Dasar Keselamatan ICT

Agensi PenguatkuasaanMaritim Malaysia (APMM)
Jabatan Perdana Menteri

2 Mac 2017

Versi 4.1

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
4 Julai 2007	1	JPICT BIL 1 TAHUN 2007	25 Julai 2007
4 Februari 2010	2	JPICT BIL 1 TAHUN 2010	23 April 2010
14 Mac 2011	3	JPICT BIL 2 TAHUN 2011	13 Julai 2011
12 Ogos 2013	4	JPICT 2013 (Secara Edaran)	18 Oktober 2013
19 Disember 2016	4.1	JPICT 2017 (Secara Edaran)	2 Mac 2017

JADUAL PINDAAN DASAR KESELAMATAN ICT APMM

TARIKH	VERSI	BUTIRAN PINDAAN
13 Julai 2011	3	i. Keseluruhan Polisi Keselamatan ICT APMM versi 2 dimansuhkan. Versi 3 Polisi Keselamatan ditukar kepada Dasar Keselamatan ICT APMM dengan menggunakan Dasar Keselamatan ICT MAMPU sebagai asas rujukan utama.
18 Oktober 2013	4	i. **Perkara 020201,** muka surat 28 DKICT APMM item "(f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT APMM dan *Non-Disclosure Agreement* (NDA)" sebagaimana **Lampiran 1-1** dan **Lampiran 1-2**. ii. Borang Lampiran 1-2 iaitu borang Menandatangani *Non Disclosure Agreement* (NDA) ditambah dalam DKICT APMM di muka surat 85. iii. **Perkara 050304,** muka surat 44 tambahan item "(c)" hingga "(g)". iv. **Perkara 080101**, muka surat 70 item "(d) Memastikan semua sistem yang dibangunkan secara *inhouse* dan *outsource* hendaklah diuji terlebih dahulu dengan *Stress Test, Load Test* dan *Penetration* Test bagi memastikan sistem berkenaan memenuhi keperluan keselamatan".

		v. **Tambahan Glosari**, muka surat 83 untuk *Inhouse*, *Stress Test, Load Test* dan *Penetration Test*.
19 Disember 2016	4.1	i. Keseluruhan format nombor DKICT APMM versi 4 ditukar sepenuhnya. ii. Pindaan dibuat pada Pengenalan muka surat 10 iaitu Cawangan Teknologi Maklumat dan Komunikasi (ICT) dipinda kepada Cawangan Teknologi Maklumat (CTM). iii. Bidang 0609 iaitu E-Dagang dimansuhkan. iv. Pindaan dibuat pada Pengurusan Kata Laluan iaitu panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan huruf, nombor dan simbol. v. Pendaftaran Peralatan *Bring Your Own Device* (B.Y.O.D)

ISI KANDUNGAN

1.0 PENGENALAN 9
2.0 OBJEKTIF 9
3.0 PERNYATAAN DASAR 10
4.0 SKOP 11
5.0 PRINSIP-PRINSIP 13
6.0 PENILAIAN RISIKO KESELAMATAN ICT 15
7.0 PEMBANGUNAN DAN PENYELENGGARAAN DASAR 16
7.1 Dasar Keselamatan ICT 16
7.1.1 Pelaksanaan Dasar 16
7.1.2 Penyebaran Dasar 16
7.1.3 Penyelenggaraan Dasar 16
7.1.4 Pengecualian Dasar 16
8.0 ORGANISASI KESELAMATAN 17
8.1 Infrastruktur Organisasi Dalaman 17
8.1.1 Ketua Pengarah APMM 17
8.1.2 Ketua Pegawai Maklumt / Chieft Information Officer (CIO) 17
8.1.3 Pegawai Keselamatan ICT / ICT Security Officer (ICTSO) 18
8.1.4 Wakil ICT 19
8.1.5 Pentadbir Sistem ICT 19
8.1.6 Pengguna 20
8.1.7 Jawatankuasa Keselamatan ICT APMM 20
8.1.8 Pasukan Tindak Balas Insiden Keselamatan ICT (CERT APMM) 21
8.2 Pihak Ketiga 21
8.2.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga 22
9.0 PENGURUSAN ASET 22
9.1 Akauntabiliti Aset 22
9.1.1 Inventori Aset ICT 22
9.2 Pengelasan dan Pengendalian Maklumat 23
9.2.1 Pengelasan Maklumat 23
9.2.2 Pengendalian Maklumat 23

9.2.3 Penghapusan Maklumat 24
10.0 KESELAMATAN SUMBER MANUSIA 24
10.1 Keselamatan Sumber Manusia Dalam Tugas Harian 24
10.1.1 Sebelum Perkhidmatan 25
10.1.2 Dalam Perkhidmatan 25
10.1.3 Bertukar Atau Tamat Perkhidmatan 25
11.0 KESELAMATAN FIZIKAL DAN PERSEKITARAN 26
11.1 Keselamatan Kawasan 26
11.1.1 Kawalan Kawasan 26
11.1.2 Kawalan Masuk Fizikal 27
11.1.3 Kawasan Larangan 27
11.2 Keselamatan Peralatan 27
11.2.1 Peralatan ICT 28
11.2.2 Media Storan 29
11.2.3 Media Tandatangan Digital 30
11.2.4 Media Perisian dan Aplikasi 31
11.2.5 Penyelenggaraan Perkakasan 31
11.2.6 Pengendalian Pergerakan Peralatan ICT 32
11.2.7 Pelupusan Perkakasan 32
11.3 Keselamatan Persekitaran 33
11.3.1 Kawalan Persekitaran 33
11.3.2 Bekalan Kuasa 34
11.3.3 Kabel 35
11.3.4 Prosedur Kecemasan 35
11.4 Keselamatan Dokumen 36
11.4.1 Dokumen 36
12.0 PENGURUSAN OPERASI DAN KOMUNIKASI 37
12.1 Pengurusan Prosedur Operasi 37
12.1.1 Pengendalian Prosedur 37
12.1.2 Kawalan Perubahan 37
12.1.3 Pengasingan Tugas dan Tanggungjawab 38
12.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga 38
12.2.1 Perkhidmatan Penyampaian 38
12.3 Perancangan dan Penerimaan Sistem 39

12.3.1 Perancangan Kapasiti 39
12.3.2 Penerimaan Sistem 39
12.4 Perisian Berbahaya 39
12.4.1 Perlindungan dari Perisian Berbahaya 39
12.4.2 Perlindungan dari Mobile Code 40
12.5 Housekeeping 40
12.5.1 Backup dan Restore 40
12.6 Pengurusan Rangkaian 41
12.6.1 Kawalan Infrastruktur Rangkaian 41
12.7 Pengurusan Media 42
12.7.1 Penghantaran dan Pemindahan 42
12.7.2 Prosedur Pengendalian Media 42
12.7.3 Keselamatan Sistem Dokumentasi 42
12.8 Pengurusan Pertukaran Maklumat 43
12.8.1 Pertukaran Maklumat 43
12.8.2 Pengurusan Mel Elektronik (E-mel) 43
12.9 Pemantauan 44
12.9.1 Pengauditan dan Forensik ICT 45
12.9.2 Jejak Audit 45
12.9.3 Sistem Log 46
12.9.4 Pemantauan Log 46
13.0 KAWALAN CAPAIAN 47
13.1 Dasar Kawalan Capaian 47
13.1.1 Keperluan Kawalan Capaian 47
13.2 Pengurusan Capaian Pengguna 47
13.2.1 Akaun Pengguna 47
13.2.2 Hak Capaian 48
13.2.3 Pengurusan Kata Laluan 48
13.2.4 Clear Desk dan Clear Screen 49
13.3 Kawalan Capaian Rangkaian 49
13.3.1 Capaian Rangkaian 50
13.3.2 Capaian Internet 50
13.4 Kawalan Capaian Sistem Pengoperasian 51
13.4.1 Capaian Sistem Pengoperasian 51

13.4.2 Kad Pintar/Token 52
13.5 Kawalan Capaian Aplikasi dan Maklumat....52
13.5.1 Capaian Aplikasi dan Maklumat....52
13.6 Peralatan Mudah Alih dan Kerja Jarak Jauh....53
13.6.1 Peralatan Mudah Alih 53
13.6.2 Kerja Jarak Jauh....53
14.0 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM 54
14.1 Keselamatan Dalam Membangunkan Sistem dan Aplikasi 54
14.1.1 Keperluan Keselamatan Sistem Maklumat....54
14.1.2 Pengesahan Data Input dan Output....54
14.2 Kawalan Kriptografi 55
14.2.1 Enkripsi....55
14.2.2 Tandatangan Digital 55
14.2.3 Pengurusan Infrastruktur Kunci Awam (PKI)....55
14.3 Keselamatan Fail Sistem....55
14.3.1 Kawalan Fail Sistem 55
14.4 Keselamatan Dalam Proses Pembangunan dan Sokongan 56
14.4.1 Prosedur Kawalan Perubahan 56
14.4.2 Pembangunan Perisian Secara Outsource....56
14.5 Kawalan Teknikal Keterdedahan (Vulnerability) 56
14.5.1 Kawalan Ancaman Teknikal 57
15.0 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN 57
15.1 Mekanisme Pelaporan Insiden Keselamatan ICT 57
15.1.1 Mekanisme Pelaporan....57
15.2 Pengurusan Maklumat Insiden Keselamatan ICT....58
15.2.1 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT 58
16.0 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN 59
16.1 Dasar Kesinambungan Perkhidmatan....59
16.1.1 Pelan Kesinambungan Perkhidmatan (PKP) 59
17.0 PEMATUHAN....60
17.1 Pematuhan dan Keperluan Perundangan 60
17.1.1 Pematuhan Dasar 60
17.1.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal 61
17.1.3 Pematuhan Keperluan Audit 61

17.1.4 Keperluan Perundangan 61
17.1.5 Pelanggaran Dasar 61
GLOSARI 62
Lampiran 1-1 67
Lampiran 1-2 68
Lampiran 2 69
Lampiran 3 70
Lampiran 4 71

1.0 PENGENALAN

Dasar Keselamatan ICT (DKICT) APMM mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Cawangan Teknologi Maklumat (CTM). Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT APMM.

2.0 OBJEKTIF

DKICT APMM diwujudkan untuk menjamin kesinambungan urusan APMM dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi APMM. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi. Manakala, objektif utama Keselamatan ICT APMM ialah seperti berikut:

(a) Memastikan kelancaran operasi APMM 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.

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

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi 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.

DKICT APMM 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 - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
(b) Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
(c) Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
(d) Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan
(e) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

4.0 SKOP

Aset ICT APMM terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. DKICT APMM 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, DKICT APMM 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 prosedur dalam pengendalian semua perkara-perkara berikut:

(a) Perkakasan

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

(b) Perisian

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

(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 kad akses; dan

iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

(d) Data atau Maklumat Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif APMM. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod APMM, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

(e) Manusia Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian APMM 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.

5.0 PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT APMM 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 set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

(c) Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan kata laluan;

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

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

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

(d) Pengasingan

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

(e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, router, firewall dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail;

(f) Pematuhan

DKICT APMM 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.

6.0 PENILAIAN RISIKO KESELAMATAN ICT

APMM hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan vulnerability yang semakin meningkat hari ini. Justeru itu APMM perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT. APMM 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 APMM termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. 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. APMM 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.

APMM 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.

7.0 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

7.1 Dasar Keselamatan ICT

Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan APMM dan perundangan yang berkaitan.

7.1.1 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah APMM selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT) APMM.	**Ketua Pengarah APMM**

7.1.2 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua pengguna APMM (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	**ICTSO**

7.1.3 Penyelenggaraan Dasar

DKICT APMM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan DKICT APMM: (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat JPICT, APMM; (c) Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JPICT; dan (d) Dasar ini hendaklah dikaji semula mengikut keperluan semasa.	**ICTSO**

7.1.4 Pengecualian Dasar

DKICT APMM adalah terpakai kepada semua pengguna ICT APMM dan tiada pengecualian diberikan.	**Semua**

8.0 ORGANISASI KESELAMATAN

8.1 Infrastruktur Organisasi Dalaman

Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT APMM.

8.1.1 Ketua Pengarah APMM

Ketua Pengarah APMM adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT APMM; (b) Memastikan semua pengguna mematuhi DKICT APMM; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT APMM; dan (e) Mempengerusikan Mesyuarat JPICT, APMM.	**Ketua Pengarah APMM**

8.1.2 Ketua Pegawai Maklumt / Chieft Information Officer (CIO)

CIO bagi APMM ialah Timbalan Ketua Pengarah Pengurusan (TKPP) APMM. Peranan dan tanggungjawab CIO 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 APMM serta pengurusan risiko dan pengauditan; dan (d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT APMM.	**CIO**

8.1.3 Pegawai Keselamatan ICT / ICT Security Officer (ICTSO)

ICTSO bagi APMM ialah Pengarah Cawangan Teknologi Maklumat (PCTM), APMM. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Mengurus keseluruhan program-program keselamatan ICT APMM; (b) Menguatkuasakan pelaksanaan DKICT APMM; (c) Memberi penerangan dan pendedahan berkenaan DKICT APMM kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT APMM; (e) Menjalankan pengurusan risiko; (f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan APMM berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (h) Melaporkan insiden keselamatan ICT kepada CIO, Pasukan Tindak Balas Insiden Keselamatan ICT (CERT APMM), dan memaklumkannya kepada GCERT MAMPU; (i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan (j) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT. (k) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan. (l) Ahli Pasukan Pemulihan Bencana ICT, Pengurusan Kesinambungan Perkhidmatan (Koordinator PKP) APMM. (m) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan APMM;	**ICTSO**

8.1.4 Wakil ICT

Wakil ICT adalah anggota yang dilantik di pejabat APMM. Peranan dan tanggungjawab Wakil ICT adalah seperti berikut: (a) Melaksanakan kawalan keselamatan ICT selaras dengan keperluan APMM; (b) Menentukan kawalan akses pengguna terhadap aset ICT APMM; dan (c) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT APMM.	**Wakil ICT**

8.1.5 Pentadbir Sistem ICT

Pentadbir Sistem ICT bagi APMM ialah Penolong Pengarah Kanan dan Penolong Pengarah setiap seksyen di Cawangan Teknologi Maklumat. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (a) Mengambil tindakan yang bersesuaian apabila dimaklumkan berlaku sebarang perubahan dalam bidang tugas; (b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT APMM; (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) Menjalankan kerja-kerja penyelesaian masalah ICT secara remote desktop terhadap komputer , komputer riba dan server; (f) Menganalisis dan menyimpan rekod jejak audit; (g) Menyediakan laporan mengenai aktiviti capaian; dan (h) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	**Pentadbir Sistem ICT**

8.1.6 Pengguna

Pengguna mempunyai peranan dan tanggungjawab seperti berikut: (a) Membaca, memahami dan mematuhi DKICT APMM; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat (rujuk Unit Keselamatan Ibu Pejabat); (d) Melaksanakan prinsip-prinsip DKICT APMM dan menjaga kerahsiaan maklumat APMM; (e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan (g) Menandatangani Surat Akuan Pematuhan DKICT APMM sebagaimana Lampiran 1-1.	**Pengguna**

8.1.7 Jawatankuasa Keselamatan ICT APMM

Jawatankuasa Pemandu ICT (JPICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT APMM. Keanggotaan JPICT APMM adalah seperti berikut: Pengerusi: Ketua Pengarah APMM Ahli: (1) CIO APMM (2) Semua Timbalan Ketua Pengarah (3) Semua Pengarah Cawangan / Ketua Penguatkuasa (4) ICTSO APMM Bidang kuasa: (a) Memperakukan/meluluskan dokumen DKICT APMM; (b) Memantau tahap pematuhan keselamatan ICT; (c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam APMM yang mematuhi keperluan DKICT APMM; (d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian	**JPICT APMM**

terhadap keperluan keselamatan ICT; (e) Memastikan DKICT APMM selaras dengan dasar-dasar ICT kerajaan semasa; (f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; (g) Membincang tindakan yang melibatkan pelanggaran DKICT APMM; dan (h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	

8.1.8 Pasukan Tindak Balas Insiden Keselamatan ICT (CERT APMM)

Keanggotaan CERT adalah seperti berikut: Pengurus: Ketua Seksyen Pengurusan Rangkaian dan Keselamatan CTM, APMM Ahli: (1) Pegawai Teknologi Maklumat di CTM, APMM; dan (2) Penolong Pegawai Teknologi Maklumat di CTM, APMM. Peranan dan tanggungjawab CERT adalah seperti berikut: (a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; (b) Merekod dan menjalankan siasatan awal insiden yang diterima; (c) Menangani tindak balas (response) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; (d) Menasihati APMM mengambil tindakan pemulihan dan pengukuhan; (e) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada APMM.	**CERT**

8.2 Pihak Ketiga

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

8.2.1 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, memahami dan mematuhi DKICT APMM; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; (d) Akses kepada aset ICT APMM perlu berlandaskan kepada perjanjian kontrak; (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. DKICT APMM; ii. Tapisan Keselamatan (rujuk Unit Keselamatan Ibu Pejabat) iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. (f) Menandatangani Surat Akuan Pematuhan DKICT APMM dan Non-Disclosure Agreement(NDA) sebagaimana Lampiran 1-1 dan Lampiran 1-2.	**CIO, ICTSO, Pengarah CTM, Pentadbir Sistem ICT dan Pihak Ketiga**

9.0 PENGURUSAN ASET

9.1 Akauntabiliti Aset

Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT APMM.

9.1.1 Inventori Aset ICT

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini;	**Pentadbir Sistem ICT dan Semua**

(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 APMM; (d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan (e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	

9.2 Pengelasan dan Pengendalian Maklumat

Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang ber-sesuaian.

9.2.1 Pengelasan Maklumat

Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	**Semua**

9.2.2 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai dan menukar hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan;	**Semua**

(d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

9.2.3 Penghapusan Maklumat

Aktiviti penghapusan penuh ke atas sesuatu maklumat yang disimpan dalam apa jua bentuk media storan hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) Semua maklumat dalam media storan tidak boleh dihapuskan sekiranya tidak mendapat kebenaran daripada pemiliknya; (b) Aktiviti format media storan tidak boleh dilakukan di dalam server kecuali oleh pentadbir sistem; © Server tidak boleh dijadikan media penduaan bagi menyalin maklumat dari media storan yang lain yang hendak diformatkan; dan (d) Aktiviti format dan penduaan mestilah dilakukan secara berasingan daripada unit operasi agar sistem tidak mudah terdedah kepada ancaman pencerobohan yang boleh mengakibatkan kerosakan seperti penghapusan maklumat;	**Semua**

10.0 KESELAMATAN SUMBER MANUSIA

10.1 Keselamatan Sumber Manusia Dalam Tugas Harian

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

10.1.1 Sebelum Perkhidmatan

Semua pihak terlibat di dalam pengurusan dan atau penggunaan aset ICT hendaklah bertanggungjawab dan mematuhi perkara berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan selaras dengan keperluan perkhidmatan mengikut peraturan sedia ada (rujuk Unit Keselamatan Ibu Pejabat); dan (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	**Semua**

10.1.2 Dalam Perkhidmatan

Semua pihak yang terlibat dalam pengurusan dan atau penggunaan aset ICT hendaklah bertanggungjawab dan mematuhi perkara berikut: (a) Mengurus keselamatan aset ICT yang dibenarkan mengikut peraturan yang ditetapkan; (b) Memastikan tindakan disiplin dan atau undang-undang dilaksanakan sekiranya berlaku pelanggaran peraturan yang ditetapkan; © Memastikan tanggungjawab dan peranan dalam pengurusan keselamatan ICT dinyatakan dalam senarai tugas; (d) Mengikuti latihan pengurusan keselamatan ICT berdasarkan keperluan.	**Semua**

10.1.3 Bertukar Atau Tamat Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada APMM 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.	**Semua**

11.0 KESELAMATAN FIZIKAL DAN PERSEKITARAN

11.1 Keselamatan Kawasan

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

11.1.1 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 dikenal pasti 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; (c) Memasang alat penggera atau kamera; (d) Menghadkan jalan keluar masuk; (e) Mengadakan kaunter kawalan; (f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; (g) Mewujudkan perkhidmatan kawalan keselamatan; (h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; (k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	**CIO, ICTSO dan Pegawai Keselamatan APMM**

11.1.2 Kawalan Masuk Fizikal

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Setiap pengguna APMM hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan balik kepada APMM apabila pengguna berhenti atau bersara; (c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter utama APMM. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (d) Kehilangan pas mestilah dilaporkan dengan segera.	**Semua**

11.1.3 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 APMM adalah bilik Pusat Operasi Maritim (POMAR), bilik Maritime Rescue Coordinator Center (MRCC), Pusat Data (Data Centre) dan bilik switch. (a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan (b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	**Ketua Jabatan**

11.2 Keselamatan Peralatan

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

11.2.1 Peralatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah menyemak dan memastikan semua peralatan 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 memformat dan membuat instalasi sebarang perisian tambahan terhadap komputer dan komputer riba, tanpa kebenaran Pentadbir Sistem ICT; (e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (activated) dan dikemas kini 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 mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai; (l) Peralatan ICT yang hendak dibawa keluar dari premis APMM, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan;	**Semua**

(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 Pentadbir Sistem ICT; (p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih; (q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (s) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (administrator password) yang telah ditetapkan oleh Pentadbir Sistem ICT; (t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (u) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan “OFF” apabila meninggalkan pejabat; (v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan (w) Memastikan plag dicabut daripada suis utama (main switch) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya. (x) Bagi peralatan BYOD seperti telefon pintar, tablet dan komputer riba yang digunakan untuk mencapai data rasmi APMM, langkah yang perlu diambil oleh warga APMM ialah mendaftar peralatan tersebut ke Cawangan ICT.	

11.2.2 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. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat,	**Semua**

terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; (c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; (e) Akses dan pergerakan media storan hendaklah direkodkan; (f) Perkakasan backup hendaklah diletakkan di tempat yang terkawal; (g) Mengadakan salinan atau penduaan (backup) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; (h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan (i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	

11.2.3 Media Tandatangan Digital

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan (c) Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	**Semua**

11.2.4 Media Perisian dan Aplikasi

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

11.2.5 Penyelenggaraan Perkakasan

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 perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengarah CTM.	**Pegawai Aset dan Cawangan Teknologi Maklumat, APMM**

11.2.6 Pengendalian Pergerakan Peralatan ICT

Perkakasan yang dibawa masuk/keluar dari premis APMM adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mendapat kelulusan Pegawai Aset mengikut peraturan yang telah ditetapkan (b) Memastikan peralatan ICT yang dibawa masuk/keluar tidak mengancam keselamatan ICT APMM; dan (c) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	**Semua**

11.2.7 Pelupusan Perkakasan

Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh APMM dan ditempatkan di APMM. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan APMM. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui shredding, grinding, degauzing atau pembakaran; (b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; (c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (f) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan	**Semua, Pegawai Aset dan Cawangan Teknologi Maklumat, APMM**

mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset (SPA); (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 dalaman CPU seperti RAM, hardisk, motherboard dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di APMM; iii. Memindah keluar dari APMM mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab APMM; dan v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau thumb drive sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	

11.3 Keselamatan Persekitaran

Objektif: Melindungi aset ICT APMM daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

11.3.1 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, perkara-perkara berikut hendaklah dipatuhi:	**Ketua Jabatan**

(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; (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; dan (h) Akses kepada saluran riser hendaklah sentiasa dikunci.	

11.3.2 Bekalan Kuasa

Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; (b) Peralatan sokongan seperti Uninterruptable Power Supply (UPS) 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.	**Cawangan Teknologi Maklumat, APMM dan ICTSO**

11.3.3 Kabel

Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (a) Menggunakan kabel mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan wire tapping; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	**Cawangan Teknologi Maklumat, APMM dan ICTSO**

11.3.4 Prosedur Kecemasan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan APMM; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras. (c) 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; (d) Peralatan perlindungan keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dicapai dan dikendalikan; (e) Bahan mudah terbakar DILARANG disimpan di dalam kawasan penyimpanan aset ICT; (f) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; (g) Pengguna adalah DILARANG merokok atau menggunakan peralatan memasak seperti cerek elektrik, ketuhar gelombang mikro dan lain-lain	**Semua dan Pegawai Keselamatan Jabatan**

berhampiran peralatan ICT;	

11.4 Keselamatan Dokumen

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

11.4.1 Dokumen

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (e) Menggunakan enkripsi (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	**Semua**

12.0 PENGURUSAN OPERASI DAN KOMUNIKASI

12.1 Pengurusan Prosedur Operasi

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

12.1.1 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	**Ketua Jabatan**

12.1.2 Kawalan Perubahan

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

12.1.3 Pengasingan Tugas dan Tanggungjawab

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	**ICTSO dan Wakil ICT**

12.2 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga

Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.

12.2.1 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 diaudit dari semasa ke semasa; dan (c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	**Ketua Jabatan**

12.3 Perancangan dan Penerimaan Sistem

Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

12.3.1 Perancangan Kapasiti

Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	**ICTSO dan Pentadbir Sistem ICT**

12.3.2 Penerimaan Sistem

Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	**ICTSO dan Pentadbir Sistem ICT**

12.4 Perisian Berbahaya

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

12.4.1 Perlindungan dari Perisian Berbahaya

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; (d) Mengemas kini anti virus dengan pattern antivirus yang terkini;	**Semua**

(e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (h) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	

12.4.2 Perlindungan dari Mobile Code

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

12.5 Housekeeping

Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

12.5.1 Backup dan Restore

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, backup hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Membuat backup keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat backup ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan backup bergantung pada tahap kritikal maklumat; (c) Menguji sistem backup dan prosedur restore sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (d) Menyimpan sekurang-kurangnya tiga (3) generasi backup; dan (e) Merekod dan menyimpan salinan backup di lokasi yang berlainan dan	**Semua**

selamat.	

12.6 Pengurusan Rangkaian

Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

12.6.1 Kawalan Infrastruktur Rangkaian

Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan mestilah melalui proses Final Acceptance Test (FAT) semasa pemasangan dan konfigurasi; (e) Firewall hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT; (f) Semua trafik keluar dan masuk hendaklah melalui firewall di bawah kawalan APMM; (g) Semua perisian sniffer atau network analyser adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; (h) Memasang perisian Intrusion Prevention System (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat APMM; (i) Memasang Web Content Filtering pada Internet Gateway untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan APMM adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian APMM sahaja dan penggunaan modem adalah dilarang sama sekali; dan	**ICTSO dan Pentadbir Sistem ICT**

(l) Kemudahan bagi wireless LAN perlu dipastikan kawalan keselamatan.	

12.7 Pengurusan Media

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

12.7.1 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	**Semua**

12.7.2 Prosedur Pengendalian Media

Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; dan (f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	**Semua**

12.7.3 Keselamatan Sistem Dokumentasi

Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia	**Semua**

ada.	

12.8 Pengurusan Pertukaran Maklumat

Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara APMM dan agensi luar terjamin.

12.8.1 Pertukaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara APMM dengan agensi luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari APMM; dan (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	**Semua**

12.8.2 Pengurusan Mel Elektronik (E-mel)

Penggunaan e-mel di APMM hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan” dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: (a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh APMM sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (b) Setiap e-mel rasmi yang disediakan hendaklah mematuhi format yang	**Semua**

telah ditetapkan oleh APMM melalui polisi e-mel; (c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; (d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; (e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sembilan megabytes (9MB) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; (f) Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; (g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; (h) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; (i) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; (j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; (k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; (l) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan (m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.	

12.9 Pemantauan

Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

12.9.1 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT APMM; (b) Serangan kod perosak (malicious code), halangan pemberian perkhidmatan (denial of service), spam, pemalsuan (forgery, phising), pencerobohan (intrusion), ancaman (threats) dan kehilangan fizikal (physical loss); (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (bandwidth) rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; dan	**ICTSO**

12.9.2 Jejak Audit

Setiap sistem mestilah mempunyai jejak audit (audit trail). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang	**Pentadbir Sistem ICT**

disarankan oleh Arahan Teknologi Maklumat MAMPU 2007 dan Akta Arkib Negara 2003. 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.	

12.9.3 Sistem Log

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**

12.9.4 Pemantauan Log

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; (c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; (e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan (f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam APMM atau domain keselamatan perlu diselaraskan dengan server NTP	**Cawangan Teknologi Maklumat, APMM dan Pentadbir Sistem ICT**

(contoh: mst.sirim.my).	

13.0 KAWALAN CAPAIAN

13.1 Dasar Kawalan Capaian

Objektif: Mengawal capaian ke atas maklumat.

13.1.1 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Kawalan ke atas kemudahan pemprosesan maklumat.	**ICTSO dan Ketua Jabatan**

13.2 Pengurusan Capaian Pengguna

Objektif: Mengawal capaian pengguna ke atas aset ICT APMM.

13.2.1 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 APMM sahaja boleh digunakan; (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian	**Semua**

paling minimum iaitu untuk melihat dan membaca sahaja. 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 APMM. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	

13.2.2 Hak Capaian

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

13.2.3 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh APMM seperti berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan huruf, nombor dan simbol; (d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan	**Pentadbir Sistem ICT dan Semua**

atau didedahkan dengan apa cara sekalipun; (e) Kata laluan windows dan screen saver hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; (g) Kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan;	

13.2.4 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 dan Clear Screen bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan password screen saver atau logout apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	**Semua**

13.3 Kawalan Capaian Rangkaian

Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

13.3.1 Capaian Rangkaian

Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian APMM, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	**ICTSO dan Pentadbir Sistem ICT**

13.3.2 Capaian Internet

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di APMM hendaklah dipantau secara berterusan oleh Pentadbir Sistem ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan malicious code, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian APMM; (b) Kaedah Content Filtering mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (c) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengarah 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; (f) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Cawangan 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	**ICTSO, Pentadbir Sistem ICT dan Semua**

untuk tujuan yang dibenarkan oleh APMM; (i) Sambungan ke internet selain daripada menggunakan rangkaian 1GovNet adalah tidak dibenarkan sama sekali; dan (j) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	

13.4 Kawalan Capaian Sistem Pengoperasian

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

13.4.1 Capaian Sistem Pengoperasian

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

prosedur log on yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Menghadkan dan mengawal penggunaan program; dan (d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	

13.4.2 Kad Pintar/Token

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan kad pintar/token Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; (b) Kad pintar/token hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (c) Perkongsian kad pintar/token untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar/token yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan (d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pihak yang berkenaan.	**Semua**

13.5 Kawalan Capaian Aplikasi dan Maklumat

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

13.5.1 Capaian Aplikasi dan Maklumat

Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna	**ICTSO dan Pentadbir Sistem ICT**

hendaklah direkodkan (sistem log); (c) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan (d) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah terhad kepada kakitangan anggota CTM yang dibenarkan sahaja. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	

13.6 Peralatan Mudah Alih dan Kerja Jarak Jauh

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

13.6.1 Peralatan Mudah Alih

Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	**Semua**

13.6.2 Kerja Jarak Jauh

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

14.0 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

14.1 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

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

14.1.1 Keperluan Keselamatan Sistem Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh 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) Memastikan semua sistem yang dibangunkan secara inhouse dan outsource hendaklah diuji terlebih dahulu dengan Stress Test dan Penetration Test bagi memastikan sistem berkenaan memenuhi keperluan keselamatan.	**ICTSO, Pentadbir Sistem ICT dan Pemilik Sistem**

14.1.2 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.	**Pentadbir Sistem ICT dan Pemilik Sistem**

14.2 Kawalan Kriptografi

Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

14.2.1 Enkripsi

Warga APMM hendaklah membuat enkripsi (encryption) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	**Semua**

14.2.2 Tandatangan Digital

Penggunaan tandatangan digital adalah digalakkan kepada warga APMM yang menguruskan transaksi maklumat rahsia rasmi secara elektronik mengikut keperluan pelaksanaan.	**Semua**

14.2.3 Pengurusan Infrastruktur Kunci Awam (PKI)

Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	**Semua**

14.3 Keselamatan Fail Sistem

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

14.3.1 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 prosedur 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 atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan	**Pentadbir Sistem ICT dan Pemilik Sistem**

(e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	

14.4 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

14.4.1 Prosedur 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 vendor; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (d) Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan (e) Menghalang sebarang peluang untuk membocorkan maklumat.	**Pentadbir Sistem ICT dan Pemilik Sistem**

14.4.2 Pembangunan Perisian Secara Outsource

Pembangunan perisian secara outsource perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (source code) bagi semua aplikasi dan perisian adalah menjadi hak milik kerajaan.	**Cawangan Teknologi Maklumat dan Pentadbir Sistem ICT**

14.5 Kawalan Teknikal Keterdedahan (Vulnerability)

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

14.5.1 Kawalan Ancaman Teknikal

Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	**Pentadbir Sistem ICT**

15.0 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

15.1 Mekanisme Pelaporan Insiden Keselamatan ICT

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

15.1.1 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, CERT APMM dan GCERT MAMPU dengan kadar segera: (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden	**Semua**

keselamatan ICT di APMM sepertimana Lampiran 2. Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	

15.2 Pengurusan Maklumat Insiden Keselamatan ICT

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

15.2.1 Prosedur 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 APMM. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	**ICTSO**

16.0 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

16.1 Dasar Kesinambungan Perkhidmatan

Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

16.1.1 Pelan Kesinambungan Perkhidmatan (PKP)

Pelan Kesinambungan Perkhidmatan 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 APMM. Perkara-perkara berikut perlu diberi perhatian: (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; (c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (d) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (f) Membuat backup; dan (g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. PKP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel APMM dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah	**Koordinator PKP APMM (Cawangan Khidmat Pengurusan)**

disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (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 PKP 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 PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel APMM yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. APMM hendaklah memastikan salinan PKP sentiasa dikemaskini dan dilindungi seperti di lokasi utama.	

17.0 PEMATUHAN

17.1 Pematuhan dan Keperluan Perundangan

Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada DKICT APMM.

17.1.1 Pematuhan Dasar

Setiap pengguna di APMM hendaklah membaca, memahami dan mematuhi DKICT APMM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di APMM termasuk maklumat yang disimpan didalamnya adalah hak milik Kerajaan. Ketua Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti	**Semua**

pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT APMM selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber APMM.	

17.1.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

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

17.1.3 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.	**Semua**

17.1.4 Keperluan Perundangan

Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua warga APMM adalah seperti di Lampiran 4.	**Semua**

17.1.5 Pelanggaran Dasar

Pelanggaran DKICT APMM boleh dikenakan tindakan tatatertib.	**Semua**

GLOSARI

Anti Spam

Perkakasan bagi memeriksa dan menyekat sebarang aktiviti emel sampah.

Antivirus

Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, optical disk, flash disk, CDROM, thumb drive untuk sebarang kemungkinan adanya virus.

Aset ICT

Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.

Backup

Proses penduaan sesuatu dokumen atau maklumat.

Bandwidth

Jalur Lebar - Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.

BYOD

Bring your own device (BYOD). Merujuk kepada peranti milik persendirian (komputer riba, tablet dan telefon pintar) yang dibawa oleh warga agensi ke pejabat atau tempat kerja dan menggunakan peranti ini untuk mencapai data, maklumat dan aplikasi APMM.

CERT

Computer Emergency Response Team atau Pasukan Tindak Balas Insiden Keselamatan ICT Agensi. Pasukan yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di APMM.

CIO

Chief Information Officer

Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.

CTM

Cawangan Teknologi Maklumat, APMM.

Denial of service

Halangan pemberian perkhidmatan.

Downloading

Aktiviti muat-turun sesuatu perisian.

Encryption

Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.

Firewall

Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.

Forgery

Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft/espionage), penipuan (hoaxes).

GCERT

Government Computer Emergency Response Team atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.

Hard disk

Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.

Hub

Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.

ICT

Information and Communication Technology/Teknologi Maklumat dan Komunikasi.

ICTSO

ICT Security Officer

Pegawai yang bertanggungjawab terhadap keselamatan ICT.

Inhouse

Perkhidmatan yang dilaksanakan secara dalaman agensi menggunakan sumber manusia yang sedia ada.

Internet

Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.

Internet Gateway

Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.

Intrusion Detection System (IDS)

Sistem Pengesan Pencerobohan

Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.

Intrusion Prevention System (IPS)

Sistem Pencegah Pencerobohan

Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code.

Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan LAN.

Ketua Jabatan

Seseorang pegawai yang mengetuai sesuatu jabatan atau Ketua Perkhidmatan, mengikut mana-mana yang berkenaan, atau mana-mana pegawai yang diberi kuasa melaksanakan tugas Ketua Jabatan atau Ketua Perkhidmatan.

Local Area Network

Rangkaian Kawasan Setempat yang menghubungkan komputer.

Load Test

Ujian capaian sistem aplikasi online bagi menguji tahap ketahanan ke sistem daripada capaian yang banyak.

Logout

Log-out computer

Keluar daripada sesuatu sistem atau aplikasi komputer.

Malicious Code

Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.

Mobile Code

Mobile code ditafsirkan sebagai kod perisian yang dipindahkan dari computer kepada komputer lain dan melaksanakan secara automatik fungsi-fungsi tertentu dengan sedikit atau tanpa interaksi daripada pengguna.

MODEM

MOdulator DEModulator

Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.

Outsource

Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.

Pemilik Sistem

Cawangan yang bertanggungjawab terhadap sistem.

Penetration Test

Kaedah menilai tahap keselamatan sistem komputer atau rangkaian dengan melakukan simulasi serangan daripada dalaman dan luaran.

Perisian Aplikasi

Ia merujuk pada perisian atau pakej yang selalu digunakan seperti spreadsheet dan word processing ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.

Public-Key Infrastructure (PKI)

Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.

Pusat Data (Data Center)

Pusat data juga meliputi bilik-bilik server di pejabat cawangan APMM.

Router

Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.

Screen Saver

Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.

Server

Pelayan komputer

Stress Test

Ujian ke atas sistem, aplikasi dan perkakasan yang memberi penekanan kepada prestasi, ketersediaan dan kawalan ralat semasa beban puncak.

Switches

Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense Multiple Access/Collision Detection (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.

Threat

Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.

Uninterruptible Power Supply (UPS)

Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.

Video Conference

Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.

Video Streaming

Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.

Virus

Atur cara yang bertujuan merosakkan data atau sistem aplikasi.

Wireless LAN

Jaringan komputer yang terhubung tanpa melalui kabel.

Wakil ICT

Anggota APMM yang bertanggungjawab terhadap keselamatan ICT.

Lampiran 1-1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT APMM

Nama (Huruf Besar): …….....……
No. Kad Pengenalan: …….....……
Jawatan: …….....……
Cawangan: …….....……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-
1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT APMM; 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 ICT

.....
(Nama Pegawai Keselamatan ICT)
b.p. Ketua Pengarah APMM

Tarikh: .....

Lampiran 1-2

NON DISCLOSURE AGREEMENT (NDA)

Saya…… No. Kad Pengenalan…….....……. berjawatan…..…… dari organisasi…… dengan ini :

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

dan

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

….....

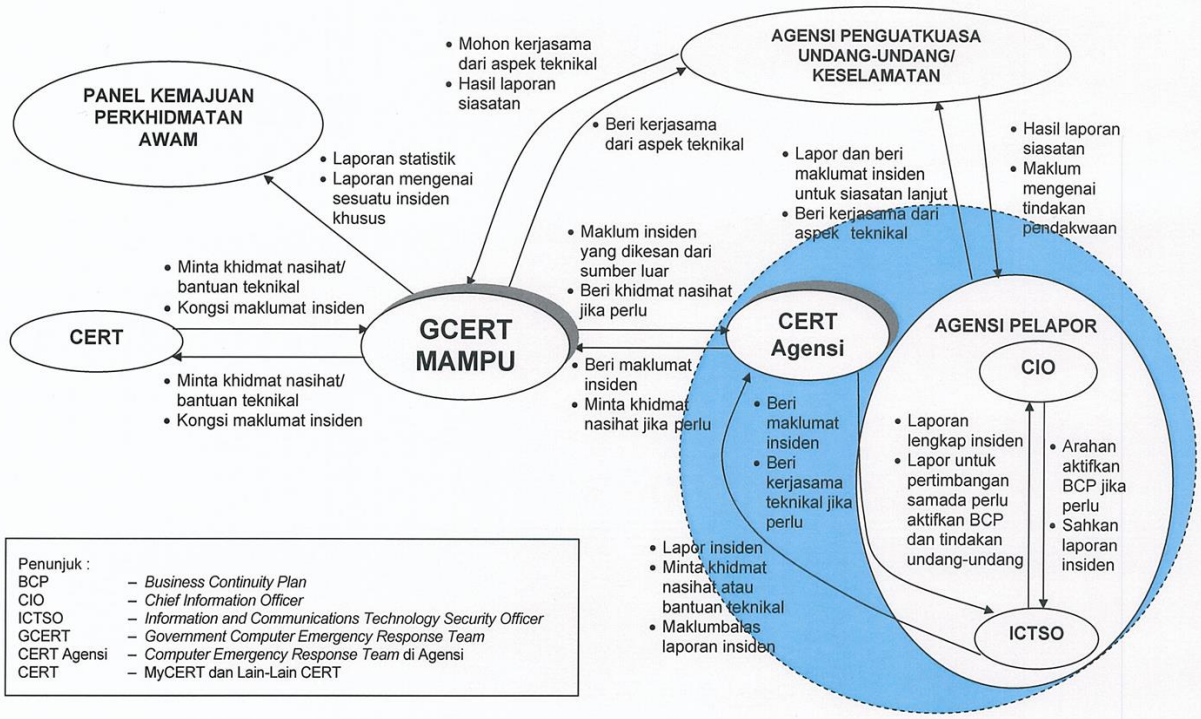
Sekian, terima kasih.

.....	.....
(Tandatangan)	(Tandatangan Saksi)
.....	.....
(Nama)	(Nama Saksi)
Tarikh:.....	.....
	(No. Kad Pengenalan Saksi)
	Tarikh:.....

Nota : Sila isi dengan pen dakwat hitam

Lampiran 2

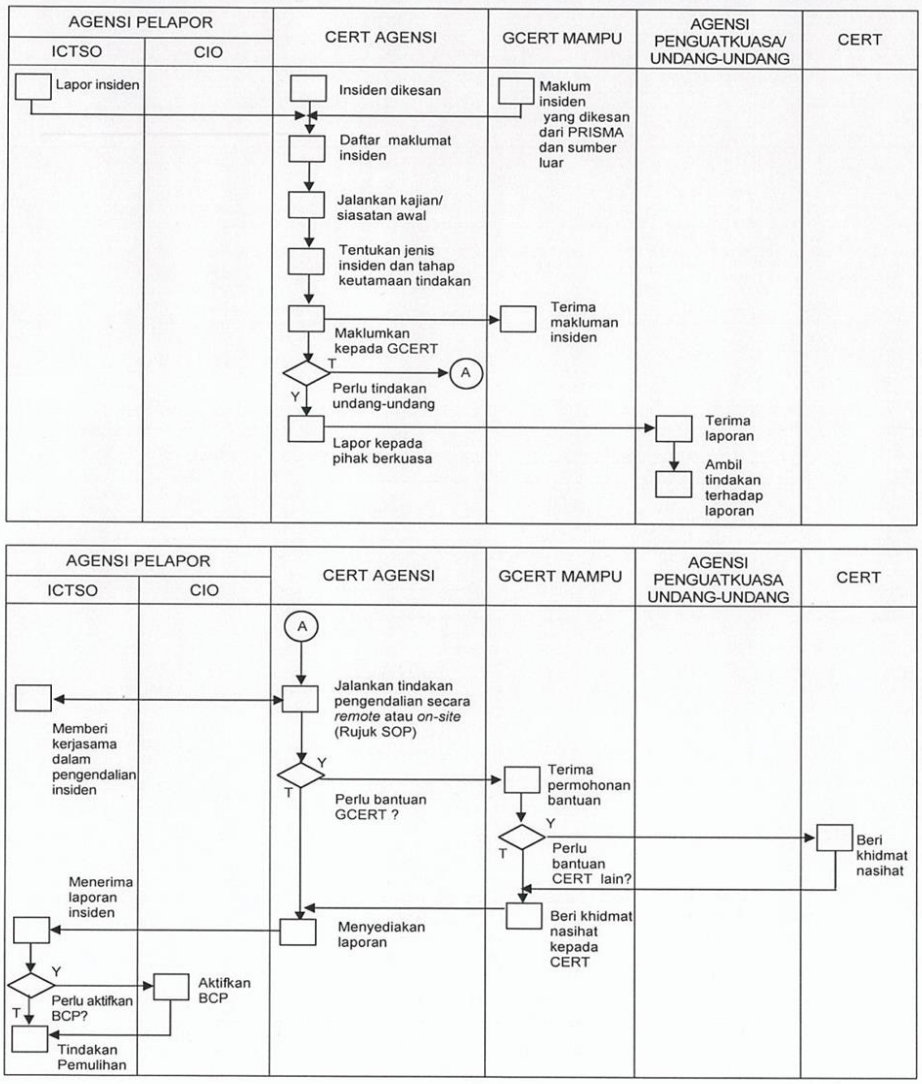
Rajah 2 : Hubungan Entiti Dalam Proses Kerja Pengurusan Pelaporan Insiden Keselamatan ICT



Lampiran 3

Penunjuk : SOP - Standard Operating Procedure

Rajah 3 : Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT Agensi



PENUTUP

17. Garis panduan ini disediakan untuk membantu *Computer Emergency Response Team* (CERT) Agensi memperkemaskan pengurusan pengendalian insiden keselamatan ICT sektor awam bagi memperkasakan agensi sektor awam menguruskan sendiri pengendalian insiden keselamatan ICT di agensi masing-masing serta meningkatkan kecekapan pengendalian insiden keselamatan ICT di agensi sektor awam.

6

Lampiran 4

SENARAI PERUNDANGAN DAN PERATURAN

[01] Arahan Keselamatan (Semakan dan Pindaan 2015).

[02] Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;

[03] Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;

[04] Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

[05] Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;

[06] Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;

[07] Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

[08] 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;

[09] Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;

[10] Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

[11] Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

[12] Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

[13] Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;

[14] Akta 562 - Akta Tandatangan Digital 1997.

[15] Akta 88 - Akta Rahsia Rasmi 1972.

[16] Akta 563 - Akta Jenayah Komputer 1997.

[17] Akta Hak Cipta (Pindaan) Tahun 1997;

[18] Akta Komunikasi dan Multimedia 1998;

[19] Akta 629 - Akta Arkib Negara 2003.

[20] Akta 680 - Aktiviti Kerajaan Elektronik 2007.
[21] Akta 709 - Akta Perlindungan Data Peribadi 2010.
[22] Arahan Perbendaharaan;
[23] Arahan Teknologi Maklumat, MAMPU, 2007.
[24] Arahan 20 – Dasar dan Mekanisme Pengurusan Bencana Negara.
[25] Arahan 24 - Dasar Dan Mekanisme Pengurusan Krisis Siber Negara.
[26] National Cyber Security Policy (NCSP)
[27] Surat Pekeliling Perbendaharaan - Garis Panduan Mengenai Pengurusan Perolehan Information Telecommunication Technology ICT Kerajaan SPP 3/2013.
[28] Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam.
[29] Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam, 22 Januari 2010.
[30] Surat Arahan Ketua Pengarah MAMPU, Garis Panduan Pelaksanaan Pengurusan Sistem Keselamatan Maklumat 24 Nov 2010.
[31] Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara.
[32] Memorandum Jemaah Menteri Pelaksanaan Pensijilan MS ISO/IEC 27001:2007
[33] Garis Panduan Perolehan ICT Kerajaan Kementerian Kewangan Malaysia. Cabutan Pekeliling Perbendaharaan Malaysia PK 2.2/2013.
[34] Garis Panduan Pengurusan Rekod Elektronik oleh Jabatan Arkib Negara.
[35] Garis Panduan Audit Pengurusan Sistem Keselamatan Maklumat Sektor Awam 24 Nov 2010.
[36] Garis Panduan Audit ICT Sektor Awam
[37] Surat Arahan Ketua Pengarah MAMPU Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam 25 Januari 2015.
[38] Akta 298 - Kawasan Larangan Tempat Larangan 1959.
[39] Garis Panduan Kontrak ICT Bagi Perolehan Perkhidmatan Pembangunan Sistem Aplikasi.
[40] Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA), April 2016, Versi 1.