. b. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: i. Mengesahkan pengguna yang dibenarkan; ii. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian; dan iii. Menjana amaran (alert) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. c. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log-on yang terjamin; ii. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; iii. Menghadkan dan mengawal penggunaan program; dan iv. Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	ICTSO dan Pentadbir Sistem ICT
7.9 Kad Pintar	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan;	ICTSO dan Pengguna Kad EG

b. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali; dan d. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pegawai yang diberikan kuasa.	
Kawalan Capaian Aplikasi dan Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
7.10 Capaian Aplikasi dan Maklumat	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); c. Menghadkan capaian sistem dan aplikasi kepada lima (5) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;(mengikut kesesuaian sistem); d. Menghadkan masa tidak aktif semasa di dalam sesi sistem selama dua (2) minit; (mengikut kesesuaian sistem); e. Memastikan kawalan keselamatan sistem rangkaian, aplikasi dan pangkalan data adalah kukuh dan menyeluruh bagi mengelakkan aktiviti atau capaian yang tidak sah; dan f. Capaian maklumat dan aplikasi di pusat data melalui jarak jauh (*remote access*) adalah terhad kepada yang dibenarkan sahaja.	ICTSO dan Pentadbir Sistem ICT

Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
7.11 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Merekodkan aktiviti keluar masuk penggunaan peralalan mudah alih bagi mengesan pergerakan perkakasan tersebut daripada kejadian kehilangan atau pun kerosakan; b. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; c. Memastikan peralatan mudah alih yang dibawa dengan kenderaan mesti disimpan dan dijaga dengan baik bagi mengelakkan daripada kecurian; dan d. Semua maklumat yang terdapat di dalam peralatan mudah alih seperti telefon pintar (*smartphone*) hendaklah dipadamkan apabila kehilangan dilaporkan.	Pengguna
7.12 Kemudahan Kerja Jarak Jauh	
Tindakan perlindungan bersesuaian akan diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Pengguna
7.13 *Bring Your Own Device* (BYOD)	
Peralatan ICT milik persendirian yang dibawa oleh pengguna MOSTI ke pejabat dan menggunakan peralatan ini untuk mencapai data dan aplikasi di MOSTI perlu mematuhi para 7.3, 7.5 dan 7.7.	

BAB 8

PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Keselamatan Dalam Membangunkan Sistem Aplikasi	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian	
8.1 Keperluan Keselamatan	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujud sebarang *vulnerability* yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan sistem hendaklah dijalankan seperti berikut: i. Semakan pengesahan dan integriti data yang dimasukkan (input); ii. Menentukan sama ada program berjalan dengan betul dan sempurna (aliran proses dan kerja); dan iii. Memastikan maklumat yang dipaparkan adalah tepat dan sahih (output); c. Memastikan sistem yang dibangunkan secara inhouse dan outsource hendaklah diuji terlebih dahulu dengan Stress Test, Load Test dan Penetration Test (mengikut keperluan sistem) bagi memastikan sistem berkenaan memenuhi keperluan keselamatan.	ICTSO dan Pentadbir Sistem ICT
Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat	
8.2 *Encryption*	
Perkara-perkara berikut hendaklah dipatuhi: a. Pengguna hendaklah membuat *encryption* ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa; b. Penggunaan tandatangan digital adalah diwajibkan kepada pengguna yang menguruskan transaksi maklumat terperingkat secara elektronik; dan	Pengguna dan Pentadbir Sistem ICT

c. *Public Key Infrastructure* (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi PKI berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah PKI tersebut.	
Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat	
8.3 Kawalan Fail-Fail Sistem	
Perkara-perkara berikut hendaklah dipatuhi: a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang diturunkan kuasa; b. Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal akses ke atas kod atau aturcara sistem 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.	Pentadbir Sistem ICT
Keselamatan Dalam Pembangunan dan Proses Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem aplikasi	
8.4 Kawalan Perubahan	
Perkara berikut hendaklah dipatuhi: a. Perubahan atau pengubahsuaian ke atas sistem aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b. Sistem Aplikasi perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Mengawal pindaan ke atas pakej perisian dan	Pentadbir Sistem ICT

memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; c. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan; d. Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e. Menghalang sebarang peluang kebocoran maklumat.	
8.5 Pembangunan Sistem Secara *Outsource*	
a. Pembangunan perisian secara outsource perlu diselia dan dipantau oleh pemilik sistem dan pentadbir sistem ICT; b. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik MOSTI; c. Perjanjian antara MOSTI dan pihak pembekal terhadap penggunaan kod sumber supaya tidak diguna semula bagi pembangunan sistem lain melainkan untuk kepentingan kerajaan; dan d. Semua projek pembangunan sistem ICT hendaklah dipantau melalui Jawatankuasa Pemantauan Projek-Projek ICT MOSTI.	Pentadbir Sistem ICT
Kawalan Teknikal Keterdedahan (*Vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
8.6 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; c. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan; dan	Pentadbir Sistem ICT

d. Sebarang aktiviti *patch* bagi sistem pengoperasian hendaklah diuji terlebih dahulu bagi menjamin ketersediaan sistem aplikasi.	

BAB 9

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

Mekanisme Pelaporan Insiden Keselamatan ICT	
Objektif: Memastikan insiden dikendalikan dengan segera dan berkesan bagi meminimakan kesan insiden keselamatan ICT.	
9.1 Mekanisme Pelaporan	**Tanggungjawab**
Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia termasuklah suatu perbuatan yang melanggar DKICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO, CERT MOSTI dan GCERT MAMPU dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka yang boleh menjejaskan keselamatan ICT; dan f. ICTSO hendaklah membuat laporan kepada Pasukan Tindakan Balas Insiden Keselamatan ICT (GCERT) MAMPU jika berlaku sebarang insiden keselamatan ICT di agensi berdasarkan kepada peraturan, arahan dan pekeliling keselamatan ICT yang berkuatkuasa.	CIO, ICTSO, Pengguna dan CERT MOSTI

9.2 Prosedur Pengurusan Insiden Keselamatan ICT	
Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan, prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: a. Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. Mematuhi Pelan Kontigensi seperti yang telah digariskan dalam Pelan Kesinambungan Perkhidmatan (PKP); c. Menyimpan audit trail dan memelihara bahan bukti dan rekod; d. Menyediakan tindakan pencegahan supaya insiden serupa tidak berulang; dan e. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan dan Cyber Security Malaysia sekiranya perlu.	CIO, ICTSO dan CERT MOSTI

BAB 10

PELAN KESINAMBUNGAN PERKHIDMATAN (PKP)

Dasar PKP	
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan memastikan penyampaian perkhidmatan yang berterusan kepada pelanggan	
10.1 PKP	**Tanggungjawab**
PKP hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada sistem penyampaian perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT (Arahan MKN No. 20) dan perkara-perkara yang perlu diberi perhatian adalah seperti berikut: a. Melaksanakan penilaian risiko bagi mengenalpasti risiko yang terlibat, kebarangkalian dan impak risiko tersebut dalam penyampaian perkhidmatan kritikal; b. Melaksanakan pelan kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; c. Mendokumentasikan proses dan prosedur yang telah dipersetujui; d. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; e. Memastikan *backup data* sedia ada dapat *restore* seperti sedia kala; f. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali secara efektif mengikut keadaan semasa; g. Mewujudkan PKP *framework* yang perlu dikemaskini bagi memastikan pelan PKP sentiasa konsisten dan mengambilkira keperluan keselamatan maklumat; dan h. Mewujudkan *Disaster Recovery Centre* di lokasi lain.	Koordinator PKP MOSTI

BAB 11

PEMATUHAN

Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan dengan mematuhi DKICT MOSTI	
11.1 Pematuhan Dokumen Keselamatan ICT	**Tanggungjawab**
a. Setiap pengguna dan pihak ketiga hendaklah membaca, memahami dan mematuhi DKICT MOSTI dan undang-undang atau peraturan/arahan berkaitan yang sedang berkuat kuasa; b. Semua aset ICT di MOSTI termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Setiausaha berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan;dan c. Sebarang penggunaan aset ICT MOSTI selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalahgunaan sumber MOSTI.	Pengguna dan Pihak Ketiga.
11.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
a. ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas setiap Pentadbir Sistem ICT mematuhi dasar, piawaian dan keperluan teknikal; dan b. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.	ICTSO
11.3 Pematuhan Keperluan Audit	
a. Pengauditan perlu dilaksanakan sekurang-kurangnya sekali setahun terhadap pengoperasian sistem maklumat bagi meminimakan ancaman dan meningkatkan ketersediaan sistem; b. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan; dan	Pengguna, Jabatan dibawah MOSTI, Pihak Ketiga dan Agensi luar.

c. Capaian ke atas sistem maklumat semasa pengauditan perlu dikawal selia bagi mengelakkan sebarang penyalahgunaan.	
11.4 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di MOSTI adalah seperti di **Lampiran 2**.	Pengguna, Jabatan dibawah MOSTI, Pihak Ketiga dan Agensi luar.
11.5 Pelanggaran Dasar Keselamatan ICT	
Pelanggaran DKICT MOSTI boleh dikenakan tindakan tatatertib dan/atau mengikut peraturan-peraturan yang sedang berkuatkuasa.	Pengguna, Jabatan dibawah MOSTI, Pihak Ketiga dan Agensi luar.

RUJUKAN

1. Arahan Keselamatan

2. Dokumen Keselamatan ICT MOSTI v 2.1

3. Dasar Keselamatan ICT MAMPU v 5.3

4. *National Cyber Security Policy*

5. *The Malaysian Public Sector ICT Management Security Handbook (MyMIS)*

6. Pekeliling Am Bilangan 1 Tahun 2001

7. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003

8. *Toolkit* Penggubalan Dasar Keselamatan ICT Sektor Awam v1.0

9. MS ISO 27001:2013– *Information Security Management System* (ISMS)

10. Rangka Kerja Keselamatan Cyber Sektor Awam (RAKKSSA) v 1.0

BAHAGIAN PENGURUSAN TEKNOLOGI MAKLUMAT
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI (MOSTI)
Aras 1, Blok C5, Kompleks C, Pusat Pentadbiran Kerajaan Persekutuan 62662 Putrajaya, Malaysia
Tel: 603-8885 8000 Fax: 603-8889 3005 E-mel: techsupport@mosti.gov.my

LAMPIRAN 1

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
MINISTRY OF SCIENCE, TECHNOLOGY AND INNOVATION

NON DISCLOSURE AGREEMENT (NDA)

Saya .....

No. Kad Pengenalan .....

berjawatan ..... dari organisasi.....

.....

dengan ini :

a) Akan memberi perlindungan kerahsiaan yang sewajarnya kepada semua maklumat dalam dokumen terbuka dan terperingkat MOSTI selaras dengan peruntukan Akta Rahsia Rasmi 1972; dan

b) Tidak mempunyai kepentingan peribadi terhadap maklumat tersebut yang saya perolehi semasa terlibat dengan
.....
.....

Sekian, terima kasih.

.....
(Tandatangan)

.....
(Nama)

Tarikh : .....

.....
(Tandatangan Saksi)

.....
(Nama Saksi)

.....
(No. Kad Pengenalan Saksi)

Tarikh : .....

Nota : Sila isi dengan pen dakwat hitam

SENARAI PERUNDANGAN DAN PERATURAN

a. Keselamatan Perlindungan Secara Am

i. *Emergency (Essential Power) Act 1964;*

ii. *Essential (Key Points) Regulations 1965;*

iii. Perakuan Jawatankuasa mengkaji semula peraturan keselamatan Pejabat Tahun 1982;

iv. Arahan Keselamatan Yang Dikuat kuasakan Melalui Surat Pekeliling Am Sulit Bil. 1 Tahun 1985;

v. Arahan Jawatankuasa Tetap Sasaran Penting Bil. 1 Tahun 1985;

vi. Arahan Tetap Sasaran Penting Yang Dikeluarkan Kepada Pihak Yang Terlibat Dalam Pengurusan Sasaran Penting Milik Kerajaan Dan Swasta Yang Diluluskan Oleh Jemaah Menteri Pada 13 Oktober 1993;

vii. Surat Pekeliling Am Sulit Bil. 1 Tahun 1993 - Meningkatkan Kualiti Kawalan Keselamatan Perlindungan Di Jabatan-Jabatan Kerajaan;

viii. Surat Pekeliling Am Bil. 2 Tahun 2006 - Pengukuhan Tadbir Urus Jawatankuasa It Dan Internet Kerajaan;

ix. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Kerajaan;

x. Pekeliling Am Bil.1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT);

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

xii. Surat Arahan MAMPU.BDPICT(S) 700-6/1/3(21) Bertarikh 19 November 2009 – “Penggunaan Media Jaringan Sosial di Sektor Awam”; dan

xiii. Arahan Teknologi Maklumat - MAMPU

b. Keselamatan Dokumen

i. *Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control);*

ii. Akta Rahsia Rasmi 1972;

iii. Akta Arkib Negara 2003;

iv. Surat Pekeliling Bil. 8 Tahun 1990 - Arahan Keselamatan Kawalan, Penyelenggaraan, Maklumat-Maklumat Ukur Dan Geografi Yang Antara Lainnya Merangkumi Peta-Peta Rasmi Dan Penderiaan Jauh;

v. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 - Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (*espionage*);

vi. Surat Pekeliling Am Bil. 2 Tahun 1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1976;
Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986 Dan Surat Pekeliling Am Bil. 2 Tahun 1987 Yang Ditandatangani Oleh Ketua Setiausaha Negara Melalui Surat M(R)10308/3/(45) Bertarikh 8 Mei 1987;

vii. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK(R)200/55 Klt.7(21) Bertarikh 21 Ogos 1999; dan

viii. Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 - Panduan Pengurusan Pejabat.

c. Keselamatan Fizikal Bangunan

i. Akta Kawasan Larangan Dan Tempat Larangan Tahun 1959;
ii. Arahan Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan Dan Tempat Larangan;
iii. *State Key Points;*
iv. Surat Pekeliling Am Rahsia Bil.1 Tahun 1975 - Keselamatan Jabatan-jabatan Kerajaan;
v. Surat Bil. KPKK/308/A (2) bertarikh 7/9/79 - Mencetak Pas-Pas Keselamatan dan Kad-Kad Pengenalan MOSTI;
vi. Surat Pekeliling Am Bil 4 Tahun 1982 - Permohonan Ruang Pejabat Sama Ada Dalam Bangunan Guna sama Atau pun Disewa Di Bangunan Swasta; dan
vii. Surat Pekeliling Am Bil. 14 Tahun 1982 – Pelaksanaan Pelan Pejabat Terbuka.

d. Keselamatan Individu

i. *Government Security Officer: Terms of Reference – Extract On Training Of Departmental Security Office Confidential;*
ii. *General Circular Memorandum**;***
iii. *Instruction On Positive Vetting Procedure;*
iv. Surat Pekeliling Am Sulit Bil.1/1966 – Perkara Keselamatan Tentang Persidangan-Persidangan/ Perjumpaan/Lawatan Sambil Belajar Antarabangsa;
v. Surat Pekeliling Tahun 1966 – Tapisan Keselamatan Terhadap Pakar/Penasihat Luar Negeri**;**
vi. Surat Pekeliling Am Sulit Bil.1/1967 – Ceramah Keselamatan bagi Pegawai-Pegawai Kerajaan dan mereka-mereka yang Bukan Pegawai-Pegawai Kerajaan yang bersama dalam

Perwakilan Rasmi Malaysia semasa melawat Negara-negara Tabir Buluh dan Tabir besi;

vii. Surat Pekeliling Am Sulit Bil. 2 Tahun 1977 - Melaporkan Perjumpaan/ Percakapan Di Antara Diplomat/ Orang-Orang Perseorangan Dari Negeri-Negeri Asing Dengan Anggota-Anggota Kerajaan; dan

viii. Pekeliling Kemajuan Pentadbiran AwamBil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.

e. Keselamatan Aset ICT

i. Akta Tandatangan Digital 1997;
Akta Jenayah PC 1997;

ii. Akta Hak Cipta (Pindaan) 1997;

iii. Akta Multimedia dan Telekomunikasi 1998;

iv. Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan;

v. Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat & Komunikasi (ICT);

vi. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi - Agensi Kerajaan;

vii. Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002;

viii. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005;

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

x. Akta dan Peraturan-peraturan lain yang berkaitan.