DASAR KESELAMATAN ICT

Lembaga Perindustrian Kayu Malaysia (MTIB)
Kementerian Perusahaan Perladangan dan Komoditi

14 Disember 2018

Versi 3.2

SEJARAH DOKUMEN DKICT MTIB

TARIKH	EDISI	KELULUSAN	TARIKH KUATKUASA
April 2017	3.1	JPICT	13 April 2017
Disember 2018	3.2	JPICT	14 Disember 2018

ISI KANDUNGAN

PENGENALAN	6
OBJEKTIF	6
PERNYATAAN DASAR	6
SKOP	7
PRINSIP-PRINSIP	9
PENILAIAN RISIKO KESELAMATAN ICT	11
PERKARA 1 : PEMBANGUNAN DAN PENYELENGGARAAN DASAR	12
1.1 Dasar Keselamatan ICT	12
1.1.1 Pelaksanaan Dasar	12
1.1.2 Penyebaran Dasar	12
1.1.3 Penyelenggaraan Dasar	12
1.1.4 Pengecualian Dasar	12
PERKARA 2: KESELAMATAN ORGANISASI	13
2.1 Infrastruktur Organisasi Dalaman	13
2.1.1 Ketua Pengarah MTIB	13
2.1.2 Ketua Pegawai Maklumat (CIO)	13
2.1.3 Pegawai Keselamatan ICT (ICTSO)	14
2.1.4 Pengurus ICT	14
2.1.5 Pentadbir Sistem ICT	15
2.1.6 Pengguna	15
2.1.7 Jawatankuasa Keselamatan Maklumat MTIB	16
2.2 Pihak Ketiga	17
2.2.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	17
PERKARA 3: KAWALAN ASET DAN PENGELASAN MAKLUMAT	19
3.1 Akauntabiliti Aset	19
3.1.1 Inventori Aset ICT	19
3.2 Pengkelasan dan Pengendalian Maklumat	19
3.2.1 Pengkelasan Maklumat	20
3.2.2 Pengendalian Maklumat	20
3.2.3 Pengurusan Rahsia Rasmi Dalam Persekitaran ICT	20
3.2.4 Pengelasan Rahsia Rasmi Dalam Persekitaran ICT	20
3.2.5 Pengelasan Semula Rahsia Rasmi Dalam Persekitaran ICT	21
3.2.6 Pemusnahan Rahsia Rasmi Dalam Persekitaran ICT	21
PERKARA 4 : KESELAMATAN SUMBER MANUSIA	22
4.1 Keselamatan Sumber Manusia Dalam Tugas Harian	22
4.1.1 Sebelum Perkhidmatan	22
4.1.2 Dalam Perkhidmatan	22
4.1.3 Bertukar Atau Tamat Perkhidmatan	23
4.1.4 Tanggungjawab Keselamatan	23
4.1.5 Terma dan Syarat Perkhidmatan	23
4.1.6 Perakuan Akta Rahsia Rasmi	23
4.2 Menangani Insiden Keselamatan ICT	23
4.2.1 Pelaporan Insiden	23
4.3 Pendidikan	24
4.3.1 Program Kesedaran Keselamatan ICT	24
4.4 Tindakan Tatatertib	24

4.4.1 Pelanggaran Dasar	24
PERKARA 5 : KESELAMATAN FIZIKAL	**25**
5.1 Keselamatan Kawasan	**25**
5.1.1 Kawalan Kawasan	25
5.1.2 Kawalan Masuk Fizikal	25
5.1.3 Kawasan Larangan	26
5.2 Keselamatan Peralatan	**26**
5.2.1 Perkakasan	26
5.2.2 Dokumen	28
5.2.3 Media Storan	28
5.2.4 Kabel	29
5.2.5 Penyelenggaraan	30
5.2.6 Peralatan di Luar Premis	30
5.2.7 Pelupusan	30
5.3 Keselamatan Persekitaran	**32**
5.3.1 Kawalan Persekitaran	32
5.3.2 Bekalan Kuasa	33
PERKARA 6 : PENGURUSAN OPERASI DAN KOMUNIKASI	**34**
6.1 Pengurusan Prosidur Operasi	**34**
6.1.1 Pengendalian Prosidur	34
6.1.2 Kawalan Perubahan	34
6.1.3 Pengasingan Tugas dan Tanggungjawab	35
6.2 Pengurusan Penyampaian Pihak Ketiga	**35**
6.2.1 Perkhidmatan Penyampaian	35
6.3 Perancangan dan Penerimaan Sistem	**36**
6.3.1 Perancangan Kapasiti	36
6.3.2 Penerimaan Sistem	36
6.4 Perisian Berbahaya	**36**
6.4.1 Perlindungan dari Perisian Berbahaya	36
6.4.2 Perlindungan dari Mobile Code	37
6.5 Pengemasan Data (Housekeeping)	**37**
6.5.1 Penduaan (*Backup*)	37
6.6 Pengurusan Rangkaian	**38**
6.6.1 Kawalan Infrastruktur Rangkaian	38
6.7 Pengurusan Media	**39**
6.7.1 Penghantaran dan Pemindahan	39
6.7.2 Prosidur Pengendalian Media	39
6.7.3 Keselamatan Sistem Dokumentasi	40
6.8 Keselamatan Komunikasi	**40**
6.8.1 Mel Elektronik	40
6.9 Pemantauan	**43**
6.9.1 Jejak Audit	43
6.9.2 Sistem Log	44
6.9.3 Pemantauan Log	44
PERKARA 7 : KAWALAN CAPAIAN	**46**
7.1 Dasar Kawalan Capaian	**46**
7.1.1 Keperluan Dasar	46
7.2 Pengurusan Capaian Pengguna	**46**
7.2.1 Akaun Pengguna	46

7.2.2 Hak Capaian 47
7.2.3 Pengurusan Kata Laluan 47
7.2.4 *Clear Desk dan Clear Screen* 48
7.3 Kawalan Capaian Rangkaian 49
7.3.1 Capaian Rangkaian 49
7.3.2 Capaian Internet 49
7.3.3 Sistem Maklumat dan Aplikasi 50
7.3.4 Pengurusan/ Kawalan Akses kod Sumber 51
7.4 Peralatan Mudah Alih dan Kerja Jarak Jauh 51
7.4.1 Penggunaan Peralatan Mudah Alih 51
7.4.2 Kerja Jarak Jauh 52

PERKARA 8 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM 53
8.1 Keselamatan dalam Membangunkan Sistem dan Aplikasi 53
8.1.1 Keperluan Keselamatan 53
8.1.2 Pengesahan Data Input dan Output 53
8.2 Kawalan Kriptografi 54
8.2.1 Penyulitan (Enkripsi) 54
8.2.2 Tandatangan Digital 54
8.3 Keselamatan Fail Sistem 54
8.3.1 Kawalan Fail Sistem 54
8.4 Keselamatan Dalam Proses Pembangunan dan Sokongan 55
8.4.1 Kawalan Perubahan 55
8.4.2 Pembangunan Perisian secara *Outsource* 55
8.5 Kawalan Teknikal Keterdedahan (*Vulnerability*) 55
8.5.1 Kawalan dari Ancaman Teknikal 55

PERKARA 9 : PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN 57
9.1 Mekanisme Pelaporan Insiden Keselamatan ICT 57
9.1.1 Mekanisme Pelaporan 57
9.2 Pengurusan Maklumat Insiden Keselamatan ICT 58
9.2.1 Prosidur Pengurusan Insiden Keselamatan ICT 58

PERKARA 10 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN 59
10.1 Dasar Kesinambungan Perkhidmatan 59
10.1.1 Pelan Kesinambungan Perkhidmatan 59

PERKARA 11 : PEMATUHAN 61
11.1 Pematuhan dan Keperluan Perundangan 61
11.1.1 Pematuhan Dasar 61
11.1.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal 61
11.1.3 Pematuhan Keperluan Audit 61
11.1.4 Keperluan Perundangan 61

PERKARA 12 : KHIDMAT NASIHAT 64

PENGENALAN

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Lembaga Perindustrian Kayu Malaysia (MTIB). Dasar ini juga menerangkan kepada semua Pengguna di MTIB mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MTIB.

OBJEKTIF

Dasar Keselamatan ICT diwujudkan untuk menjamin kesinambungan urusan MTIB dengan meminimumkan kesan insiden keselamatan ICT.

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

Manakala, objektif utama Keselamatan ICT MTIB ialah seperti berikut :

a) Memastikan kelancaran operasi MTIB dan meminimumkan kerosakan atau kemusnahan;

b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu :

a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

b) Menjamin setiap maklumat adalah tepat dan sempurna;

c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT MTIB merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut :

a) Kerahsiaan (*Confidentiality*) – Maklumat tidak boleh disebarkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

b) Integriti (*Integrity*) – Data dan maklumat hendaklah tepat, lengkap dikemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;

c) Tidak Boleh Disangkal – Punca data dan maklumat hendaklah daripunca yang sah dan tidak boleh disangkal;

d) Kesahihan (*Authenticity*) – Data dan maklumat hendaklah dijamin kesahihannya; dan

e) Ketersediaan (*Availability*) – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

Aset ICT MTIB terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT MTIB menetapkan keperluan-keperluan asas berikut;

a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT MTIB ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosidur dalam pengendalian semua perkara-perkara berikut;

a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan. Contoh: komputer, pelayan, peralatan komunikasi dan sebagainya;

b) Perisian

Program, prosidur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada MTIB;

c) Perkhidmatan

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

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem akses biometrik; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penyaman udara, sistem pencegahan kebakaran dan lain-lain.

d) Data atau Maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif MTIB. Contohnya, sistem dokumentasi, prosidur operasi, rekod-rekod, pangkalan data dan lain-lain;

e) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

f) Premis Komputer dan Komunikasi

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

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

PRINSIP- PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT MTIB 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 perenggan 53, muka surat 15;

b) Hak akses minimum

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

c) Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT MTIB. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan kata laluan;

v. Mematuhi standard, prosidur, langkah dan garis panduan keselamatan yang ditetapkan;

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

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

d) Pengasingan

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

e) Pengauditan

Pengauditan adalah untuk mengenal insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

Dengan itu, aset ICT seperti komputer, pelayan, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f) Pematuhan

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

g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/ kesinambungan perkhidmatan; dan

h) Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

MTIB hendaklah mengambil kira kewujudan risiko ke atas perkakasan ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu MTIB perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko perkakasan ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

MTIB hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat MTIB termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosidur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

MTIB bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

MTIB perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

a) mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;

b) menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;

c) mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan

d) memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

<table>
<tr><td colspan="2">PERKARA 1 - PEMBANGUNAN DAN PENYELENGGARAAN DASAR</td></tr>
<tr><td colspan="2">1.1 Dasar Keselamatan ICT</td></tr>
<tr><td colspan="2">Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan dan perundangan yang berkaitan.</td></tr>
<tr><td colspan="2">1.1.1 Pelaksanaan Dasar</td></tr>
<tr><td>Pelaksanaan dasar ini adalah tanggungjawab Ketua Pengarah MTIB selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT) MTIB yang terdiri daripada Timbalan Ketua Pengarah, Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan semua Pengarah Bahagian.</td><td>Ketua Pengarah MTIB</td></tr>
<tr><td colspan="2">1.1.2 Penyebaran Dasar</td></tr>
<tr><td>Dasar ini perlu disebarkan kepada semua pengguna MTIB (termasuk wargakerja, pembekal, pakar runding dan pihak yang berurusan dengan MTIB).</td><td>ICTSO</td></tr>
<tr><td colspan="2">1.1.3 Penyelenggaraan Dasar</td></tr>
<tr><td>Dasar Keselamatan ICT MTIB adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosidur dan proses selaras dengan perubahan teknologi, aplikasi, prosidur, perundangan dan kepentingan sosial.

Berikut adalah prosidur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT MTIB:
a) Kenal pasti dan tentukan perubahan yang diperlukan;
b) Kemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) MTIB;
c) Perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna; dan
d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun (jika perlu).</td><td>ICTSO</td></tr>
<tr><td colspan="2">1.1.4 Pengecualian Dasar</td></tr>
<tr><td>Dasar keselamatan ICT MTIB adalah terpakai kepada semua pengguna ICT MTIB dan tiada pengecualian diberikan.</td><td>Semua</td></tr>
</table>

PERKARA 2 - KESELAMATAN ORGANISASI	
2.1 Infrastruktur Organisasi Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT MTIB.	
2.1.1 Ketua Pengarah MTIB	
Peranan dan tanggungjawab Ketua Pengarah MTIB adalah seperti berikut: a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MTIB; b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT MTIB; c) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT MTIB; d) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; e) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT MTIB; dan f) Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) MTIB.	Ketua Pengarah MTIB
2.1.2 Ketua Pegawai Maklumat (CIO)	
Pengarah Khidmat Pengurusan MTIB adalah merupakan Ketua Pegawai Maklumat (CIO) MTIB. Peranan dan tanggung jawab beliau adalah seperti berikut: a) Membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b) Menentukan keperluan keselamatan ICT; c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT MTIB serta pengurusan risiko dan pengauditan; dan d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT MTIB.	CIO

2.1.3 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MTIB kepada semua pengguna; b) Mewujudkan garis panduan, prosidur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MTIB; c) Menjalankan pengurusan risiko; d) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan MTIB berdasarkan hasil penemuan dan menyediakan laporan mengenainya; e) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; f) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada CIO; g) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; h) Menyiasat dan memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT MTIB; dan i) Mengurus, menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	ICTSO
2.1.4 Pengurus ICT	
Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MTIB; b) Menentukan kawalan akses pengguna terhadap aset ICT MTIB; c) Melaporkan sebarang perkara atau penemuan mengenai Keselamatan ICT kepada ICTSO; d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MTIB.	Pengurus ICT

2.1.5 Pentadbir Sistem ICT	
Pegawai Teknologi Maklumat merupakan pentadbir sistem ICT MTIB. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut: a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai wargakerja yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan dalam Dasar Keselamatan ICT MTIB; c) Memantau aktiviti capaian harian sistem aplikasi pengguna; d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta-merta; e) Menyimpan dan menganalisis rekod jejak audit; f) Menyediakan laporan mengenai aktiviti capaian berdasarkan keperluan; dan g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya dalam keadaan yang baik.	Unit Teknologi Maklumat
2.1.6 Pengguna	
Pengguna adalah merupakan semua pegawai/ wargakerja MTIB. Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT MTIB; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat MTIB; e) Melaksanakan langkah-langkah perlindungan seperti berikut:	Pengguna

i) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii) Menentukan maklumat sedia untuk digunakan; iv) Menjaga kerahsiaan kata laluan; v) Mematuhi standard, prosidur, langkah dan garis panduan keselamatan yang ditetapkan; vi) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO, Pengurus ICT dan Pentadbir Sistem ICT dengan segera; dan g) Menghadiri program-program kesedaran mengenai keselamatan ICT; h) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MTIB sebagaimana **Lampiran 1.**	
2.1.7 Jawatankuasa Keselamatan Maklumat MTIB	**Tindakan**
Jawatankuasa Keselamatan Maklumat MTIB adalah jawatankuasa yang bertanggungjawab dalam keselamatan maklumat MTIB dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan maklumat MTIB. Keanggotaan Jawatankuasa Keselamatan Maklumat MTIB adalah seperti berikut : **Pengerusi :** Timbalan Ketua Pengarah **Ahli** : (1) CIO MTIB (2) Semua Pengarah Bahagian (3) Pegawai Keselamatan MTIB (4) ICTSO MTIB **Urus Setia :** Unit Pentadbiran/ Pejabat Ketua Pengarah	Jawatankuasa Keselamatan Maklumat MTIB

Bidang Kuasa : (a) Memantau dan menyemak: i. pelaksanaan pensijilan ISMS ke atas perkhidmatan MTIB; ii. menetap kriteria penerimaan risiko, tahap risiko dan *risk treatment plan;* iii. penemuan awal penilaian risiko aset sistem MyRisk di MTIB; iv. menetapkan struktur organisai ISMS; v. pengurusan dokumen dan rekod pelaksanaan ISMS; (b) Menguruskan perlantikan Pasukan Audit Dalam dan Ketua Audit Dalam ISMS MTIB; (c) Mengadakan Mesyuarat Kajian Semula Pengurusan ISMS; (d) Memantau pelaksanaan tindakan pembetulan/ penambahbaikan dan pencegahan; (e) Memantau keberkesanan tindakan pembetulan/ penambahbaikan dan pencegahan; (f) Merancang keberkesanan Pengurusan Keselamatan Maklumat di MTIB; dan (g) Menjadi *liason* kepada pengauditan pihak ketiga.	
2.2 Pihak Ketiga	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (pembekal, pakar runding dan lain-lain)	
2.2.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: a) Membaca, mematuhi dan memahami Dasar Keselamatan ICT MTIB; b) Mengenalpasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c) Mengenalpasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d) Akses kepada aset ICT MTIB perlu berlandaskan kepada perjanjian kontrak;	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

e) Memastikan semua syarat-syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan dalam perjanjian yang dimeterai:

i. Dasar Keselamatan ICT MTIB;

ii. Tapisan Keselamatan

iii. Perakuan Akta Rahsia Rasmi 1972 dimana adalah menjadi kesalahan Seksyen 8 Akta Rahsia Rasmi sekiranya sebarang rahsia rasmi dibocorkan;

iv. Hak Harta Intelek;

Pihak Ketiga adalah bertanggungjawab untuk mendapatkan Hak Harta Intelek untuk sebarang perkakasan dan perisian yang dibekalkan kepada MTIB. MTIB tidak akan bertanggungjawab ke atas sebarang isu yang berkaitan dengan Hak Harta Intelek perkakasan dan perisian yang dibekalkan.

f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT MTIB sebagaimana **Lampiran 2**.

<table>
<tr><th colspan="2">PERKARA 3 – KAWALAN ASET DAN PENGKELASAN MAKLUMAT</th></tr>
<tr><td colspan="2">3.1 Akauntabiliti Aset</td></tr>
<tr><td colspan="2">Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT MTIB.</td></tr>
<tr><td colspan="2">3.1.1 Inventori Aset ICT</td></tr>
<tr><td>Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing.

Perkara yang perlu dipatuhi adalah seperti berikut:

a) Memastikan semua aset ICT dikenalpasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemaskini;

b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;

c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di MTIB;

d) Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, di dokumen dan dilaksanakan; dan

e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.</td><td>Pentadbir Sistem dan Semua</td></tr>
<tr><td colspan="2">3.2 Pengkelasan dan Pengendalian Maklumat</td></tr>
<tr><td colspan="2">Objektif:
Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.</td></tr>
<tr><td colspan="2">3.2.1 Pengkelasan Maklumat</td></tr>
<tr><td>Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan.

Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:

a. Rahsia Besar;</td><td>Semua dan Pegawai Pengkelas Dokumen</td></tr>
</table>

b. Rahsia; c. Sulit; atau d. Terhad.	
3.2.2 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat, menyemak dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi standard, prosidur, langkah dan garis panduan keselamatan yang ditetapkan; f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua
3.2.3 Pengurusan Rahsia Rasmi Dalam Persekitaran ICT	
Mematuhi tatacara pengurusan rahsia rasmi dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa.	Semua
3.2.4 Pengelasan Rahsia Rasmi Dalam Persekitaran ICT	
Pengelasan perlu dibuat oleh Pengawal Pengelas yang dilantik dibawah Seksyen 2B Akta 88. Sistem aplikasi yang menyimpan maklumat rahsia rasmi perlulah berupaya untuk memberikan tanda keselamatan pada setiap antara muka (interface).	Pengawal Pengelas

3.2.5 Pengelasan Semula Rahsia Rasmi Dalam Persekitaran ICT	
Mengambil tindakan untuk mengelaskan semua maklumat rahsia rasmi berdasarkan kepada peruntukan Seksyen 2C Akta 88 sekiranya maklumat berkenaan tidak perlu menjadi rahsia rasmi.	Pengawal Pengelas
3.2.6 Pemusnahan Rahsia Rasmi Dalam Persekitaran ICT	
Mendapatkan khidmat nasihat daripada Ketua Pengarah Keselamatan Kerajaan dan Ketua Pengarah Arkib Negara berhubung dengan pemusnahan maklumat rahsia rasmi.	Pengawal Pengelas

PERKARA 4 – KESELAMATAN SUMBER MANUSIA	
4.1 Keselamatan Sumber Manusia Dalam Tugas Harian	
Objektif: Memastikan semua sumber manusia yang terlibat termasuk pegawai dan wargakerja MTIB, pembekal, pakar runding dan pihak-pihak berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Wargakerja MTIB hendaklah mematuhi terma dan syarat perkhidmtan serta peraturan semasa yang berkuatkuasa.	
4.1.1 Sebelum Perkhidmatan	
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan wargakerja MTIB serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pegawai dan wargakerja MTIB serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	
4.1.2 Dalam Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut : a) Memastikan pegawai dan wargakerja MTIB serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundagan dan peraturan yang ditetapkan oleh MTIB; b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT MTIB secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan wargakerja MTIB serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh MTIB; dan d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan	

ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian khidmat Pengurusan, MTIB.	
4.1.3 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut : a) Memastikan semua aset ICT dikembalikan kepada MTIB mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh MTIB dan/atau terma perkhidmatan.	
4.1.4 Tanggungjawab Keselamatan	
Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkodkan, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.	Semua
4.1.5 Terma dan Syarat Perkhidmatan	
Semua warga MTIB yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan oleh peraturan semasa yang berkuat kuasa.	Semua
4.1.6 Perakuan Akta Rahsia Rasmi	
Warga MTIB yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua
4.2 Menangani Insiden Keselamatan ICT	
Objektif: Meminimumkan kesan insiden keselamatan ICT.	
4.2.1 Pelaporan Insiden	
Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO atau Pengurus ICT dengan kadar segera: ▪ Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;	Semua

▪ Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; ▪ Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; ▪ Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan kesilapan komunikasi; ▪ Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Nota : Pekeliling Am Bilangan 1 Tahun 2001 bertajuk **"Mekanisme Pelaporan Insiden Keselamatan ICT"** dan Surat pekeliling Am Bilangan 4 Tahun 2006 bertajuk **"Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam"** mengenainya bolehlah dirujuk.	
4.3 Pendidikan	
Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT	
4.3.1 Program Kesedaran Keselamatan ICT	
Setiap pengguna di MTIB perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT MTIB.	ICTSO
4.4 Tindakan Tatatertib	
Objektif: Meningkatkan kesedaran dan pematuhan ke atas Dasar Keselamatan ICT MTIB	
4.4.1 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT MTIB boleh dikenakan tindakan tatatertib.	Semua

PERKARA 5 – KESELAMATAN FIZIKAL DAN PERSEKITARAN	
5.1 Keselamatan Kawasan	
Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
5.1.1 Kawalan Kawasan	
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Kawasan keselamatan fizikal hendaklah dikenalpasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat (jika perlu); c) Memasang alat penggera atau kamera; d) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan wargakerja yang diberi kebenaran sahaja boleh memasuki pintu masuk ini; dan e) Menyediakan garis panduan untuk wargakerja yang bekerja di dalam kawasan terhad;	CIO, ICTSO
5.1.2 Kawalan Masuk Fizikal	
Kawalan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis atau bangunan MTIB. a) Setiap pengguna MTIB hendaklah menggunakan sistem akses biometrik; b) Hanya pengguna yang diberi kebenaran sahaja (yang mempunyai akses) boleh mencapai atau menggunakan aset ICT MTIB; c) Setiap pelawat hendaklah mendapatkan Pas Pelawat di Tingkat 15, Ibu Pejabat MTIB (hanya di Ibu Pejabat sahaja). Pas ini hendaklah dikembalikan semula selepas tamat lawatan.	Semua

5.1.3 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 MTIB adalah bilik Ketua Pengarah, bilik Timbalan Ketua Pengarah dan pusat data. a) Secara umumnya, peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu; b) Pihak-pihak lain adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan c) Semua penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran.	Semua
5.2 Keselamatan Peralatan	
Objektif: Melindungi peralatan dan maklumat dari kehilangan, kerosakan, kecurian serta gangguan.	
5.2.1 Perkakasan	
Secara umumnya aset ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu. Perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna; b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; e) Pengguna adalah bertanggungjawab atas kerosakan atau	Semua

kehilangan peralatan ICT di bawah kawalannya; f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan; g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; k) Semua peralatan yang digunakan secara berterusan hendaklah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; l) Peralatan ICT yang hendak dibawa keluar dari MTIB perlulah mendapat kelulusan dan direkodkan bagi tujuan pemantauan; m) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran; p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan untuk dibaik pulih; 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; s) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah	

digunakan sepenuhnya bagi urusan rasmi sahaja; t) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan u) Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
5.2.2 Dokumen	
Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat perlu dilaksanakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b) Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen (jika perlu); c) Mewujudkan sistem pengurusan dokumen terperingkat bagi menerima, memproses, menyimpan dan menghantar dokumen terperingkat supaya ianya diuruskan berasingan daripada dokumen-dokumen tidak terperingkat; d) Memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak; e) Memastikan maklumat yang hendak dikirim menggunakan media elektronik hanya maklumat yang betul; f) Dokumen rahsia rasmi tidak dibenarkan dihantar menggunakan e-mel kecuali dengan kelulusan; dan g) Menggunakan enkripsi (*encryption*) ke atas dokumen terperingkat yang disediakan dan dihantar secara elektronik (jika perlu).	Semua
5.2.3 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain. Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-	Semua

langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat : a) Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b) Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; c) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; d) Merekodkan sistem pengurusan media termasuk inventori, pergerakan, melabel dan penduaan (*backup*); e) Mengimbas untuk memastikan media storan mudah alih (seperti *thumb/ pen drive*, disket dan sebagainya) bebas dari virus dan apa-apa perisian yang boleh mengakibatkan berlakunya insiden keselamatan ICT. f) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; g) 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; h) Akses dan pergerakan media storan hendaklah direkodkan; i) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; dan j) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat.	
5.2.4 Kabel	
Kabel termasuk kabel elektrik dan komunikasi hendaklah dilindung kerana boleh menjadi punca maklumat menjadi terdedah. Perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman dan kerosakan *wire tapping*; dan d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel	ICTSO dan Unit Teknologi Maklumat

daripada kerosakan dan pintasan maklumat.	
5.2.5 Penyelenggaraan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b) Memastikan semua perkakasan hanya boleh diselenggara oleh wargakerja atau pihak yang dibenarkan sahaja; c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	Semua
5.2.6 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari MTIB adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Peralatan perlu dilindungi dan dikawal sepanjang masa; b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; c) Peralatan, maklumat atau perisian yang dibawa keluar mestilah mendapat kelulusan Pengurus ICT/ pegawai yang mentadbir peralatan dan tertakluk kepada tujuan yang dibenarkan.	Semua
5.2.7 Pelupusan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh MTIB. Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan	Semua

semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MTIB.

Perkara-perkara yang perlu dipatuhi adalah seperti berikut:

a) Semua kandungan peralatan khususnya maklumat rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding*, *grinding*, *degauzing* atau pembakaran;

b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;

c) Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;

d) Lembaga Pemeriksa Pelupusan hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya;

e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut;

f) Pegawai aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemaskini rekod pelupusan peralatan ICT ke dalam sistem inventori Sistem Pengurusan Aset;

g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

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

   i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalam CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya;

   ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian;

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

   iv. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.

Nota: Maklumat lanjut pelupusan bolehlah merujuk kepada Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan".	
5.3 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT MTIB dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
5.3.1 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	Semua

5.3.2 Bekalan Kuasa	
a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b) Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Unit Teknologi Maklumat dan ICTSO

PERKARA 6 – PENGURUSAN OPERASI DAN KOMUNIKASI	
6.1 Pengurusan Prosidur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
6.1.2 Pengendalian Prosidur	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosidur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b) Setiap prosidur 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; c) Semua prosidur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan; d) Semua wargakerja MTIB hendaklah mematuhi prosidur yang telah ditetapkan.	Semua
6.1.3 Kawalan Perubahan	
a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosidur mestilah mendapat kebenaran dari pegawai atasan atau pemilik aset terlebih dahulu; b) Aktiviti-aktiviti seperti memasang, menyelenggara, 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 berkenaan; c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d) Semua aktiviti perubahan atau pengubahsuaian hendaklah	Semua

direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau tidak.	
6.1.4 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b) Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan c) Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*.	Pengurus ICT dan ICTSO
6.2 Pengurusan Penyampaian Pihak Ketiga	
Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
6.2.1 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diperiksa sekurang-kurangnya dua (2) kali setahun atau mengikut keperluan dan c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua

<table>
<tr><td colspan="2">6.3 Perancangan dan Penerimaan Sistem</td></tr>
<tr><td colspan="2">Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.</td></tr>
<tr><td colspan="2">6.3.1 Perancangan Kapasiti</td></tr>
<tr><td>Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang;

Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang; dan

Penggunaan peralatan mestilah dipantau, ditala (tuned) dan perancangan perlu dibuat bagi memastikan prestasi sistem di tahap optimum.</td><td>ICTSO</td></tr>
<tr><td colspan="2">6.3.2 Peneriman Sistem</td></tr>
<tr><td>Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria dan diujilari minimum lima belas (15) hari sebelum diterima atau dipersetujui.</td><td>Pentadbir Sistem ICT dan ICTSO</td></tr>
<tr><td colspan="2">6.4 Perisian Berbahaya</td></tr>
<tr><td colspan="2">Objektif:

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian seperti virus, malware, adware dan phishing.</td></tr>
<tr><td colspan="2">6.4.1 Perlindungan dari Perisian Berbahaya</td></tr>
<tr><td>a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, intrusion detection system (IDS), intrusion prevention system (IPS) dan mengikut prosidur penggunaan yang betul dan selamat;

b) Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997;

c) Pengguna mesti mengimbas semua perisian atau sistem dengan perisian keselamatan seperti antivirus, spyware, adware sebelum menggunakannya;

d) Mengemaskini pattern atau signature perisian keselamatan secara berkala oleh Pentadbir Sistem secara automatik;</td><td>Semua</td></tr>
</table>

e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g) 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 program berbahaya; h) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
6.4.2 Perlindungan dari *Mobile Code*	**Tindakan**
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
6.5 Pengemasan Data (Housekeeping)	
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.	
6.5.1 Penduaan (*Backup*)	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b) Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan penduaan bergantung pada tahap kritikal maklumat; c) Menguji sistem penduaan sedia ada sekurang-kurangnya setahun sekali bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d) Salinan maklumat dan perisian perlu dibuat dan diuji secara berkala berdasarkan kepada prosidur penduaan; e) Menyimpan sekurang-kurangnya tiga (3) generasi	Semua

penduaan;dan f) Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.	
6.6 Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
6.6.1 Kawalan Infrastruktur Rangkaian	
Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan:- a) Tanggungjawab atau kerja-kerja operasi rangkaian komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Semua peralatan perlu melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e) *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem/ pentadbir rangkaian; f) Semua trafik keluar dan masuk hendaklah melalui sistem tapisan keselamatan seperti *firewall* dan *web content filtering* di bawah kawalan MTIB; g) Pemasangan sistem tapisan keselamatan pada laluan keluar dan masuk rangkaian (*Internet Gateway)* adalah perlu untuk menyekat aktiviti yang dilarang seperti yang termaktub dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; h) Sebarang penyambungan rangkaian yang bukan di bawah kawalan MTIB hendaklah mendapat kebenaran ICTSO; i) Semua pengguna hanya dibenarkan menggunakan rangkaian di bawah kawalan MTIB sahaja. Penggunaan peralatan perhubungan rangkaian yang lain adalah dilarang sama sekali; j) Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih	Unit Teknologi Maklumat

optimum; dan Penggunaan tanpa wayar LAN di MTIB hendaklah mematuhi peraturan-peraturan yang dikeluarkan dari masa ke semasa oleh agensi tertentu seperti PKPA MAMPU dan sebagainya.	
6.7 Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan daripada pemilik terlebih dahulu.	
6.7.1 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu. Media yang mengandungi maklumat Kerajaan perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari MTIB. Prosidur perlu disediakan untuk pengurusan media mudah alih.	Semua
6.7.2 Prosidur Pengendalian Media	
Prosidur ini bertujuan untuk mengendali dan menyimpan maklumat yang perlu diwujudkan untuk melindungi maklumat daripada didedahkan tanpa kebenaran atau disalahguna. a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat (jika perlu); b) Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e) Menyimpan semua media di tempat yang selamat; f) Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosidur yang betul dan selamat. Nota: Maklumat lanjut pelupusan bolehlah merujuk kepada Surat Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk “Tatacara Pengurusan Aset Alih Kerajaan”.	Semua

6.7.3 Keselamatan Sistem Dokumentasi	
Dokumentasi sistem perlu dilindungi daripada capaian yang tidak dibenarkan. Langkah-langkah yang perlu dipatuhi ialah: a) Memastikan sistem penyimpan dokumentasi mempunyai ciri-ciri keselamatan; b) Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c) Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Semua
6.8 Keselamatan Komunikasi	
Objektif: Melindungi aset ICT melalui sistem komunikasi yang selamat.	
6.8.1 Mel Elektronik	
E-mel merupakan satu cara perhubungan yang paling mudah dan murah di antara pengguna dengan pelbagai pihak. Unit Teknologi Maklumat memandang serius mengenai aspek keselamatan perhubungan melalui e-mel di antara wargakerja MTIB, terutama yang melibatkan dokumen terperingkat. **E-mel yang diperuntukkan oleh Jabatan hanya boleh digunakan untuk tujuan rasmi sahaja.** E-mel rasmi boleh dibahagikan kepada dua kategori berikut: **i. E-mel Rahsia Rasmi** E-mel yang mengandungi maklumat atau perkara rahsia rasmi yang mesti diberi perlindungan utuk kepentingan keselamatan yang dikelaskan mengikut pengelasannya sama ada Terhad, Sulit, Rahsia atau Rahsia Besar. **ii. E-mel Bukan Rahsia Rasmi** E-mel yang tidak mengandungi maklumat atau perkara rahsia rasmi. **Semua wargakerja** MTIB adalah **diperuntukkan satu akaun e-mel rasmi**, walau bagaimanapun **pewujudan akaun ini bukan secara automatik**. **Permohonan akaun emel baru** perlu dibuat melalui **e-mel rasmi Jabatan**. Semua urusan ***reset* kata laluan** dan **penutupan akaun** juga perlu melalui e-mel rasmi Jabatan. Unit Teknologi Maklumat **tidak akan melayan permohonan yang tidak melalui emel rasmi Jabatan.**	Semua

Maklumat yang terdapat dalam mel elektronik MTIB perlu dilindungi sebaik-baiknya bagi menghindari capaian atau sebaran maklumat yang tidak dibenarkan. Akaun atau alamat e-mel adalah bukan hak mutlak pengguna dan penggunaannya tertakluk kepada peraturan yang ditetapkan. Akaun atau alamat e-mel ini adalah hak milik MTIB. Perkara yang perlu dipatuhi adalah seperti berikut: a) Pengguna hanya boleh menggunakan akaun atau alamat e-mel yang diperuntukkan oleh MTIB. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b) Pengguna mestilah bertanggungjawab atas akaun e-mel yang diberikan kepadanya; c) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh MTIB; d) Pengguna mestilah memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; e) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; f) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi 10 Mb semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; g) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui yang berkemungkinan mengandungi virus; h) Pengguna dilarang menyebarkan kod perosak seperti virus, *worm*, *Trojan Horse* dan *trap door* yang boleh merosakkan sistem komputer dan maklumat pengguna lain; i) Pengguna dilarang menyebarkan gambar-gambar lucah, e-mel berunsurkan fitnah, perkauman, gangguan seksual atau yang berkaitan dengannya; j) Pengguna dilarang membuka e-mel yang mengandungi fail kepilan (attachment file) seperti *.scr, *.com, *.exe, *.pif, *.vbs, *.bat, *.asd, *.chm, *.ocx, *.hlp, *.hta, *.js, *.shb, *.shs, *.vb, *.vbe, *.wsf, *.wsh, *.reg, *.ini, *.diz, *.cpp, *.cpl, *.vxd, *.sys dan *.cmd. Ia berkemungkinan akan menyebarkan virus apabila dibuka. k) Pengendalian E-mel Rahsia Rasmi Pengurusan maklumat terperingkat adalah tertakluk di bawah peruntukan Akta Rahsia Rasmi 1972. Perkara–perkara berikut perlu dilaksanakan bagi menentukan keselamatan dan kesahihan e-mel rahsia rasmi iaitu:	

i) Maklumat terperingkat sebolehnya **tidak di e-mel kecuali perlu**;
ii) **Penyulitan** mesti dilakukan ke atas semua e-mel rahsia rasmi yang dihantar, diterima dan disimpan;
iii) Penerima e-mel rahsia rasmi mesti **mengesahkan kesahihan dokumen** apabila ditandatangani secara digital oleh pengirim;
iv) Penerima mesti **membuat akuan penerimaan** e-mel rahsia rasmi sebaik sahaja menerimanya;
v) E-mel rahsia rasmi bertanda **Rahsia Besar dan Rahsia tidak boleh dimajukan** kepada pihak lain. Sementara e-mel bertanda **Sulit dan Terhad** yang hendak dimajukan kepada pihak lain **memerlukan izin daripada pemula dokumen**; dan
vi) E-mel yang melibatkan maklumat rahsia rasmi yang hendak dimusnahkan perlulah **dihapuskan secara kekal** dari folder 'Deleted Items' atau dengan melaksanakan 'Empty Trash'.

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

m) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan (dalam *inbox* atau disimpan dalam *folder* yang berasingan pada *desktop*) mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan dan tidak boleh dihapuskan;

n) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi boleh dihapuskan;

o) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

p) Pengguna dilarang menggunakan e-mel rasmi untuk kepentingan peribadi, aktiviti komersial dan politik.

q) Unit Pengurusan Sumber Manusia hendaklah memaklumkan kepada Pentadbir Sistem bagi penghapusan akaun pengguna yang tidak aktif di MTIB.

r) Tidak mendedahkan kata laluan kepada sesiapa walaupun diminta sama ada melalui e-mel atau medium lain;

s) Memastikan kata laluan mengandungi kombinasi nombor, huruf, dan simbol dengan minimum enam (6) aksara;

t) Mencetak dan mendokumenkan semua e-mel yang penting untuk mengelakkan kehilangan maklumat penting apabila berlaku kerosakan kepada cakera keras komputer;

u) Membuat salinan dan menyimpan fail kepilan ke dalam satu folder berasingan dari setiap e-mel yang penting bagi tujuan backup jika berlaku sebarang masalah kepada cakera keras komputer; v) Melakukan imbasan ke atas semua fail dan fail kepilan bagi mengenalpasti fail yang diserang virus dengan perisian anti virus yang digunapakai MTIB; w) Memastikan kemudahan e-mel digunakan pada keseluruhan waktu bekerja supaya e-mel yang dialamatkan sampai tepat pada masanya dan tindakan segera dapat diambil ke atasnya; x) Untuk keselamatan dokumen rahsia rasmi dan maklumat terperingkat yang dihantar melalui e-mel disulitkan terlebih dahulu; y) Menggunakan *carbon copy* (cc) apabila e-mel tersebut perlu dimaklumkan kepada penerima lain. z) Memaklumkan dengan segera nama wargakerja yang bertukar atau berhenti kepada Unit Teknologi Maklumat agar akaun mereka dapat dikemaskini. Unit Teknologi Maklumat tidak akan bertanggungjawab ke atas e-mel yang hilang bagi pengguna yang tidak mematuhi polisi penggunaan e-mel Nota: Maklumat lanjut mengenai keselamatan e-mel boleh lah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan’.	
6.9 Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
6.9.1 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (audit trail). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam system secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identity pengguna,	Pentadbir Sistem ICT

sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
6.9.2 Sistem Log	Tindakan
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT
6.9.3 Pemantauan Log	Tindakan
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (b) Prosidur 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;	Unit IT dan Pentadbir Sistem ICT

(e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan (f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam MTIB atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

PERKARA 7 – KAWALAN CAPAIAN	
7.1 Dasar Kawalan Capaian	
Objektif: Memahami dan mematuhi keperluan dalam mencapai dan menggunakan aset ICT MTIB.	
7.1.1 Keperluan Dasar	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas perkakasan ICT mengikut keperluan keselamatan dan peranan pengguna; b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d) Kawalan ke atas kemudahan sistem aplikasi dan pemprosesan maklumat;	Unit Teknologi Maklumat, ICTSO
7.2 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas aset ICT MTIB.	
7.2.1 Akaun Pengguna	
Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a) Akaun yang diperuntukkan oleh MTIB sahaja boleh digunakan; b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c) Akaun pengguna diwujudkan berdasarkan peranan yang diluluskan oleh pemilik sistem. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan MTIB. Akaun boleh ditarik	Pemilik Sistem dan Pentadbir Sistem

balik jika penggunaannya melanggar peraturan; e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; f) Pentadbir sistem ICT boleh membeku akaun pengguna atas sebab-sebab berikut setelah mendapat arahan daripada pemilik sistem : i. Pengguna yang tidak hadir bertugas dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; g) Pentadbir sistem ICT boleh menamatkan akaun pengguna setelah mendapat arahan daripada pentadbir sistem atas sebab-sebab berikut: i. Bertukar ke agensi lain; ii. Bersara; atau iii. Ditamatkan perkhidmatan.	
7.2.2 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
7.2.3 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosidur yang ditetapkan seperti berikut: a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c) Panjang kata laluan adalah sekurang-kurangnya enam (6) aksara dengan gabungan aksara, angka dan aksara khusus; d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan	Semua dan Pentadbir Sistem ICT

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 (jika perlu); h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) Tentukan had masa pengesahan selama tiga puluh (30) minit maksimum (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; j) Kata laluan digalakkan ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan k) Mengelakkan penggunaan semula kata laluan yang telah bocor atau dikompromi.	
7.2.4 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja wargakerja atau di paparan skrin apabila wargakerja tidak berada di tempatnya : a) Gunakan kemudahan *password screen saver* atau log keluar secara automatik had masa 30 minit bagi pegawai dan 10 minit di ruang terbuka apabila meninggalkan komputer; dan b) Bahan-bahan bukan untuk pengetahuan orang lain hendaklah disimpan dalam laci atau kabinet fail yang berkunci; dan c) Kaedah penyimpanan maklumat terperingkat d) Adalah menjadi tanggungjawab seseorang individu untuk memastikan komputer yang digunakan tidak mendedahkan maklumat terperingkat.	Semua

7.3 Kawalan Capaian Rangkaian	
Objektif : Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
7.3.1 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian yang bertujuan meningkatkan tahap keselamatan adalah dengan: a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian MTIB, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan c) Menguatkuasa dan memantau kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Rangkaian
7.3.2 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan Internet di MTIB hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang dilarang atau tidak sepatutnya ke dalam rangkaian MTIB; b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;	Pentadbir Rangkaian
c) Penggunaan Internet hanyalah untuk kegunaan rasmi dan yang dibenarkan berdasarkan peraturan kerajaan sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; d) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Pengarah/ pegawai yang diberi kuasa; e) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;	Semua

f) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet; g) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; h) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh MTIB; i) Setiap wargakerja hendaklah beretika dan menjaga imej organisasi ketika berinteraksi secara maya di internet. Hanya pegawai yang mendapat kebenaran sahaja boleh bertindak mewakili MTIB menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; j) Penggunaan modem atau peralatan selain dibekalkan oleh MTIB untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan k) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur lucah.	
7.3.3 Sistem Maklumat dan Aplikasi	
Capaian sistem dan aplikasi di MTIB adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan *sensitivity* maklumat yang telah ditentukan; b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan	Pentadbir Sistem ICT, ICTSO

aktiviti-aktiviti yang tidak diingini; c) Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d) Menghadkan capaian sistem dan aplikasi kepada beberapa kali cubaan bergantung kepada sistem. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat (bergantung pada sistem); e) Memastikan kawalan sistem rangkaian dilaksanakan berdasarkan arahan kerajaan atau amalan terbaik dan lengkap dengan ciri-ciri keselamatan bagi mengurangkan risiko aktiviti atau capaian yang tidak sah; dan f) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah terhad kepada perkhidmatan yang dibenarkan sahaja.	
7.3.4 Pengurusan/ Kawalan Akses kod Sumber	
Kod sumber hendaklah dilaksanakan ke atas sistem aplikai yang dibekalkan hasil pembangunan secara outsource atau in-house. Ini bagi memastikan kesinambungan sistem aplikasi. Juga, bagi mengawal capaian ke atas kod sumber (aturcara program) bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian selearas keperluan DKICT MTIB. Pembangunan aplikasi atau perisian secara outsource perlu diselia dan dipantau oleh personel Teknologi Maklumat iaitu: a) Wargakerja MTIB perlu dihadkan akses kepada kod sumber; b) Kawal akses kod sumber menerusi kelulusan; c) Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada prosidur kawalan perubahan; dan d) Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik MTIB.	Pengurus ICT, Pentadbir Sistem
7.4 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.	
7.4.1 Penggunaan Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut:	Semua

a) Merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan kehilangan atau kerosakan; dan b) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	
7.4.2 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

PERKARA 8 – PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
8.1 Keselamatan dalam Membangunkan Sistem dan Aplikasi	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
8.1.1 Keperluan Keselamatan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem *output* untuk memastikan data yang telah diproses adalah tepat; c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO
8.1.2 Pengesahan Data Input dan Output	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem dan Pentadbir Sistem ICT

8.2 Kawalan Kriptografi	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
8.2.1 Enkripsi	
Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
8.2.2 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
8.3 Keselamatan Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
8.3.1 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosidur yang telah ditetapkan; b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c) Mengawal capaian ke atas kod atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; dan e) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal.	Pentadbir Sistem ICT

8.4 Pembangunan dan Proses Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi	
8.4.1 Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d) Akses kepada kod sumber (*source code*) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e) Menghalang sebarang peluang untuk membocorkan maklumat.	Pemilik Sistem dan Pentadbir Sistem ICT
8.4.2 Pembangunan Perisian Secara *Outsource*	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem dan Pentadbir Sistem; Kod sumber (*source code*) bagi aplikasi dan perisian yang dibangunkan adalah menjadi hak milik MTIB kecuali pakej perisian yang dikenalpasti memerlukan pengubahsuaian mengikut keperluan.	Pemilik Sistem dan Pentadbir Sistem
8.5 Kawalan Teknikal Keterdedahan (*Vulnerability*)	
Objektif : Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
8.5.1 Kawalan dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memperoleh maklumat teknikal keterdedahan yang tepat	Pentadbir Sistem ICT

pada masanya ke atas sistem maklumat yang digunakan; b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	

PERKARA 9 – PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN	
9.1 Mekanisme Pelaporan Insiden Keselamatan ICT	
Objektif: Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.	
9.1.1 Mekanisme Pelaporan	
Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan GCERT dengan kadar segera: a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Prosidur pelaporan insiden keselamatan ICT berdasarkan: a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	ICTSO

9.2 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
9.2.1 Prosidur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada MTIB. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; d) Menyediakan tindakan pemulihan segera; dan e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO

<table>
<tr><td colspan="2">PERKARA 10 – PENGURUSAN KESINAMBUNGAN PERKHIDMATAN</td></tr>
<tr><td colspan="2">10.1 Dasar Kesinambungan Perkhidmatan</td></tr>
<tr><td colspan="2">Objektif:

Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.</td></tr>
<tr><td colspan="2">10.1.1 Pelan Kesinambungan Perkhidmatan</td></tr>
<tr><td>Pelan Kesinambungan Perkhidmatan (Business Continuity Management – BCM) bagi perkhidmatan utama MTIB 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 JPICT dan perkara-perkara berikut perlu diberi perhatian:

a) Mengenal pasti semua tanggungjawab dan prosidur kecemasan atau pemulihan;
b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT;
c) Melaksanakan prosidur-prosidur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
d) Mendokumentasikan proses dan prosidur yang telah dipersetujui;
e) Mengadakan program latihan kepada pengguna mengenai prosidur kecemasan;
f) Membuat backup; dan
g) Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.

Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut:

a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;
b) Senarai personel MTIB dan pembekal berserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel</td><td>ICTSO dan Pengurus ICT</td></tr>
</table>

tidak dapat hadir untuk menangani insiden;

c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;

d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan

e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

MTIB hendaklah memastikan salinan pelan BCM sentiasa dikemaskini dan dilindungi seperti di lokasi utama.

PERKARA 11 – PEMATUHAN	
11.1 Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT MTIB	
11.1.1 Pematuhan Dasar	
Setiap pengguna di MTIB hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MTIB dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di MTIB termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan/ pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT MTIB selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber MTIB.	Semua
11.1.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
ICTSO hendaklah memastikan semua prosidur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
11.1.3 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	
11.1.4 Keperluan Perundangan	
Dasar ini bertujuan memastikan reka bentuk, operasi, penggunaan dan pengurusan sistem maklumat adalah selaras serta berkeupayaan menghalang pelanggaran mana-mana keperluan perundangan, peraturan dan perjanjian yang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut:	Semua

a) Semua perlembagaan, undang-undang, peraturan, perjanjian yang dimeterai dan lain-lain perkara yang relevan kepada keselamatan sistem maklumat dan organisasi hendaklah dikenal pasti; b) Peraturan yang sesuai dilaksanakan untuk pematuhan ke atas perlembagaan, undang-undang dan keperluan kontrak mengenai penggunaan bahan yang tertakluk kepada hak milik harta intelek; c) Rekod penting hendaklah dilindungi daripada hilang, rosak dan dipalsukan selaras dengan keperluan undang-undang, peraturan dan keperluan perjanjian MTIB; d) Perlindungan ke atas data dan hak milik peribadi hendaklah mematuhi perundangan, peraturan dan terma perjanjian jika perlu; e) Pengguna dilarang menggunakan kemudahan proses maklumat untuk tujuan yang tidak dibenarkan; dan Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MTIB: a) Arahan Keselamatan; b) Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan; c) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS); d) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan komunikasi (ICT); e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan; f) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; g) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; h) Surat Arahan Ketua Setiausaha Negara – Langkah-langkah untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-agensi Kerajaan yang bertarikh 20 Oktober 2006. i) Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Mengenai Pengurusan Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 1 Jun 2007; j) Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah	

Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 23 November 2007; k) Surat Pekeliling Am Bilangan 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di bawah Jawatankuasa IT dan Internet Kerajaan (JITIK); l) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender; m) Surat Pekeliling Perbendaharaan Bil.3/1995 – Peraturan Perolehan Perkhidmatan Perundingan; n) Akta Tandatangan Digital 1997; o) Akta Rahsia Rasmi 1972; p) Akta Jenayah Komputer 1997; q) Akta Hak Cipta (Pindaan) Tahun 1997; r) Akta Komunikasi dan Multimedia 1998; s) Perintah-perintah Am; t) Arahan Perbendaharaan; u) Arahan Teknologi Maklumat 2007; v) Pekeliling Perbendaharaan Bil.5 Tahun 2007 – Tatacara Pengurusan Aset Alih Kerajaan; w) Garis Panduan: i. Portal MyGovernment dan Laman Web/ Portal Agensi-agensi Sektor Awam; ii. Garis Panduan IT Outsourcing Agensi-agensi Sektor Awam (MAMPU, Oktober 2006); iii. Garis Panduan Biometrik.	

PERKARA 12 – KHIDMAT NASIHAT
Sebarang kemusykilan atau pertanyaan berkaitan Dasar Keselamatan ICT (DKICT) MTIB ini, sila hubungi Unit Teknologi Maklumat, Bahagian Khidmat Pengurusan. **Cik Haslila Othman : 03 – 9282 2235 ext 1279(haslila.othman@mtib.gov.my)** **Puan Nur Hayati Ahmad : 03 – 9282 2235 ext 2010 (nurhayati@mtib.gov.my)** **Puan Noraniza Abdul Ghani : 03 - 92822235 ext 1251 (noraniza@mtib.gov.my)**

DASAR KESELAMATAN ICT LEMBAGA PERINDUSTRIAN KAYU MALAYSIA

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT MTIB

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

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT MTIB; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

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

Pengesahan Pegawai Keselamatan (ICTSO) MTIB

……………………………………..

(**NORANIZA ABDUL GHANI)**
b.p. Ketua Pengarah MTIB
Tarikh : …………………..

Lampiran 2

ARAHAN KEPADA PEKHIDMAT, KONTRAKTOR DAN PIHAK KETIGA

Selaras dengan pematuhan Dasar Keselamatan ICT MTIB, tuan/ puan hendaklah mematuhi peraturan keselamatan ICT yang telah ditetapkan. Pelanggaran kepada dasar ini boleh menyebabkan perkhidmatan/ bekalan tuan/ puan dihentikan serta-merta dan dikenakan penalti sewajarnya. Perkara-perkara yang mesti dipatuhi termasuk yang berikut :

a) Mendapatkan kebenaran daripada MTIB untuk menjalankan aktiviti perkhidmatan/ bekalan dengan memaklumkan tarikh, masa dan bilangan pekerja yang terlibat. Semua pembekal bertanggungjawab memastikan pekerja adalah bebas jenayah.

b) Menyatakan dengan lengkap dan jelas skop kerja/ bekalan/ perkhidmatan yang akan dijalankan.

c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.

d) Bilik Server dan bilik/ ruang yang terdapat peralatan ICT kritikal/ kabel telekomunikasi adalah kawasan larangan ICT dan kebenaran hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. Pembekal adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi tujuan tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal dan hendaklah diiringi pegawai yang dibenarkan sepanjang masa sehingga tugas di kawasan berkenaan selesai.

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

SURAT AKUAN PEMATUHAN BAGI PEKHIDMAT, KONTRAKTOR DAN PIHAK KETIGA DASAR KESELAMATAN ICT MTIB

Nama (Huruf Besar) : ....
No. Kad Pengenalan : ....
Jawatan : ....
Syarikat : ....
Skop Kerja : ....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT MTIB; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tanda tangan : ……………………….
Tarikh : ……………………….

Pengesahan Pegawai Keselamatan (ICTSO) MTIB

……………………………………..
(NORANIZA ABDUL GHANI)
b.p. Ketua Pengarah MTIB
Tarikh : …………………..