



DASAR KESELAMATAN ICT

**KEMENTERIAN SAINS, TEKNOLOGI DAN
INOVASI**

ISI KANDUNGAN

1. PENDAHULUAN	5
1.1 TUJUAN	5
1.2 OBJEKTIF	5
1.3 SKOP.....	5
1.4 PRINSIP.....	6
2. PERKARA 01 : PEMBANGUNAN DAN PENYELENGGARAAN DASAR	9
DASAR KESELAMATAN ICT	9
2.1 PELAKSANAAN DASAR.....	9
2.2 PENYEBARAN DASAR.....	9
2.3 PENYELENGGARAAN DASAR	9
2.4 PENGECUALIAN DASAR.....	10
3. PERKARA 02 : KESELAMATAN ORGANISASI	10
INFRASTRUKTUR ORGANISASI KESELAMATAN	10
3.1 KETUA SETIAUSAHA/KETUA JABATAN	10
3.2 KETUA PEGAWAI MAKLUMAT (CIO).....	10
3.3 PEGAWAI KESELAMATAN ICT (ICTSO)	11
3.4 PENGURUS PERKHIDMATAN ICT	12
3.5 PENTADBIR SISTEM ICT	13
3.6 PENGGUNA ^G	14
PIHAK KETIGA ^G /LUAR	15
3.7 KEPERLUAN KESELAMATAN KONTRAK DENGAN PIHAK KETIGA ^G	15
4. PERKARA 03 : KAWALAN DAN PENGELASAN ASET	16
AKAUNTABILITI ASET	16
4.1 INVENTORI ASET	16
KATEGORI DAN PENGENDALIAN MAKLUMAT.....	16
4.2 KATEGORI MAKLUMAT	16
4.3 PENGENDALIAN MAKLUMAT	16
5. PERKARA 04 : KESELAMATAN SUMBER MANUSIA	17
KESELAMATAN ICT DALAM TUGAS HARIAN	17
5.1 TANGGUNGJAWAB KESELAMATAN SEMASA DALAM PERKHIDMATAN	17
5.2 BERTUKAR ATAU TAMAT PERKHIDMATAN.....	18
5.3 TERMA DAN SYARAT PERKHIDMATAN	18
5.4 PERAKUAN AKTA RAHSIA RASMI.....	18
MENANGANI INSIDEN ^G KESELAMATAN ICT	18
5.5 PELAPORAN INSIDEN ^G KESELAMATAN	18
PENDIDIKAN.....	19
5.6 PROGRAM KESEDARAN KESELAMATAN ICT.....	19
TINDAKAN TATATERTIB	19
5.7 PELANGGARAN DASAR	20
6. PERKARA 05 : KESELAMATAN FIZIKAL	20
KESELAMATAN KAWASAN	20
6.1 PERIMETER KESELAMATAN FIZIKAL	20
6.2 KAWALAN MASUK FIZIKAL	21
6.3 KAWASAN LARANGAN ^G	21
KESELAMATAN PERALATAN ICT DAN MAKLUMAT	22
6.4 PERALATAN ICT	22
6.5 DOKUMEN ^G /MAKLUMAT	23
6.6 MEDIA STORAN ^G	23
6.7 KABEL PERALATAN ICT	24

6.8	PENYELENGGARAAN	24
6.9	PINJAMAN PERALATAN ICT.....	25
6.10	PERALATAN ICT DI LUAR PREMIS KEMENTERIAN / JABATAN	25
6.11	PELUPUSAN ASET ICT ^G	26
6.12	<i>CLEAR DESK</i> DAN <i>CLEAR SCREEN</i>	26
	KESELAMATAN PERSEKITARAN	27
6.13	KAWALAN PERSEKITARAN	27
6.14	BEKALAN KUASA.....	28
6.15	PROSEDUR KECEMASAN	28
7.	PERKARA 06 : PENGURUSAN OPERASI DAN KOMUNIKASI	29
	PENGURUSAN PROSEDUR OPERASI.....	29
7.1	PENGENDALIAN PROSEDUR.....	29
7.2	KAWALAN PERUBAHAN.....	29
7.3	PROSEDUR PENGURUSAN INSIDEN ^G	30
	PERANCANGAN DAN PENERIMAAN SISTEM.....	30
7.4	PERANCANGAN KAPASITI.....	30
7.5	PENERIMAAN SISTEM	31
	PERLINDUNGAN DARI <i>MALWARE</i> ^G	32
7.6	PERISIAN KESELAMATAN	32
	<i>HOUSEKEEPING</i>	33
7.7	<i>BACK-UP</i>	33
7.8	SISTEM LOG	33
	PENGURUSAN RANGKAIAN DAN KESELAMATAN	34
7.9	KAWALAN KESELAMATAN INFRASTRUKTUR RANGKAIAN	34
	PENGURUSAN MEDIA STORAN ^G	36
7.10	PENGHANTARAN DAN PEMINDAHAN	36
7.11	PROSEDUR PENGENDALIAN MEDIA STORAN ^G	36
7.12	KESELAMATAN SISTEM DOKUMENTASI	37
	KESELAMATAN KOMUNIKASI ICT	37
7.13	INTERNET	37
7.14	MEL ELEKTRONIK	38
8.	PERKARA 07 : KAWALAN AKSES	40
	DASAR KAWALAN AKSES.....	40
8.1	KEPERLUAN DASAR.....	40
	PENGURUSAN AKSES PENGGUNA ^G	40
8.2	ID PENGGUNA ^G SISTEM APLIKASI.....	40
8.3	<i>AUDIT TRAIL</i>	41
	KAWALAN AKSES SISTEM APLIKASI	41
8.4	SISTEM APLIKASI.....	41
	<i>NOTEBOOK</i>	42
8.5	PENGGUNAAN <i>NOTEBOOK</i>	42
9.	PERKARA 08 : PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	43
	CIRI-CIRI KESELAMATAN DALAM MEMBANGUNKAN SISTEM APLIKASI	43
9.1	KEPERLUAN KESELAMATAN	43
	KRIPTOGRAFI ^G	44
9.2	<i>ENCRYPTION</i>	44
	FAIL SISTEM	44
9.3	KAWALAN FAIL-FAIL SISTEM.....	44
	PEMBANGUNAN DAN PROSES SOKONGAN.....	45
9.4	KAWALAN PERUBAHAN.....	45
10.	PERKARA 09 : <i>BUSINESS CONTINUITY PLAN</i> (BCP)	45
	DASAR BCP.....	45
10.1	BCP	45

11.	PERKARA 10 : PEMATUHAN	46
	PEMATUHAN DAN KEPERLUAN PERUNDANGAN	46
11.1	PEMATUHAN DASAR	46
11.2	KEPERLUAN PERUNDANGAN	46
12.	GLOSARI (G)	52
13.	RUJUKAN	54
13.1	ARAHAN KESELAMATAN	54
13.2	DASAR KESELAMATAN ICT MAMPU	54
13.3	DASAR KESELAMATAN ICT KEMENTERIAN PELAJARAN MALAYSIA	54
13.4	NATIONAL CYBER SECURITY POLICY	54
14.	LAMPIRAN	54
14.1	GARIS PANDUAN DAN ETIKA PENGGUNAAN E-MEL DAN INTERNET MOSTI	54

1. PENDAHULUAN

1.1 TUJUAN

Tujuan dasar ini adalah untuk memaklumkan peraturan-peraturan yang perlu dipatuhi oleh semua Warga Kementerian/Jabatan untuk menjaga keselamatan aset Teknologi Maklumat dan Komunikasi (ICT). 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 Kementerian/Jabatan dapat ditingkatkan.

1.2 OBJEKTIF

Objektif Dasar Keselamatan ICT adalah seperti berikut:

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

1.3 SKOP

Dasar ini meliputi semua aset ICT^G yang digunakan seperti maklumat (contoh: fail, dokumen^G, data elektronik), perisian (contoh: aplikasi dan sistem perisian) dan fizikal (contoh: *Data Centre*, PC, *server*, peralatan komunikasi, media^G magnet dan lain-lain). Dasar ini adalah terpakai oleh

semua pengguna^G di Kementerian/Jabatan termasuk pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, memuat naik, menyediakan, berkongsi, menyimpan dan menggunakan aset ICT^G Kementerian/Jabatan.

1.4 PRINSIP

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

a. **Akses atas dasar perlu mengetahui**

Akses terhadap penggunaan aset ICT^G hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna^G tertentu atas dasar “perlu mengetahui” sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna^G memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen^G Arahan Keselamatan perenggan 53, muka surat 15.

b. **Hak akses minimum**

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

c. **Akauntabiliti**

Semua pengguna^G adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT^G Kementerian/Jabatan.

d. **Pengasingan**

Tugas mewujudkan, memadam, menambah, mengubah dan mengesahkan data/maklumat perlu diasingkan. Ini adalah untuk mengelakkan akses yang tidak dibenarkan dan melindungi aset ICT^G daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara aktiviti di atas dan pegawai bertanggungjawab.

e. **Pengauditan**

Pengauditan adalah tindakan untuk mengenal pasti insiden^G berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT^G seperti PC, *server*, peralatan keselamatan/rangkaian dan sebagainya hendaklah dipastikan dapat menjana dan menyimpan log untuk tujuan *audit trail*.

f. **Pematuhan**

Dasar Keselamatan ICT 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 meminimumkan sebarang gangguan atau kerugian perkhidmatan akibat daripada *unavailability* sistem. Pemulihan boleh dilakukan melalui kaedah *redundancy* dan mewujudkan *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (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.

2. PERKARA 01 : PEMBANGUNAN DAN PENYELENGGARAAN DASAR

Dasar Keselamatan ICT	
2.1 Pelaksanaan Dasar	
Ketua Setiausaha/Ketua Jabatan adalah bertanggungjawab ke atas pelaksanaan arahan dengan dibantu oleh Jawatankuasa Pemandu ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), SUBK (Pengurusan), Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik.	Ketua Setiausaha / Ketua Jabatan, TKSU(DS), SUBK(P), SUB(P TM) atau lain-lain Pegawai Yang Diturunkan Kuasa
2.2 Penyebaran Dasar	
Dasar ini perlu disebar kepada semua pengguna ^G Kementerian/Jabatan termasuk pembekal, pakar runding dan lain-lain.	ICTSO
2.3 Penyelenggaraan Dasar	
Dasar Keselamatan ICT MOSTI adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT MOSTI: <ul style="list-style-type: none"> a. kenal pasti dan tentukan perubahan yang diperlukan; b. kemuka cadangan pindaan secara bertulis kepada CIO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JP ICT); c. perubahan yang telah dipersetujui oleh JP ICT dimaklumkan kepada semua pengguna^G; dan d. dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun. 	ICTSO

2.4 Pengecualian Dasar	
Dasar Keselamatan ICT MOSTI adalah terpakai kepada semua pengguna ^G ICT Kementerian/Jabatan dan tiada pengecualian diberikan.	Warga Kementerian / Jabatan

3. PERKARA 02 : KESELAMATAN ORGANISASI

Infrastruktur Organisasi Keselamatan	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi	
3.1 Ketua Setiausaha/Ketua Jabatan	
Peranan dan tanggungjawab Ketua Setiausaha/Ketua Jabatan adalah seperti berikut: <ul style="list-style-type: none"> a. Memastikan pelaksanaan Jawatankuasa Pemandu ICT (JPIC) Kementerian/Jabatan merangkumi perkara mengenai keselamatan ICT Kementerian/Jabatan; b. memastikan semua pengguna^G mematuhi Dasar Keselamatan ICT MOSTI terkini; c. merancang semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan d. merancang penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT MOSTI. 	Ketua Setiausaha / Ketua Jabatan atau Pegawai Yang Diturunkan Kuasa
3.2 Ketua Pegawai Maklumat (CIO)	
Setiausaha Bahagian Kanan (Pengurusan) dilantik sebagai CIO MOSTI. Peranan dan tanggungjawab beliau adalah seperti berikut: <ul style="list-style-type: none"> a. Mewujud dan mengetuai pasukan kerja 	SUBK(P) / CIO Jabatan

<p>keselamatan ICT Kementerian/Jabatan;</p> <p>b. membantu Ketua Setiausaha/Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;</p> <p>c. menjadi penasihat keselamatan ICT;</p> <p>d. menyelaraskan pembangunan dan pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT;</p> <p>e. memastikan semua pengguna^G memahami dan mematuhi Dasar Keselamatan ICT MOSTI;</p> <p>f. memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan</p> <p>g. memastikan penilaian risiko dan program keselamatan dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT MOSTI.</p>	
<p>3.3 Pegawai Keselamatan ICT (ICTSO)</p>	
<p>Setiausaha Bahagian Pengurusan Teknologi Maklumat dilantik sebagai ICTSO MOSTI. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:</p> <p>a. Mengurus pelaksanaan keseluruhan program keselamatan ICT Kementerian/Jabatan;</p> <p>b. menguatkuasakan Dasar Keselamatan ICT MOSTI;</p> <p>c. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MOSTI kepada semua pengguna^G;</p> <p>d. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar</p>	<p>SUB(PTM), Pengurus ICT Jabatan atau Pegawai Yang Diturunkan Kuasa</p>

<p>Keselamatan ICT MOSTI;</p> <ul style="list-style-type: none"> e. menjalankan pengurusan risiko; f. menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. memberi amaran terhadap kemungkinan berlakunya ancaman seperti <i>virus</i>, <i>spam</i> dan lain-lain; h. memberi khidmat nasihat dan menyediakan langkah-langkah perlindungan yang bersesuaian; i. melaporkan insiden^G keselamatan ICT kepada Pasukan Tindak Balas Insiden^G Keselamatan ICT (GCERT) MAMPU dan memaklumpkannya kepada CIO; j. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden^G keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; k. mengesyor dan menyokong proses pengambilan tindakan tatatertib ke atas pengguna^G yang melanggar Dasar Keselamatan ICT MOSTI; dan l. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT. 	
<p>3.4 Pengurus Perkhidmatan ICT</p>	
<p>Ketua Penolong Setiausaha Operasi, Rangkaian dan Keselamatan dilantik sebagai Pengurus Perkhidmatan ICT MOSTI. Peranan dan tanggungjawab Pengurus Perkhidmatan ICT adalah seperti berikut:</p> <ul style="list-style-type: none"> a. Memahami, mematuhi dan melaksana Dasar 	<p>KPSU(O) / Pengurus Perkhidmatan ICT Jabatan atau Pegawai Yang</p>

<p>Keselamatan ICT MOSTI;</p> <p>b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Kementerian/Jabatan;</p> <p>c. menentukan kawalan akses semua pengguna^G terhadap aset ICT^G Kementerian/Jabatan;</p> <p>d. melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan</p> <p>e. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Kementerian/Jabatan.</p>	Diturunkan Kuasa
<p>3.5 Pentadbir Sistem ICT</p>	
<p>Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut:</p> <p>a. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas;</p> <p>b. menentukan ketepatan dan kesempurnaan sesuatu tahap akses berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT MOSTI;</p> <p>c. memantau aktiviti akses harian pengguna^G;</p> <p>d. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan/penggodaman dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta;</p> <p>e. memastikan pembangunan sistem aplikasi mengambil kira dan mematuhi ciri-ciri</p>	Pentadbir Sistem ICT Kementerian / Jabatan

<p>keselamatan yang termaktub di dalam Dasar Keselamatan ICT MOSTI;</p> <p>f. menyimpan dan menganalisis rekod <i>audit trail</i>; dan</p> <p>g. menyediakan laporan mengenai aktiviti akses kepada pemilik maklumat berkenaan secara berkala.</p>	
<p>3.6 Pengguna</p>	
<p>Peranan dan tanggungjawab pengguna^G adalah seperti berikut:</p> <p>a. memahami dan mematuhi Dasar Keselamatan ICT MOSTI;</p> <p>b. mengetahui dan memahami implikasi keselamatan ICT dan kesan dari tindakannya;</p> <p>c. lulus tapisan keselamatan;</p> <p>d. melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat Kementerian/Jabatan;</p> <p>e. melaksanakan langkah-langkah perlindungan seperti berikut :</p> <p>i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;</p> <p>ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;</p> <p>iii. menentukan maklumat sedia untuk digunakan;</p> <p>iv. menjaga kerahsiaan kata laluan;</p> <p>v. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;</p> <p>vi. memberi perhatian kepada maklumat</p>	<p>Warga Kementerian / Jabatan</p>

<p>terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan</p> <p>vii. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.</p> <p>f. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;</p> <p>g. menghadiri program-program kesedaran mengenai keselamatan ICT; dan</p> <p>h. menandatangani surat akuan pematuhan Dasar Keselamatan ICT MOSTI.</p>	
Pihak Ketiga/Luar	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga	
3.7 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
<p>Akses kepada aset ICT Kementerian/Jabatan perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai:</p> <ol style="list-style-type: none"> a. Dasar Keselamatan ICT MOSTI; b. Tapisan Keselamatan; c. Perakuan Akta Rahsia Rasmi 1972; dan d. Hak Harta Intelekt. <p><u>Rujukan:</u> <i>Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk "Tatacara Penyediaan, Penilaian dan Penerimaan Tender" dan Surat Pekeliling Perbendaharaan Bilangan 3 Tahun 1995 bertajuk "Peraturan Perolehan Perkhidmatan Perundingan".</i></p>	<p>CIO, ICTSO, Pengurus Perkhidmatan ICT, Pentadbir Sistem ICT dan Pihak Ketiga^G di Kementerian / Jabatan</p>

4. PERKARA 03 : KAWALAN DAN PENGELASAN ASET

Akauntabiliti Aset	
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT ^G Kementerian/Jabatan	
4.1 Inventori Aset	
Semua aset ICT ^G Kementerian/Jabatan hendaklah direkodkan. Ini termasuklah mengenalpasti aset, mengkategorikan aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Setiap pengguna ^G adalah bertanggungjawab ke atas semua aset ICT ^G di bawah kawalannya.	Pentadbir Sistem ICT dan Warga Kementerian / Jabatan
Kategori dan Pengendalian Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT ^G diberikan tahap perlindungan yang bersesuaian	
4.2 Kategori Maklumat	
Maklumat hendaklah dikategori dan dilabelkan sewajarnya. Setiap maklumat yang dikategori mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen ^G Arahan Keselamatan seperti berikut: <ul style="list-style-type: none"> a. Rahsia Besar^G; b. Rahsia^G; c. Sulit^G; atau d. Terhad^G. 	Pegawai Yang Diturunkan Kuasa
4.3 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira perkara-perkara berikut : <ul style="list-style-type: none"> a. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. memeriksa maklumat dan menentukan ia tepat 	Warga Kementerian / Jabatan

<p>dan lengkap dari semasa ke semasa;</p> <p>c. menentukan maklumat sedia untuk digunakan;</p> <p>d. menjaga kerahsiaan kata laluan;</p> <p>e. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;</p> <p>f. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan</p> <p>g. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.</p>	
--	--

5. PERKARA 04 : KESELAMATAN SUMBER MANUSIA

Keselamatan ICT Dalam Tugas Harian	
Objektif: Meminimumkan risiko seperti kesilapan, kecuaiian, kecurian, penipuan dan penyalahgunaan aset ICT ^G Kementerian/Jabatan	
5.1 Tanggungjawab Keselamatan Semasa Dalam Perkhidmatan	
<p>Memastikan semua pengguna^G sedar akan ancaman keselamatan maklumat dan perkakasan serta memahami peranan dan tanggungjawab masing-masing untuk menyokong Dasar Keselamatan ICT MOSTI. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a. Memastikan semua pengguna^G menjaga keselamatan ICT berlandaskan dasar dan peraturan yang ditetapkan oleh Kementerian/Jabatan;</p> <p>b. semua pengguna^G termasuk pihak ketiga^G perlu memahami dan mempunyai kesedaran terhadap pengurusan keselamatan ICT melalui program</p>	Warga Kementerian/ Jabatan

latihan yang diberi dari semasa ke semasa; dan c. memahami dan menyedari bahawa tindakan disiplin akan diambil sekiranya berlaku pelanggaran dan ketidakpatuhan ke atas dasar dan peraturan yang telah ditetapkan oleh Kementerian/Jabatan.	
5.2 Bertukar Atau Tamat Perkhidmatan	
Memastikan semua pengguna ^G Kementerian/Jabatan yang tamat perkhidmatan atau bertukar diurus dengan teratur. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT ^G Kerajaan dikembalikan mengikut peraturan dan/atau terma yang ditetapkan oleh MOSTI; dan b. memastikan semua kebenaran akses ke atas maklumat dan kemudahan proses maklumat dibatalkan mengikut peraturan yang ditetapkan oleh MOSTI.	Warga Kementerian / Jabatan
5.3 Terma dan Syarat Perkhidmatan	
Semua Warga Kementerian/Jabatan dan pihak ketiga ^G yang bertugas di Kementerian/Jabatan hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang sedang berkuat kuasa.	Warga Kementerian / Jabatan dan Pihak Ketiga ^G
5.4 Perakuan Akta Rahsia Rasmi	
Warga Kementerian/Jabatan yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Warga Kementerian / Jabatan dan Pihak Ketiga ^G
Menangani Insiden^G Keselamatan ICT	
Objektif: Meminimumkan kesan insiden ^G keselamatan ICT	
5.5 Pelaporan Insiden^G Keselamatan	
Insiden ^G keselamatan ICT seperti berikut hendaklah	Warga

<p>dilaporkan kepada ICTSO dengan kadar segera:</p> <ul style="list-style-type: none"> a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa; ataupun disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. sistem aplikasi digunakan tanpa kebenaran atau disyaki sedemikian; c. katalaluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; ataupun disyaki hilang, dicuri atau didedahkan; d. berlaku kejadian kehilangan fail, sistem kerap kali gagal dan maklumat komunikasi tersalah hantar; e. berlaku percubaan mencerooboh, penyelewengan dan insiden-insiden^G yang tidak diingini. <p><u>Rujukan:</u> <i>Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden^G Keselamatan ICT”.</i></p>	<p>Kementerian / Jabatan dan Pihak Ketiga^G</p>
<p>Pendidikan</p>	
<p>Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT</p>	
<p>5.6 Program Kesedaran Keselamatan ICT</p>	
<p>Setiap pengguna^G di Kementerian/Jabatan perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden^G juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT Kementerian/Jabatan.</p>	<p>ICTSO dan Pegawai Yang Diturunkan Kuasa</p>
<p>Tindakan Tatatertib</p>	
<p>Objektif: Meningkatkan kesedaran dan pematuhan ke atas Dasar Keselamatan ICT MOSTI</p>	

5.7 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT MOSTI akan dikenakan tindakan tatatertib.	Warga Kementerian / Jabatan

6. PERKARA 05 : KESELAMATAN FIZIKAL

Keselamatan Kawasan	
Objektif: Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat	
6.1 Perimeter Keselamatan Fizikal	
<p>Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut:</p> <ol style="list-style-type: none"> Kawasan keselamatan fizikal hendaklah di kenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; memperkuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; memperkuhkan dinding dan siling; memasang alat penggera dan sistem CCTV; menghadkan jalan keluar masuk; mengadakan kaunter kawalan; menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan mewujudkan perkhidmatan kawalan keselamatan. 	Pejabat Ketua Pegawai Keselamatan Kerajaan, Pegawai Keselamatan Kementerian / Jabatan, CIO, ICTSO dan Pegawai Keselamatan Bahagian.

<p>6.2 Kawalan Masuk Fizikal</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Setiap pengguna^G Kementerian/Jabatan hendaklah memakai Pas Keselamatan sepanjang waktu bertugas; b. setiap pelawat mestilah mendaftar dan mendapatkan Pas Keselamatan Pelawat di pintu masuk utama Kementerian/Jabatan untuk ke kawasan/tempat berurusan dan hendaklah dikembalikan semula selepas tamat urusan; c. semua Pas Keselamatan hendaklah diserahkan semula kepada Kementerian/Jabatan apabila pengguna^G bertukar, berhenti atau bersara; dan d. kehilangan Pas Keselamatan mestilah dilaporkan dengan segera kepada Pegawai Keselamatan organisasi masing-masing dan pejabat yang mengeluarkannya. 	<p>Semua Warga Kementerian / Jabatan dan Pelawat</p>
<p>6.3 Kawasan Larangan^G</p>	
<p>Kawasan larangan^G ditakrifkan sebagai kawasan yang dihadkan kemasukan oleh pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT^G yang terdapat di dalam kawasan tersebut. Kawasan larangan^G di Kementerian/Jabatan adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Aras 7, Blok C5, MOSTI; b. Pejabat Ketua Setiausaha dan Timbalan Ketua Setiausaha, Blok C5, MOSTI; c. Pejabat Ketua Jabatan; d. Data Centre Kementerian/Jabatan; dan e. Kawasan-kawasan lain yang dikategorikan sebagai Kawasan Larangan^G oleh Kementerian/Jabatan. 	<p>Warga Kementerian / Jabatan dan Pihak Ketiga^G</p>

<p>Akses kepada kawasan tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja.</p> <p>Pihak ketiga^G adalah dilarang sama sekali untuk memasuki kawasan larangan^G 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.</p> <p>Semua aktiviti di kawasan larangan^G termasuk penghantaran, kemas kini dan penghapusan maklumat rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Setiausaha/Ketua Jabatan.</p>	
Keselamatan Peralatan ICT Dan Maklumat	
Objektif: Melindungi peralatan ICT dan maklumat	
6.4 Peralatan ICT	
<p>Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan dengan mengambil tindakan berikut:</p> <ol style="list-style-type: none"> a. Setiap pengguna^G hendaklah memeriksa dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna dan melaporkan sebarang kerosakan kepada Pegawai Aset ICT^G Kementerian/Jabatan; b. Setiap pengguna^G adalah bertanggungjawab ke atas kerosakan dan kehilangan atas kecuaiannya sendiri, peralatan ICT di bawah kawalannya; c. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan selamat; dan 	<p>Warga Kementerian / Jabatan dan Pihak Ketiga^G</p>

<p>d. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.</p>	
<p>6.5 Dokumen^G/Maklumat</p>	
<p>Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:</p> <ul style="list-style-type: none"> a. Memastikan sistem dokumentasi atau penyimpanan dokumen^G/maklumat adalah selamat dan terjamin; b. menggunakan tanda atau label keselamatan seperti Rahsia Besar^G, Rahsia^G, Sulit^G, Terhad^G dan Terbuka^G kepada dokumen^G/maklumat; c. menggunakan <i>encryption</i> ke atas dokumen^G/maklumat terperingkat rasmi yang disediakan dan dihantar secara elektronik; dan d. memastikan cetakan yang mengandungi maklumat terperingkat diambil segera dari pencetak. 	<p>Warga Kementerian / Jabatan</p>
<p>6.6 Media Storan^G</p>	
<p>Keselamatan media storan^G perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat secara sekunder. Tindakan berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan adalah terjamin dan selamat:</p> <ul style="list-style-type: none"> a. Sediakan ruang penyimpanan yang kondusif^G dan selamat serta bersesuaian dengan kandungan maklumat; b. mendapatkan kebenaran terlebih dahulu sebelum memasuki kawasan penyimpanan media storan^G. Kawasan ini adalah terhad kepada mereka yang 	<p>Warga Kementerian / Jabatan</p>

<p>dibenarkan sahaja;</p> <p>c. merekodkan pergerakan media storan^G;</p> <p>d. melaksanakan aktiviti <i>backup</i> yang berkala; dan</p> <p>e. mendapat kelulusan pemilik maklumat terlebih dahulu sebelum menghapuskan maklumat atau kandungan media storan^G.</p>	
<p>6.7 Kabel Peralatan ICT</p>	
<p>Kabel peralatan ICT hendaklah dilindungi kerana ia adalah salah satu punca maklumat. Langkah-langkah keselamatan kabel adalah seperti berikut::</p> <p>a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; dan</p> <p>b. melindungi kabel dengan menggunakan conduit untuk mengelakkan kerosakan yang disengajakan atau tidak disengajakan.</p>	<p>ICTSO dan Pegawai Yang Diturunkan Kuasa</p>
<p>6.8 Penyelenggaraan</p>	
<p>Peralatan ICT hendaklah diselenggarakan dengan baik bagi memastikan kerahsiaan, integriti dan kebolehsediaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a. Semua peralatan ICT yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan;</p> <p>b. peralatan ICT hanya boleh diselenggarakan oleh pegawai^G yang diturunkan kuasa atau pihak ketiga^G yang dibenarkan sahaja;</p> <p>c. semua peralatan ICT hendaklah diperiksa dan diuji sebelum dan selepas proses penyelenggaraan dilakukan;</p> <p>d. semua penyelenggaraan mestilah mendapat kebenaran daripada pemilik; dan</p> <p>e. memastikan media storan^G maklumat terperingkat</p>	<p>Warga Kementarian / Jabatan, Pegawai Yang Diturunkan Kuasa dan Pihak Ketiga^G</p>

<p>dikeluarkan terlebih dahulu daripada peralatan ICT sebelum dibawa keluar pejabat untuk diselenggara.</p>	
<p>6.9 Pinjaman Peralatan ICT</p>	
<p>Peralatan ICT yang dipinjam adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Mendapatkan kelulusan mengikut peraturan di bawah Pekeliling Perbendaharaan Tatacara Pengurusan Aset atau peraturan Kementerian/Jabatan bagi membawa keluar peralatan atau maklumat tertakluk kepada tujuan yang dibenarkan; b. peminjam perlu melindungi dan mengawal peralatan sepanjang masa; c. memastikan aktiviti pinjaman dan pemulangan peralatan ICT direkodkan; dan d. memastikan peralatan ICT yang dipulangkan dalam keadaan baik dan lengkap. 	<p>Warga Kementerian / Jabatan dan Pegawai Yang Diturunkan Kuasa</p>
<p>6.10 Peralatan ICT di Luar Premis Kementerian / Jabatan</p>	
<p>Bagi peralatan ICT yang dibawa keluar dari premis Kementerian/Jabatan, langkah-langkah keselamatan berikut hendaklah diambil:</p> <ol style="list-style-type: none"> 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 	<p>Warga Kementerian / Jabatan</p>

<p>Kerajaan. Ia perlu dihapuskan dari peralatan tersebut setelah disalin ke media storan^G sekunder.</p>	
<p>6.11 Pelupusan Aset ICT^G</p>	
<p>Aset ICT^G yang hendak dilupuskan perlu melalui proses pelupusan semasa mengikut Pekeliling Perbendaharaan Bil. 5 Tahun 2007 Tatacara Pengurusan Aset Alih Kerajaan. Pelupusan peralatan ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Kementerian/Jabatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut::</p> <ol style="list-style-type: none"> a. Semua kandungan peralatan ICT khususnya maklumat terperingkat hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui <i>shredding</i>, <i>grinding</i>, <i>degauzing</i> atau pembakaran; dan b. sekiranya maklumat perlu disimpan, maka pengguna^G bolehlah membuat salinan. 	<p>Pegawai Yang Diturunkan Kuasa</p>
<p>6.12 <i>Clear Desk dan Clear Screen</i></p>	
<p>Semua maklumat dalam apa jua bentuk media storan^G hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. <i>Clear Desk</i> dan <i>Clear Screen</i> 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:</p> <ol style="list-style-type: none"> a. Gunakan kemudahan <i>password screen saver</i> atau log keluar apabila meninggalkan PC; dan b. bahan-bahan sensitif dan terperingkat hendaklah disimpan dalam laci atau kabinet fail yang 	<p>Warga Kementerian / Jabatan</p>

berkunci.	
Keselamatan Persekitaran	
Objektif: Melindungi aset ICT ^G Kementerian/Jabatan dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan	
6.13 Kawalan Persekitaran	
<p>Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT^G, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa dan mengubahsui hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil :</p> <ol style="list-style-type: none"> a. Merancang dan menyediakan pelan keseluruhan susun atur Data Centre (bilik percetakan, peralatan PC 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 dicapai dan dikendalikan; d. bahan mudah terbakar dilarang disimpan di dalam kawasan penyimpanan aset ICT^G; e. semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT^G; f. pengguna^G adalah dilarang merokok atau 	Warga Kementerian / Jabatan

<p>menggunakan peralatan memasak seperti cerek elektrik, ketuhar gelombang mikro dan lain-lain berhampiran peralatan PC; dan</p> <p>g. semua peralatan perlindungan keselamatan hendaklah diperiksa dan diuji sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.</p>	
<p>6.14 Bekalan Kuasa</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT;</p> <p>b. peralatan sokongan seperti <i>Uninterruptable Power Supply</i> (UPS) dan penjana (<i>generator</i>) boleh digunakan bagi perkhidmatan kritikal seperti di <i>Data Centre</i> supaya mendapat bekalan kuasa berterusan; dan</p> <p>c. semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.</p>	<p>BPTM^G, ICTSO dan Penyelenggara Bangunan</p>
<p>6.15 Prosedur Kecemasan</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a. Memastikan setiap pengguna^G membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada prosedur kecemasan yang telah ditetapkan;</p> <p>b. melaporkan insiden^G kecemasan persekitaran kepada Pegawai Keselamatan Kementerian/Jabatan (PKJ);</p> <p>c. mengadakan, menguji dan mengemaskini pelan</p>	<p>Warga Kementerian / Jabatan</p> <p>Bahagian</p>

kecemasan dari semasa ke semasa; dan d. merancang dan mengadakan latihan kebakaran bangunan (<i>fire drill</i>) secara berkala.	Pentadbiran Kementerian / Jabatan
--	---

7. PERKARA 06 : PENGURUSAN OPERASI DAN KOMUNIKASI

Pengurusan Prosedur Operasi	
Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan baik dan selamat	
7.1 Pengendalian Prosedur	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur keselamatan ICT yang diwujudkan, dikenalpasti dan masih digunapakai hendaklah didokumenkan, 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.	Warga Kementerian / Jabatan
7.2 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 ^G terlebih dahulu; b. aktiviti-aktiviti seperti memasang, menyelenggara,	Warga Kementerian / Jabatan

<p>menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT^G berkenaan;</p> <p>c. semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan</p> <p>d. semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.</p>	
<p>7.3 Prosedur Pengurusan Insiden^G</p>	
<p>Bagi memastikan tindakan menangani insiden^G keselamatan ICT diambil dengan cepat, teratur dan berkesan, prosedur pengurusan insiden^G mestilah mengambil kira kawalan-kawalan berikut:</p> <p>a. Menenal pasti semua jenis insiden^G keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran;</p> <p>b. menyediakan Pelan Kontigensi dan mengaktifkan Pelan Kesyinambungan Perkhidmatan (BCP);</p> <p>c. menyimpan audit <i>trail</i> dan memelihara bahan bukti; dan</p> <p>d. menyediakan tindakan pemulihan segera.</p>	<p>JPICT Kementerian / Jabatan dan ICTSO</p>
<p>Perancangan dan Penerimaan Sistem</p>	
<p>Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem</p>	
<p>7.4 Perancangan Kapasiti</p>	

<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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. keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. 	<p>Pentadbir Sistem ICT, ICTSO dan Pegawai Yang Diturunkan Kuasa</p>
<p>7.5 Penerimaan Sistem</p>	
<p>Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> 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 penggunaan peralatan bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem sentiasa di tahap optimum; c. menetapkan kriteria penerimaan sistem baru dan sistem yang ditingkatkan (versi baru). Pengujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem; dan 	<p>Pentadbir Sistem ICT, ICTSO dan Pegawai Yang Diturunkan Kuasa</p>

<p>d. mengambil kira ciri-ciri keselamatan ICT dalam perancangan keperluan kapasiti supaya dapat meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.</p>	
<p>Perlindungan dari <i>Malware</i>^G</p>	
<p>Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh <i>malware</i>^G</p>	
<p>7.6 Perisian Keselamatan</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Memasang perisian keselamatan untuk mengesan <i>malware</i>^G seperti anti virus dan <i>Intrusion Detection System</i> (IDS). Prosedur penggunaan yang betul dan selamat perlulah diikuti; b. memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997; c. mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. mengemas kini <i>pattern</i> perisian keselamatan setiap masa; e. menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi <i>malware</i>^G; g. mengadakan program dan prosedur jaminan 	<p>Pentadbir Sistem ICT, ICTSO dan Pegawai Yang Diturunkan Kuasa</p>

<p>kualiti ke atas semua perisian yang dibangunkan;</p> <p>h. memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus dan lain-lain; dan</p> <p>i. menghadiri program kesedaran mengenai ancaman <i>malware</i>^G dan cara mengendalikannya.</p>	<p>Warga Kementerian / Jabatan</p>
<p>Housekeeping</p>	
<p>Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar sentiasa tepat dan terkini dan boleh diakses pada bila-bila masa dengan cepat</p>	
<p>7.7 Back-up</p>	
<p>Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, <i>back-up</i> mestilah dilakukan setiap kali perubahan berlaku, contoh: konfigurasi, data/maklumat, <i>program coding</i> dan lain-lain. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Membuat <i>back-up</i> ke atas semua data dan maklumat mengikut keperluan operasi dan <i>back-up</i> hendaklah direkodkan dan di simpan di <i>off site</i>; b. membuat <i>master copy</i> ke atas semua perisian dan sistem aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; dan c. menguji <i>back-up</i> sedia ada bagi memastikan ianya dapat <i>restore</i> dan berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila diperlukan. 	<p>Pentadbir Sistem ICT, ICTSO dan Pegawai Yang Diturunkan Kuasa</p>
<p>7.8 Sistem Log</p>	
<p>Sistem log membantu untuk memudahkan pengesanan ke atas aktiviti sistem yang telah dijalankan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna^G; 	<p>Pentadbir Sistem ICT, ICTSO dan Pegawai Yang Diturunkan Kuasa</p>

<ul style="list-style-type: none"> 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. 	
Pengurusan Rangkaian Dan Keselamatan	
Objektif: Melindungi maklumat dalam infrastruktur dan rangkaian ICT	
7.9 Kawalan Keselamatan Infrastruktur Rangkaian	
<p>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:</p> <ul style="list-style-type: none"> a. Tanggungjawab atau kerja-kerja operasi yang melibatkan rangkaian dan perkakasan ICT hendaklah diasingkan untuk mengurangkan akses dan pengubahsuaian 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 pengguna^G yang dibenarkan sahaja; d. semua peralatan mestilah melalui proses <i>Factory Acceptance Check</i> (FAC) semasa instalasi, konfigurasi dan pentauliahan; e. sistem aplikasi yang melibatkan maklumat terperinci Kerajaan hendaklah dilindungi oleh 	<p>Pentadbir Sistem ICT, ICTSO dan Pegawai Yang Diturunkan Kuasa</p>

<p><i>firewall</i> yang dipasang di antara rangkaian dalaman dan zon yang menempatkan sistem tersebut. Peralatan ini hendaklah dikonfigurasi sendiri oleh pentadbir sistem;</p> <p>f. semua trafik keluar dan masuk hendaklah melalui <i>firewall</i> (gateway) yang dikawal oleh Kementerian/Jabatan;</p> <p>g. semua sistem aplikasi berasaskan web hendaklah diletakkan di dalam zon DMZ (<i>Demilitarized Zone</i>), manakala pangkalan data ditempatkan di <i>Secured Zone</i>;</p> <p>h. memasang perisian <i>Intrusion Detection System</i> (IDS) dan <i>Intrusion Protection System</i> (IPS) bagi mengesan dan melindungi dari sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat Kementerian/Jabatan;</p> <p>i. memasang <i>Web Content Filtering</i> pada <i>Internet Gateway</i> 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”;</p> <p>j. sebarang penyambungan rangkaian yang bukan di bawah kawalan Kementerian/Jabatan hendaklah mendapat kebenaran ICTSO;</p> <p>k. memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum;</p> <p>l. semua pengguna^G hanya dibenarkan</p>	<p>Warga Kementerian / Jabatan</p>
---	--

<p>menggunakan rangkaian Kementerian/Jabatan sahaja. Penggunaan modem adalah dilarang sama sekali kecuali dengan kebenaran ICTSO; dan</p> <p>m. semua perisian <i>sniffer</i> atau <i>network analyser</i> adalah dilarang dipasang pada PC pengguna^G kecuali dengan kebenaran ICTSO.</p>	
<p>Pengurusan Media Storan^G</p>	
<p>Objektif: Melindungi aset ICT^G dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal</p>	
<p>7.10 Penghantaran dan Pemindahan</p>	
<p>Perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a. Penghantaran atau pemindahan media storan^G ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Setiausaha/Ketua Jabatan terlebih dahulu.</p>	<p>Warga Kementerian / Jabatan</p>
<p>7.11 Prosedur Pengendalian Media Storan^G</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a. Melabelkan semua media storan^G mengikut tahap sensitiviti sesuatu maklumat;</p> <p>b. menghadkan dan menentukan akses media storan^G kepada pengguna^G yang sah sahaja;</p> <p>c. menghadkan pendedaran data atau media storan^G untuk tujuan yang dibenarkan;</p> <p>d. mengawal dan merekodkan aktiviti penyelenggaraan media storan^G bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;</p> <p>e. menyimpan semua media storan^G di tempat yang selamat; dan</p> <p>f. media storan^G yang mengandungi maklumat</p>	<p>Pentadbir Sistem ICT, ICTSO dan Pegawai Yang Diturunkan Kuasa</p>

terperingkat hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	
7.12 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: <ul style="list-style-type: none"> a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. menyedia dan memantapkan keselamatan sistem dokumentasi; dan c. mengawal dan merekodkan semua aktiviti akses sistem dokumentasi sedia ada. 	Pentadbir Sistem ICT, ICTSO dan Pegawai Yang Diturunkan Kuasa
Keselamatan Komunikasi ICT	
Objektif: Melindungi aset ICT ^G melalui sistem komunikasi yang selamat	
7.13 Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: <ul style="list-style-type: none"> a. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Bahagian/Jabatan; b. bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan; c. bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian/Jabatan sebelum dimuat naik ke Internet; d. pengguna^G hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; e. sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang 	Warga Kementrian / Jabatan

<p>dibenarkan oleh Kementerian/Jabatan; dan</p> <p>f. hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti <i>newsgroup</i> dan <i>bulletin board</i>. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Setiausaha/Ketua Jabatan terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan.</p> <p><u>Rujukan:</u></p> <ol style="list-style-type: none"> 1. <i>Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.</i> 2. <i>Garis Panduan dan Etika Penggunaan E-mel dan Internet MOSTI.</i> 	
<p>7.14 Mel Elektronik</p>	
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Akaun-akaun mel elektronik (e-mel) yang diperuntukkan oleh Kementerian/Jabatan sahaja boleh digunakan. Penggunaan akaun-akaun milik orang lain atau akaun-akaun yang dikongsi bersama adalah dilarang; b. setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh Kementerian/Jabatan; c. memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d. penghantaran e-mel rasmi hendaklah menggunakan akaun^G e-mel rasmi dan pastikan 	<p>Warga Kementerian / Jabatan</p>

- alamat e-mel penerima adalah betul;
- e. pengguna^G dinasihatkan menggunakan fail kepilan, dengan saiz fail tidak melebihi dua (2) megabait semasa penghantaran kecuali dengan kebenaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;
 - f. pengguna^G hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui oleh itu identiti pengguna^G hendaklah dikenal pasti terlebih dahulu sebelum meneruskan transaksi maklumat melalui e-mel;
 - g. setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;
 - h. e-mel dari sumber yang tidak diketahui, tidak penting, tidak mempunyai nilai arkib dan yang telah diambil tindakan perlulah dihapuskan;
 - i. e-mel yang diperlukan sebagai bahan rujukan di masa akan datang hendaklah disimpan di dalam storan sekunder; dan
 - j. pengguna^G hendaklah menentukan tarikh dan masa sistem PC adalah tepat.

Rujukan:

1. *Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*
2. *Garis Panduan dan Etika Penggunaan E-mel dan Internet MOSTI.*

8. PERKARA 07 : KAWALAN AKSES

Dasar Kawalan Akses	
Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT ^G Kementerian/Jabatan	
8.1 Keperluan Dasar	
Akses kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna ^G yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan akses pengguna ^G sedia ada.	BPTM ^G Kementerian / Jabatan dan ICTSO
Pengurusan Akses Pengguna^G	
Objektif: Mengawal akses pengguna ^G ke atas aset ICT ^G Kementerian/Jabatan	
8.2 ID Pengguna^G Sistem Aplikasi	
Pengguna ^G adalah bertanggungjawab ke atas sistem ICT yang digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: <ul style="list-style-type: none"> a. ID pengguna^G mestilah unik; b. pemilikan ID pengguna^G bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan Kementerian/Jabatan. Akaun^G boleh ditarik balik jika penggunaannya melanggar peraturan; c. Pentadbir Sistem aplikasi ICT boleh membeku dan membatalkan ID pengguna^G atas sebab-sebab berikut: <ul style="list-style-type: none"> i. pengguna^G bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu kecuali dengan kebenaran; ii. bertukar bidang tugas kerja; iii. bertukar ke agensi lain; iv. bersara; atau 	Pentadbir Sistem ICT dan Pegawai Yang Diturunkan Kuasa

<p>v. ditamatkan perkhidmatan.</p> <p>d. ID pengguna^G yang diperuntukkan oleh Kementerian/Jabatan sahaja boleh digunakan; dan</p> <p>e. menggunakan ID pengguna^G orang lain atau ID pengguna^G yang dikongsi bersama adalah dilarang.</p>	<p>Warga Kementerian / Jabatan</p>
<p>8.3 <i>Audit Trail</i></p>	
<p><i>Audit trail</i> akan merekodkan semua aktiviti sistem. <i>Audit trail</i> juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti <i>audit trail</i> mengandungi:</p> <ul style="list-style-type: none"> a. maklumat identiti pengguna^G, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b. aktiviti akses pengguna^G ke atas sistem ICT sama ada secara sah atau sebaliknya; dan c. maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. <p>Pentadbir Sistem ICT hendaklah menyemak catatan <i>audit trail</i> dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. <i>Audit trail</i> juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubah-suaian yang tidak dibenarkan.</p>	<p>Pentadbir Sistem ICT</p>
<p>Kawalan Akses Sistem Aplikasi</p>	
<p>Objektif: Melindungi sistem aplikasi daripada sebarang bentuk akses yang tidak dibenarkan yang boleh menyebabkan kerosakan</p>	
<p>8.4 <i>Sistem Aplikasi</i></p>	
<p>Akses sistem aplikasi adalah terhad kepada pengguna^G dan</p>	<p>Pentadbir Sistem</p>

<p>kerusakan;</p> <p>b. <i>notebook</i> hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan</p> <p>c. memastikan <i>notebook</i> tidak disimpan di dalam kenderaan bagi mengelakkan daripada dikesan oleh pencuri.</p>	
---	--

9. PERKARA 08 : PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Ciri-ciri Keselamatan Dalam Membangunkan Sistem Aplikasi	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian	
9.1	Keperluan Keselamatan
<p>Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <p>a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujud sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;</p> <p>b. ujian keselamatan hendaklah dijalankan seperti berikut:</p> <p>i. sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan;</p> <p>ii. sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna; dan</p> <p>iii. sistem output untuk memastikan data yang telah diproses adalah tepat.</p> <p>c. sebaik-baiknya, semua sistem yang dibangunkan sama ada secara dalaman atau <i>outsourc</i>e hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan mematuhi keperluan</p>	<p>Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO</p>

keselamatan yang telah ditetapkan sebelum digunakan.	
Kriptografi^G	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat	
9.2 Encryption	
<p>Perkara-perkara berikut hendaklah dipatuhi:</p> <ol style="list-style-type: none"> Pengguna^G hendaklah membuat <i>encryption</i> ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa; penggunaan tandatangan digital adalah dimestikan kepada semua pengguna^G khususnya mereka yang menguruskan transaksi maklumat terperingkat secara elektronik; dan <i>Public Key Infrastructure</i> (PKI) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi PKI berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah PKI tersebut. <p><u>Rujukan:</u></p> <ol style="list-style-type: none"> <i>Arahan Keselamatan Klausa 66 Mengenai Penghantaran Maklumat Terperingkat Melalui Telefon, Telegraf dan Wayarles Oleh Pejabat Keselamatan Kerajaan.</i> <i>The Malaysian Public Sector ICT Management Security Handbook (MyMIS)</i> 	Warga Kementerian / Jabatan
Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat	
9.3 Kawalan Fail-Fail Sistem	
<p>Perkara-perkara berikut hendaklah dipatuhi:</p> <ol style="list-style-type: none"> Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau 	Pentadbir Sistem ICT

<p>pegawai yang diturunkan kuasa;</p> <p>b. <i>coding</i> sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji;</p> <p>c. mengawal akses ke atas <i>coding</i> bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan</p> <p>d. mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.</p>	
<p>Pembangunan dan Proses Sokongan</p>	
<p>Objektif: Menjaga dan menjamin keselamatan sistem aplikasi</p>	
<p>9.4 Kawalan Perubahan</p>	
<p>Perkara berikut hendaklah dipatuhi:</p> <p>a. Perubahan atau pengubahsuaian ke atas sistem aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.</p>	<p>Pentadbir Sistem ICT</p>

10. PERKARA 09 : BUSINESS CONTINUITY PLAN (BCP)

<p>Dasar BCP</p>	
<p>Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan memastikan penyampaian perkhidmatan yang berterusan kepada pelanggan</p>	
<p>10.1 BCP</p>	
<p>BCP hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPIC dan perkara-perkara berikut perlulah diberi perhatian:</p>	<p>ICTSO</p>

<ul style="list-style-type: none"> a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. melaksanakan prosedur-prosedur 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^G mengenai prosedur kecemasan; e. membuat <i>back-up</i>; dan f. menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. 	
--	--

11. PERKARA 10 : PEMATUHAN

Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT MOSTI	
11.1 Pematuhan Dasar	
Setiap pengguna ^G di Kementerian/Jabatan hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MOSTI dan undang-undang atau peraturan/arahan berkaitan yang sedang berkuat kuasa. Semua aset ICT ^G di Kementerian/Jabatan termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Setiausaha/Ketua Jabatan berhak untuk memantau aktiviti pengguna ^G untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Warga Kementerian / Jabatan
11.2 Keperluan Perundangan	
Berikut adalah keperluan perundangan atau peraturan-	

<p>peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna^G di Kementerian/Jabatan:</p>	
<p>a. Keselamatan Perlindungan Secara Am</p> <ul style="list-style-type: none"> i. <i>Emergency (Essential Power) Act 1964;</i> ii. <i>Essential (Key Points) Regulations 1965;</i> iii. Perakuan Jawatankuasa mengkaji semula peraturan keselamatan Pejabat Tahun 1982; iv. Arahan Keselamatan Yang Dikuatkuasakan 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; dan vii. Surat Pekeliling Am Sulit Bil. 1 Tahun 1993 - Meningkatkan Kualiti Kawalan Keselamatan Perlindungan Di Jabatan-Jabatan Kerajaan. 	<p>Warga Kementerian / Jabatan</p>
<p>b. Keselamatan Dokumen^G</p> <ul style="list-style-type: none"> i. <i>Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control);</i> ii. Akta Rahsia Rasmi 1972; iii. Akta Arkib Negara 2003; iv. Surat Pekeliling Bil. 8 Tahun 1990 - Arahan Keselamatan Kawalan, 	<p>Warga Kementerian / Jabatan</p>

<p>Penyelenggaraan, Maklumat-Maklumat Ukur Dan Geografi Yang Antara Lainnya Merangkumi Peta-Peta Rasmi Dan Penderiaan Jauh;</p> <p>v. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 - Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (<i>espionage</i>);</p> <p>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; dan</p> <p>vii. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen^G Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK(R)200/55 Klt.7(21) Bertarikh 21 Ogos 1999.</p>	
<p>c. Keselamatan Fizikal Bangunan</p> <p>i. Akta Kawasan Larangan^G Dan Tempat Larangan Tahun 1959;</p> <p>ii. Arahan Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan^G Dan Tempat</p>	<p>Warga Kementerian / Jabatan</p>

<p>Larangan;</p> <ul style="list-style-type: none"> iii. <i>State Key Points</i>; 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 Kementerian/Jabatan; 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. 	
<p>d. Keselamatan Individu</p> <ul style="list-style-type: none"> i. <i>Government Security Officer: Terms of Reference – Extract On Training Of Departmental Security Office Confidenti</i>; ii. <i>General Circular Memorandum</i>; iii. <i>Instruction On Positive Vetting Procedure</i>; 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- 	<p>Warga Kementerian / Jabatan</p>

<p>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;</p> <p>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</p> <p>viii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.</p>	
<p>e. Keselamatan Aset ICT^G</p> <p>i. Akta Tandatanganan Digital 1997; Akta Jenayah PC 1997;</p> <p>ii. Akta Hak Cipta (Pindaan) 1997;</p> <p>iii. Akta Multimedia dan Telekomunikasi 1998;</p> <p>iv. Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan;</p> <p>v. Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden^G Keselamatan Teknologi Maklumat & Komunikasi (ICT);</p> <p>vi. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan</p>	<p>Warga Kementerian / Jabatan</p>

<p>mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi - Agensi Kerajaan;</p> <p>vii. <i>Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002</i>; dan</p> <p>viii. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005.</p> <p>ix. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden^G Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam .</p> <p>x. Akta dan Peraturan-peraturan lain yang berkaitan.</p>	
--	--

12. GLOSARI ^(G)

Bahagian ini menerangkan istilah-istilah utama yang digunakan di dalam dokumen 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 Kementerian/Jabatan.
BPTM	Bahagian Pengurusan Teknologi Maklumat, MOSTI
Dokumen	Semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut (<i>soft copy</i>), elektronik, dalam talian, kertas lutsinar, risalah atau slaid.
Insiden	Musibah (<i>adverse event</i>) 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.

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

<i>Malware</i>	Merujuk kepada virus, <i>worms</i> , <i>trojan horses</i> , <i>bots</i> dan lain-lain kod jahat.
Media storan	Perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti disket, katrij, cakera padat, cakera mudah alih, pita, cakera keras dan pemacu pena.
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 Kementerian/Jabatan yang menggunakan aset ICT.
Pihak Ketiga	Pihak yang membekalkan perkhidmatan kepada Kementerian/Jabatan.
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 memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing hendaklah diperingkatkan Sulit.

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

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.

13. RUJUKAN

- 13.1 Arahan Keselamatan
- 13.2 Dasar Keselamatan ICT MAMPU
- 13.3 Dasar Keselamatan ICT Kementerian Pelajaran Malaysia
- 13.4 *National Cyber Security Policy*

14. LAMPIRAN

- 14.1 Garis Panduan Dan Etika Penggunaan E-Mel Dan Internet MOSTI

**BAHAGIAN PENGURUSAN TEKNOLOGI MAKLUMAT
KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI, MALAYSIA**
Aras 1, Blok C5, Kompleks C, Pusat Pentadbiran Kerajaan Persekutuan 62662 Putrajaya, Malaysia
Tel: 603-8885 8899 Fax: 603-8889 3005 E-mel: bptm@mosti.gov.my