



DASAR KESELAMATAN ICT

MAJLIS AGAMA ISLAM

DAN ADAT MELAYU PERAK

TARIKH KUATKUASA :

20 NOV 2015

VERSI 1.0

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	1/55

KANDUNGAN

Muka Surat

PENDAHULUAN		6
Bab 1	PENGENALAN	8
	Am	
	Definisi Dasar	8
	Objektif Dasar	8
	Skop Dasar	8
Bab 2	PRINSIP-PRINSIP	9
	Prinsip-Prinsip Asas	9
	Akses atau Dasar Perlu Mengetahui	9
	Hak Akses Minimum	9
	Akauntabiliti	9
	Pengasingan	10
	Pengauditan	10
	Pematuhan	10
	Pemulihan	10
Saling Bergantungan	11	
Bab 3	PENGURUSAN DAN TANGGUNGJAWAB DASAR	12
	KESELAMATAN ICT	
	Pelaksanaan Dasar	12
	Pelaksanaan Dasar dan Ahli Jawatankuasa Keselamatan ICT	12
	Penyebaran Dasar	12
	Dasar Perlu Disebarkan	12
	Penyelenggaraan Dasar	12
	Semakan dan Pindaan Dasar	12
	Pengecualian Dasar	13
	Tiada Siapa Dikecualikan	13

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	2/55

Bab 4	ORGANISASI DAN INFRASTRUKTUR KESELAMATAN ICT	14
	Infrastruktur Keselamatan Organisasi	14
	Tanggungjawab Ketua Pegawai Maklumat (CIO)	14
	Tanggungjawab Ketua Unit (UTM)	14
	Tanggungjawab ICTSO	15
	Tanggungjawab Pentadbir Sistem	16
	Tanggungjawab Pegawai Pengkelasan Dokumen	17
	Tanggungjawab Pengguna	17
Bab 5	KAWALAN DAN PENGELASAN ASET	19
	Akauntabiliti Aset	19
	Inventori Aset	19
	Pemilikan Aset	19
	Pengelasan Maklumat	19
	Pengendalian Maklumat	20
Bab 6	KESELAMATAN SUMBER MANUSIA	21
	Keselamatan ICT Dalam Tugas Harian	21
	Tanggungjawab Keselamatan	21
	Terma dan Syarat Perkhidmatan	21
	Perakuan Akta Rahsia Rasmi	21
	Menangani Insiden Keselamatan ICT	21
	Pelaporan Insiden	21
	Pendidikan	22
	Program Kesedaran Keselamatan ICT	22
Pelanggaran Dasar	22	
Bab 7	KESELAMATAN FIZIKAL	23
	Keselamatan Kawasan	23
	Perimeter Keselamatan Fizikal	23
	Kawalan Masuk Fizikal	23
	Kawalan Larangan	24
	Perkakasan	24
	Dokumen	25
	Media Storan	26

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	3/55

	Kabel	26
	Penyelenggaraan	27
	Peminjaman Perkakasan Untuk Kegunaan di Luar Pejabat	27
	Peralatan Di Luar Premis	27
	Pelupusan	28
	Clear Desk dan Clear Screen	28
	Keselamatan Persekitaran	29
	Kawalan Persekitaran	29
	Bekalan Kuasa	29
	Prosedur Kecemasan	29
Bab 8	PENGURUSAN KOMUNIKASI DAN OPERASI	31
	Pengurusan Prosedur Operasi	31
	Pengendalian Prosedur	31
	Kawalan Perubahan	31
	Kawalan Prosedur	32
	Perancangan dan Penerimaan Sistem	32
	Perancangan Kapasiti	32
	Penerimaan Sistem	33
	Perisian Berbahaya	33
	Perlindungan dan Perisian Berbahaya	33
	Housekeeping	34
	Penduaan	34
	Sistem Log	34
	Pengurusan Rangkaian	35
	Kawalan Infrastruktur Rangkaian	35
	Rangkaian Tanpa Wayar	37
	Pengurusan Media	38
	Penghantaran dan Pemindahan	38
	Prosedur Pengendalian Media	38
	Keselamatan Sistem Dokumentasi	39
	Keselamatan Komunikasi	39
	Internet	39
	Mel Elektronik (Emel)	40

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	4/55

Bab 9	KAWALAN CAPAIAN	42
	Dasar Kawalan Capaian	42
	Keperluan Dasar	42
	Akaun Pengguna	42
	Jejak Audit	43
	Sistem Maklumat dan Aplikasi	43
	Peralatan Komputer Mudah Alih	44
	Penggunaan Peralatan Komputer Mudah Alih	44
Bab 10	PEMBANGUNAN DAN PENYELENGGARAN SISTEM	45
	Keselamatan Dalam Membangunkan Sistem Aplikasi	45
	Keperluan Dasar	45
	Kriptografi	45
	Penyulitan	45
	Tandatangan Digital	45
	Pengurusan Kunci (Key)	46
	Sistem Fail	46
	Kawalan Sistem Fail	46
	Pembangunan dan Proses Sokongan	46
	Kawalan Perubahan	46
Bab 11	KESINAMBUNGAN PERKHIDMATAN	47
	Dasar Kesinambungan Perkhidmatan	47
	Pelan Kesinambungan Keselamatan	47
Bab 12	PEMATUHAN DASAR	49
	Pematuhan dan Keperluan Perundangan	49
	Pematuhan Dasar	49
	Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	49
	Pematuhan Keperluan Audit	49
	Keperluan Perundangan	50
	Pelanggaran Dasar	51
GLOSARI		52
LAMPIRAN		55

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	5/55

PENDAHULUAN

Dasar Keselamatan ICT MAIPk adalah bagi menjamin segala urusan menyedia dan membekalkan perkhidmatan berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

Empat (4) komponen asas keselamatan ICT iaitu :-

- i. melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
- ii. menjamin setiap maklumat adalah tepat dan sempurna;
- iii. memastikan ketersediaan maklumat apabila diperlukan oleh pengguna;
- iv. memastikan akses kepada hanya pengguna-pengguna yang sah atau penerima maklumat.

Dasar Keselamatan ICT MAIPk ini juga bertujuan untuk menjamin keselamatan sumber maklumat dan kebolehsediaan kepada semua pengguna yang dibenarkan. Semua pengguna teknologi maklumat yang sah di MAIPk dibenarkan membuat capaian ke atas sistem yang bersesuaian. Capaian dikawal dan dipantau selaras dengan Dasar Keselamatan ICT MAIPk. Ciri-ciri utama keselamatan Sumber Maklumat Elektronik adalah seperti berikut:-

- **Kerahsiaan**

Sumber Maklumat Elektronik tidak boleh didedahkan sewenang-wenangnya atau dibiarkan dicapai tanpa kebenaran pihak berkuasa.

- **Integriti**

Data dan maklumat hendaklah tepat, lengkap dan dikemaskini. Ia hanya boleh diwujudkan, diubah atau dihapus oleh orang yang diberi kuasa yang sah sahaja dan mengikut prosedur yang dibenarkan.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	6/55

Dasar Keselamatan ICT MAIPk

- **Tidak Boleh Disangkal**

Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal.

- **Kesahihan**

Data dan maklumat hendaklah dijamin kesahihannya.

- **Kebolehsediaan**

Memastikan pengguna-pengguna yang sah boleh mencapai sumber maklumat. Menjalankan urusan pentadbiran awam bergantung kepada kebolehsediaan maklumat dan proses pengurusan.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	7/55

PENGENALAN

1.1 AM

1.1.1 Definisi Dasar

Dasar Keselamatan ICT MAIPk ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset ICT MAIPk. Dasar ini juga menerangkan kepada semua pengguna di MAIPk mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT MAIPk.

1.1.2 Objektif Dasar

Dasar Keselamatan ICT MAIPk diwujudkan untuk menjamin kesinambungan urusan MAIPk dengan meminimumkan kesan insiden keselamatan ICT. Dasar ini juga adalah bagi menjamin keselamatan maklumat terperingkat dan maklumat rasmi kerajaan dari dicapai tanpa kuasa yang sah.

1.1.3 Skop Dasar

Dasar ini meliputi semua sumber atau aset ICT yang digunakan seperti maklumat (contoh : fail, dokumen, data elektronik), perisian (contoh : aplikasi dan sistem perisian) dan fizikal (contoh : komputer, peralatan komunikasi dan media storan). Dasar ini adalah terpakai oleh semua pengguna di MAIPk termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyediakan, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT MAIPk.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	8/55

PRINSIP-PRINSIP

2.1 Prinsip-Prinsip Asas

2.1.1 Akses atau Dasar Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atau 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.

2.1.2 Hak Akses Minimum

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

2.1.3 Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT MAIPk. Tanggungjawab ini perlu dinyatakan dalam jelas sesuai 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.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	9/55

DASAR KESELAMATAN ICT MAIPk

2.1.4 Pengasingan

Tugas mewujudkan, memadam, kemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian yang bertujuan untuk mengasingkan akses kepada domain kedua-dua kumpulan tersebut seperti akses kepada fail data, fail pengguna, kemudahan sistem dan komunikasi, manakala pemisahan antara domain pula adalah untuk mengawal dan mengurus perubahan pada konfigurasi dan keperluan sistem.

2.1.5 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*.

2.1.6 Pematuhan

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

2.1.7 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

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	10/55

DASAR KESELAMATAN ICT MAIPk

aktiviti penduaan dan mewujudkan Pelan Pemulihan Bencana/Kesinambungan Perkhidmatan.

2.1.8. 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.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	11/55

PENGURUSAN DAN TANGGUNGJAWAB DASAR KESELAMATAN ICT

3.1 Pelaksanaan Dasar

3.1.1 Pelaksanaan Dasar dan Ahli Jawatankuasa Keselamatan ICT

Pelaksanaan Dasar ini akan dijalankan dan dipengerusikan oleh Timbalan Ketua Pegawai Eksekutif (Pentadbiran) merangkap CIO dibantu oleh Jawatankuasa Keselamatan ICT yang terdiri daripada pegawai-pegawai berikut:

- i) Ketua Penolong Setiausaha
- ii) Penolong Setiausaha (Bahagian Khidmat Pengurusan)
- iii) Ketua Audit Dalam
- iv) Pegawai Keselamatan ICT (ICTSO)
- v) Pentadbir Sistem / Rangkaian.
- vi) Pentadbir Web

3.2 Penyebaran Dasar

3.2.1 Dasar Perlu Disebarkan.

Dasar ini perlu disebarikan kepada semua pengguna MAIPk (termasuk kakitangan, pembekal, pakar runding dll.)

3.3 Penyelenggaraan Dasar

3.3.1 Semakan dan Pindaan Dasar

Dasar Keselamatan ICT MAIPk adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT MAIPk:

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	12/55

DASAR KESELAMATAN ICT MAIPk

- i) kenalpasti dan tentukan perubahan yang diperlukan:
 - Berdasarkan situasi ancaman.
 - Berdasarkan situasi pencerobohan.
 - Berdasarkan laporan maklumat insiden keselamatan.
 - Berdasarkan cadangan yang diberi oleh pihak pengurusan.
- ii) kemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Teknikal ICT MAIPk;
- iii) perubahan yang telah dipersetujui oleh JTICT dimaklumkan kepada semua pengguna; dan
- iv) dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun;

3.4 Pengecualian Dasar

3.4.1. Tiada Siapa Dikecualikan.

Dasar Keselamatan ICT MAIPk adalah terpakai kepada semua pengguna ICT MAIPk dan tiada pengecualian diberikan.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	13/55

ORGANISASI KESELAMATAN ICT

4.1 Infrastruktur Keselamatan Organisasi

4.1.1 Tanggungjawab Ketua Pegawai Maklumat (CIO)

Timbalan Ketua Pegawai Eksekutif (Pentadbiran) adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab CIO adalah seperti berikut:

- i. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MAIPk.
- ii. memastikan semua pengguna mematuhi Dasar Keselamatan ICT MAIPk. Tindakan sewajarnya hendaklah diambil apabila berlaku sebarang pelanggaran keselamatan;
- iii. memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi;
- iv. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT MAIPk; dan
- v. memastikan Pelan Rancangan Pematuhan yang bertujuan untuk mengurus risiko yang timbul akibat daripada ketidakpatuhan Dasar Keselamatan ICT MAIPk.

4.1.2 Tanggungjawab Ketua Unit (UTM)

Peranan dan tanggungjawab Ketua Unit (UTM) MAIPk adalah seperti berikut:

- i. membantu CIO/TKPE MAIPk (Pentadbiran) dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	14/55

DASAR KESELAMATAN ICT MAIPk

- ii. menentukan keperluan keselamatan ICT; dan
- iii. membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.

4.1.3 Tanggungjawab ICTSO

Timbalan Ketua Pegawai Eksekutif (Pembangunan) adalah merupakan Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut:

- i. mengurus keseluruhan program-program keselamatan ICT MAIPk;
- ii. menguatkuasakan Dasar Keselamatan ICT MAIPk;
- iii. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MAIPk, kepada semua pengguna;
- iv. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MAIPk;
- v. menjalankan pengurusan risiko;
- vi. menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya;
- vii. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian;
- viii. melaporkan insiden keselamatan ICT kepada pasukan Tindak Balas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumpkannya kepada CIO;
- ix. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	15/55

DASAR KESELAMATAN ICT MAIPk

- x. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT MAIPk; dan
- xi. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.

4.1.4 Tanggungjawab Pentadbir Sistem

Pegawai Teknologi Maklumat (Rangkaian) atau mana-mana pegawai yang dilantik oleh jabatan untuk mentadbir sesuatu sistem ICT di MAIPk adalah merupakan Pentadbir Sistem ICT MAIPk. Peranan dan tanggungjawab adalah seperti berikut:

- i. mengambil tindakan yang bersesuaian dengan segera ke atas aset ICT apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas;
- ii. menentukan ketetapan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT MAIPk;
- iii. memantau aktiviti capaian harian pengguna;
- iv. mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikanannya dengan serta-merta;
- v. menyimpan dan menganalisis rekod jejak audit; dan
- vi. menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	16/55

DASAR KESELAMATAN ICT MAIPk

4.1.5 Tanggungjawab Pegawai Pengkelasan Dokumen

Pegawai Pengkelasan Dokumen MAIPk ialah pegawai yang dilantik oleh Menteri Besar di bawah Akta Rahsia Rasmi 1972, perakuan di bawah Seksyen 2B yang dipertanggungjawab untuk mengelaskan apa-apa surat rasmi atau bahan sebagai “Rahsia Besar”, Rahsia, Sulit atau Terhad”.

4.1.6 Tanggungjawab Pengguna

Pengguna ialah semua kakitangan MAIPk, peserta kursus dan pihak kontraktor yang menjalankan kerja-kerja di MAIPk. Peranan dan tanggungjawab pengguna adalah seperti berikut:

- i. membaca, memahami dan mematuhi Dasar Keselamatan ICT MAIPk;
- ii. mengetahui dan memahami implikasi keselamatan ICT, kesan dari tindakannya;
- iii. lulus tapisan keselamatan;
- iv. melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat MAIPk;
- v. melaksanakan langkah-langkah perlindungan seperti:
 - Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
 - Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
 - Menentukan maklumat sedia untuk digunakan;
 - Menjaga kerahsiaan kata laluan;
 - Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	17/55

DASAR KESELAMATAN ICT MAIPk

- Memberi perhatian kepada maklumat terperingkat terutamanya semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
 - Menjaga kerahsiaan langkah-langkah Keselamatan ICT dari diketahui umum.
- vi. melaporkan sebarang aktiviti yang mengancam keselamatan ICT dengan segera;
- vii. menghadiri program-program kesedaran mengenai keselamatan ICT; dan
- viii. menandatangani surat akuan pematuhan Dasar Keselamatan ICT MAIPk.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	18/55

KAWALAN DAN PENGELASAN ASET

5.1 Akauntabiliti Aset

5.1.1 Inventori Aset

Semua aset ICT MAIPk hendaklah direkodkan. Ini termasuklah mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 Tatacara Pengurusan Aset Alih Kerajaan dan Arahan Keselamatan hendaklah dipatuhi.

5.1.2 Pemilikan Aset

Setiap pengguna adalah bertanggungjawab ke atas semua aset di bawah kawalannya. Semua pengguna aset ICT MAIPk hendaklah mematuhi peraturan-peraturan penggunaan maklumat dan aset ICT yang telah ditetapkan oleh pihak pengurusan.

5.1.3 Pengelasan Maklumat

Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam Arahan Keselamatan seperti berikut:

- i. Rahsia Besar;
- ii. Rahsia;
- iii. Sulit; dan
- iv. Terhad.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	19/55

5.1.4 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:-

- i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
- iii. menentukan maklumat sedia untuk digunakan;
- iv. menjaga kerahsiaan kata laluan;
- v. mematuhi standard, 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.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	20/55

KESELAMATAN SUMBER MANUSIA

6.1 Keselamatan ICT Dalam Tugas Harian

6.1.1 Tanggungjawab Keselamatan

Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.

6.1.2 Terma dan Syarat Perkhidmatan

Semua warga MAIPk yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa.

6.1.3 Perakuan Akta Rahsia Rasmi

Warga MAIPk yang menguruskan maklumat terperingkat hendaklah mematuhi semua peraturan Arahan Keselamatan dan Akta Rahsia Rasmi 1972.

6.2 Menangani Insiden Keselamatan ICT

6.2.1 Pelaporan Insiden

Insiden keselamatan ICT seperti berikut hendaklah dilaporkan dengan kadar segera:

- i. maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;
- ii. sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	21/55

DASAR KESELAMATAN ICT MAIPk

- iii. kata laluan atau mekanisme kawalan akses hilang, dicuri, didedahkan atau disyaki hilang;
- iv. berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar;
- v. berlaku percubaan mencerooh, penyelewengan dan insiden-insiden yang tidak diingini.

Nota 2:

Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “ Mekanisme Pelaporan Insiden Keselamatan ICT” mengenainya bolehlah dirujuk.

6.3 Pendidikan

6.3.1 Program Kesedaran Keselamatan ICT

Setiap pengguna di MAIPk perlu diberikan program kesedaran, latihan dan kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT MAIPk.

6.3.2 Pelanggaran Dasar

Pelanggaran Dasar Keselamatan ICT MAIPk akan dikenakan tindakan tatatertib.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	22/55

KESELAMATAN FIZIKAL

7.1 Keselamatan Kawasan

7.1.1 Perimeter Keselamatan Fizikal

Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut:

- i. kawalan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko;
- ii. memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan;
- iii. memperkukuhkan dinding dan siling;
- iv. menghadkan jalan keluar masuk;
- v. mengadakan kaunter kawalan;
- vi. menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan
- vii. mewujudkan perkhidmatan kawalan keselamatan.

7.1.2 Kawalan Masuk Fizikal

- i) Setiap pengguna MAIPk hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas;
- ii) Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di pintu masuk utama dan hendaklah dikembalikan semula selepas tamat lawatan;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	23/55

DASAR KESELAMATAN ICT MAIPk

- iii) Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti, bertukar atau bersara;
- iv) Setiap pelawat hendaklah mendaftar di pintu masuk utama MAIPk;
- v) Kehilangan pas keselamatan mestilah dilaporkan dengan segera;
- vi) Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT MAIPk.

7.1.3 Kawasan Larangan

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di MAIPk adalah bilik Ketua Pegawai Eksekutif, bilik-bilik ketua Bahagian, bilik kebal dan bilik server. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja.

Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.

7.1.4 Perkakasan

Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu:

- i. setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna;
- ii. semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	24/55

DASAR KESELAMATAN ICT MAIPk

- iii. setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan
- iv. sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada pegawai atasan.

7.1.5 Dokumen

Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:

- i. memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin;
- ii. menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen;
- iii. menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik. Penyulitan (*encryption*) bermaksud proses untuk mengubah data ke dalam bentuk yang tidak dapat dibaca tanpa melakukan proses deskripsi (*decrypting*), iaitu mengubah kembali ke bentuk aslinya terlebih dahulu; dan
- iv. pada dasarnya, enkripsi (*encryption*) adalah proses untuk mengubah pesanan atau data ke dalam bentuk yang tidak dapat dibaca tanpa melakukan proses dekripsi (*decrypting*), iaitu mengubah kembali ke bentuk aslinya terlebih dahulu.
- v. memastikan dokumen yang mengandungi bahan atau maklumat sulit diambil segera dari pencetak.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	25/55

DASAR KESELAMATAN ICT MAIPk

7.1.6 Media Storan

Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat:

- i. penyediaan ruang untuk penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;
- ii. akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja;
- iii. penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan
- iv. pergerakan media storan hendaklah direkodkan.

7.1.7 Kabel

Kabel komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:

- i. menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan;
- ii. melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; dan
- iii. melindungi laluan pemasangan kabel sepenuhnya.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	26/55

DASAR KESELAMATAN ICT MAIPk

7.1.8 Penyelenggaraan

Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti.

- i. semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang telah ditetapkan;
- ii. perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; dan
- iii. semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan.

7.1.9 Peminjaman Perkakasan Untuk Kegunaan di Luar Pejabat

Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjami keselamatan perkakasan:

- i. peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan
- ii. aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan dan mengikut prosedur yang ditetapkan oleh Unit Teknologi Maklumat (UTM).

7.1.10 Peralatan Di Luar Premis

Bagi perkakasan yang dibawa keluar dari premis MAIPk, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawasan MAIPk:

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	27/55

DASAR KESELAMATAN ICT MAIPk

- i. peralatan perlu dilindungi dan dikawal sepanjang masa; dan
- ii. penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.

7.1.11 Pelupusan

Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MAIPk:

- i. semua kandungan peralatan ICT termasuk maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum dilupuskan.
- ii. sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan
- iii. maklumat lanjut pelupusan bolehlah merujuk kepada Surat Pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk “Garis Panduan Pelupusan Peralatan Komputer” dan Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk “Tatacara Pengurusan Aset Alih Kerajaan”.

7.1.12 Clear Desk dan Clear Screen

Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian dan kehilangan. Clear Desk bermaksud tidak meninggalkan bahan-bahan yang rahsia terdedah sama ada atas meja atau di paparan skrin:

- i. gunakan kemudahan password screen saver atau log keluar apabila meninggalkan komputer;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	28/55

DASAR KESELAMATAN ICT MAIPk

- ii. bahan-bahan rahsia hendaklah disimpan dalam laci atau kabinet fail yang berkunci.

7.2 Keselamatan Persekitaran

7.2.1 Kawalan Persekitaran

Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai atau pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil:

- i. merancang dan menyediakan pelan keseluruhan susun atur data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti;
- ii. 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;
- iii. peralatan perlindungan keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;
- iv. bahan mudah terbakar mestilah disimpan di luar kawasan kemudahan penyimpanan aset ICT;
- v. semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT;
- vi. pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	29/55

DASAR KESELAMATAN ICT MAIPk

- vii. semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.

7.2.2 Bekalan Kuasa

Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT. Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.

7.2.3 Prosedur Kecemasan

Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	30/55

PENGURUSAN KOMUNIKASI DAN OPERASI

8.1 Pengurusan Prosedur Operasi

8.1.1 Pengendalian Prosedur

Semua prosedur keselamatan ICT yang diwujudkan, dikenalpasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal. 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. Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.

8.1.2 Kawalan Perubahan

Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu.

Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan.

Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau tidak sengaja.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	31/55

DASAR KESELAMATAN ICT MAIPk

8.1.3 Kawalan Prosedur

Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan. Prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut:

- i. mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran;
- ii. menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan;
- iii. menyimpan jejak audit dan memelihara bahan bukti; dan
- iv. menyediakan tindakan pemulihan segera.

8.2 Perancangan dan Penerimaan Sistem

8.2.1 Perancangan Kapasiti

- i. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan
- ii. 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.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	32/55

DASAR KESELAMATAN ICT MAIPk

8.2.2 Penerimaan Sistem

Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.

8.3 Perisian Berbahaya

8.3.1 Perlindungan dan Perisian Berbahaya

- i. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan *Intrusion Detection System (IDS)* dan mengikut prosedur penggunaan yang betul dan selamat;
- ii. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997;
- iii. Mengimbas semua perisian atau sistem dengan *anti virus* sebelum menggunakannya;
- iv. Mengemaskini pattern *anti virus*;
- v. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;
- vi. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;
- vii. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	33/55

Dasar Keselamatan ICT MAIPk

- viii. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan
- xi. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.

8.4 Housekeeping

8.4.1 Penduaan

Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan disimpan di *off site*;

- i. membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru;
- ii. membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan
- iii. menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.

8.4.2 Sistem Log

- i. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna;
- ii. Mewujudkan satu sistem log secara berpusat dan perlu dibuat pendua;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	34/55

DASAR KESELAMATAN ICT MAIPk

- iii. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan
- iv. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan dengan segera kepada Pegawai Atasan.

8.5 Pengurusan Rangkaian

8.5.1 Kawalan Infrastruktur Rangkaian

Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan:

- i. tanggungjawab atau kerja-kerja operasi rangkaian dan operasi komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;
- ii. peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;
- iii. capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;
- iv. semua peralatan mestilah melalui proses *Factory Acceptance Check (FAC)* semasa pemasangan dan konfigurasi;
- v. *firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi kerajaan serta dikonfigurasi oleh pentadbir sistem;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	35/55

DASAR KESELAMATAN ICT MAIPk

- vi. semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MAIPk;
- vii. semua perisian sniffer atau network analyser atau perisian seumpama denganya adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;
- viii. memasang perisian *Intrusion Detection System (IDS)* bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MAIPk;
- ix. memasang *Web Content Filter* pada Internet Gateway untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”;
- x. sebarang penyambungan rangkaian yang bukan di bawah kawalan MAIPk hendaklah mendapat kebenaran ICTSO;
- xi. semua pengguna hendaklah dibenarkan menggunakan rangkaian MAIPk sahaja. Penggunaan modem hendaklah mendapat kebenaran ICTSO;
- xii. MAIPk berhak untuk menamatkan perkhidmatan rangkaian VPN (MAIPkNet) sesuatu jabatan atau agensi yang melalui firewall MAIPk sekiranya difikirkan tidak perlu lagi; dan
- xiii. memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	36/55

8.5.2 Rangkaian Tanpa Wayar

Langkah-langkah minimum perlu dilaksanakan bagi memperkukuhkan kawalan keselamatan sistem rangkaian tanpa wayar. Berikut adalah langkah-langkah pengukuhan sistem tanpa wayar:

- i. langkah-langkah mesti mengikut Arahan Keselamatan dan para 4.4.3.3 Malaysia Public Sector Management of ICT Security Handbook (MyMIS) yang dikeluarkan oleh MAMPU pada 2001.
- ii. melaksanakan enkripsi ke atas wireless access point (AP).
- iii. meningkatkan keselamatan penggunaan wireless access point menerusi kaedah berikut:
 - Menggunakan enkripsi dan network key yang kukuh dengan kombinasi pelbagai *character* seperti *alphabet*, aksara khas dan nombor;
 - Kerap menukar kata laluan atau *network key*; dan
 - Kawalan penggunaan *MAC Address*.
- iv. pengukuhan struktur rangkaian setempat boleh dilaksanakan seperti berikut:
 - merekabentuk sistem rangkaian setempat supaya akses menerusi wireless access point (AP) perlu melalui tapisan keselamatan yang sewajarnya; dan
 - merekabentuk kawalan capaian menggunakan pengenalan pengguna (user authentication) melalui penggunaan Radius Server.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	37/55

DASAR KESELAMATAN ICT MAIPk

- v. pengukuhan keselamatan fizikal pula boleh dilaksanakan seperti berikut:
- memasang alat reflector yang akan mengawal pancaran signal radio wireless access point (AP) dalam jarak yang dikehendaki;
 - menggunakan cat dinding khas yang dapat menghalang pancaran signal supaya dapat melampaui jarak yang dikehendaki seperti *Defend Air Radio Shield Paint*; dan
 - menggunakan window shield yang dapat menghalang signal daripada melepasi melalui tingkap.

8.6 Pengurusan Media

8.6.1 Penghantaran dan Pemindahan

Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pegawai Atasan terlebih dahulu.

8.6.2 Prosedur Pengendalian Media

- i. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat;
- ii. Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja;
- iii. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan;
- iv. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan;
- v. Menyimpan semua media di tempat yang selamat; dan

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	38/55

DASAR KESELAMATAN ICT MAIPk

- vi. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapuskan atau dimusnahkan mengikut prosedur yang betul dan selamat.

8.6.3 Keselamatan Sistem Dokumentasi

- i. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan;
- ii. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan
- iii. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.

8.7 Keselamatan Komunikasi

8.7.1 Internet

- i. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan;
- ii. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan;
- iii. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet;
- iv. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;
- v. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh Jabatan;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	39/55

DASAR KESELAMATAN ICT MAIPk

- vi. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; dan
- vii. Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.

8.7.2 Mel Elektronik (Emel)

- i. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh jabatan sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;
- ii. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh MAIPk;
- iii. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;
- iv. Penghantaran e-mel rasmi hendaklah menggunakan e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;
- v. Pengguna dinasihatkan menggunakan fail kepilang, sekiranya perlu, tidak melebihi dua (2) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	40/55

DASAR KESELAMATAN ICT MAIPk

- vi. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;
- vii. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;
- viii. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;
- ix. E-mel yang tidak penting dan tidak mempunyai nilai arkid yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;
- x. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan
- xi. Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	41/55

KAWALAN CAPAIAN

9.1 Dasar Kawalan Capaian

9.1.1 Keperluan Dasar

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada.

9.1.2 Akaun Pengguna

Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenalpasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi:

- i. akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan;
- ii. akaun pengguna mestilah unik;
- iii. akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;
- iv. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan;
- v. pengguna akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan
- vi. pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut;

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	42/55

DASAR KESELAMATAN ICT MAIPk

- pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu;
- bertukar bidang tugas kerja;
- bertukar ke agensi lain;
- bersara; dan
- ditamatkan perkhidmatan.

9.1.3 Jejak Audit

Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi:

- i. maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan;
- ii. aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan
- iii. maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan.

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.

9.1.4 Sistem Maklumat dan Aplikasi

Capaian sistem dan aplikasi di MAIPk adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi:

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	43/55

DASAR KESELAMATAN ICT MAIPk

- i. pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan;
- ii. setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;
- iii. memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan;
- iv. menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat;
- v. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan
- vi. capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.

9.2 Peralatan Komputer Mudah Alih

9.2.1 Penggunaan Peralatan Komputer Mudah Alih

- i. Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan
- ii. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	44/55

PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

10.1 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

10.1.1 Keperluan Dasar

- i. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujud sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat;
- ii. 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; dan
- iii. Sebaik-baiknya, semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.

10.2 Kriptografi

10.2.1 Penyulitan

Pengguna hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.

10.2.2 Tandatangan Digital

Pengguna tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	45/55

10.2.3 Pengurusan Kunci (Key)

Pengurusan kunci (key) hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci (key) berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.

10.3 Sistem Fail

10.3.1 Kawalan Sistem Fail

- i. proses pengemaskini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan;
- ii. kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji;
- iii. mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan
- iv. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.

10.4 Pembangunan dan Proses Sokongan

10.4.1 Kawalan Perubahan

Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	46/55

KESINAMBUNGAN PERKHIDMATAN

11.1 Dasar Kesenambungan Perkhidmatan

11.1.1 Pelan Kesenambungan Keselamatan

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 JTICT dan perkara-perkara berikut perlu diberi perhatian:

- i. mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;
- ii. melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;
- iii. mendokumentasikan proses dan prosedur yang telah dipersetujui;
- iv. mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;
- v. membuat penduaan; dan
- vi. menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	47/55

DASAR KESELAMATAN ICT MAIPk

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

Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

Senarai personel MAIPk dan vendor beserta nombor yang boleh dihubungi (faksmile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden;

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

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

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

Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan.

Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

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

MAIPk dan bahagian yang berkenaan yang mempunyai pelan BCM hendaklah memastikan salinan pelan BCM masing-masing sentiasa dikemas kini dan dilindungi seperti di lokasi utama.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	48/55

PEMATUHAN DASAR

12.1 Pematuhan dan Keperluan Perundangan

12.1.1 Pematuhan Dasar

Setiap pengguna di MAIPk hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MAIPk dan undang-undang atau peraturan-peraturan lain yang berkaitan dan masih berkuatkuasa.

Semua aset ICT di MAIPk termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.

Sebarang penggunaan aset ICT MAIPk dan bahagian masing-masing selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber.

12.1.2 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

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

Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.

12.1.3 Pematuhan Keperluan Audit

Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	49/55

DASAR KESELAMATAN ICT MAIPk

Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.

12.1.4 Keperluan Perundangan

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MAIPk:

- Arahan Keselamatan;
- Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;
- Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS);
- Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
- Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan”;
- Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
- Akta Tandatangan Digital 1997;
- Akta Jenayah Komputer 1997;
- Akta Hak Cipta (Pindaan) Tahun 1997; dan
- Akta Komunikasi dan Multimedia 1998.
- Pekeliling-pekelling dan prosedur-prosedur yang dikeluarkan dari masa ke semasa.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	50/55

DASAR KESELAMATAN ICT MAIPk

12.1.5 Pelanggaran Dasar

Pelanggaran Dasar Keselamatan ICT ini boleh dikenakan tindakan tatatertib.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPk	1.0	20.11.2015	51/55

GLOSARI

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetic, <i>optical disk</i> , <i>flash disk</i> , CDROM, <i>thumb drive</i> untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Back up	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	<i>Chief Information Officer</i> Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
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 (<i>information theft/espionage</i>), penipuan (<i>hoaxes</i>)
GCERT	<i>Government Computer Emergency Response Team</i> 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.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPK	1.0	20.11.2015	52/55

DASAR KESELAMATAN ICT MAIPK

Hub	Hab (hub) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bus 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 sistem komputer.
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 Pencegahan 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 computer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau <i>malicious code</i> . Contohnya : <i>Network-based IPS</i> yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer.
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, <i>trojan horse</i> , <i>worm</i> , <i>spyware</i> dan sebagainya.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPK	1.0	20.11.2015	53/55

DASAR KESELAMATAN ICT MAIPk

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.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti <i>spreadsheet</i> dan <i>word processing</i> 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.
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.
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 protocol penghantaran dengan mengurangkan perlanggaran yang berlaku.
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.

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKCIT MAIPk	1.0	20.11.2015	54/55

DASAR KESELAMATAN ICT MAIPK PERAK

LAMPIRAN 1 : SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT

Nama (Huruf Besar) : DR. AMIRUDDIN B. MUHAMED

No Kad Pengenalan : 720313 -08 -6139

Jawatan : KETUA PEGAWAI EKSEKUTIF

Bahagian :

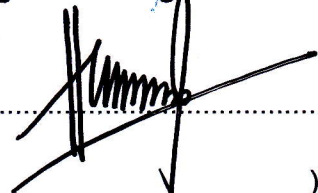
Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT ini; dan
2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tanda tangan : 

Tarikh : 20.11.2015

Pengesahan Pegawai Keselamatan ICT


.....
(.....)

MOHD HAIDI BIN SULAIMAN 7/12/15
Timbalan Ketua Pegawai Eksekutif
(Pengurusan)
Majlis Agama Islam dan 'Adat Melayu Perak

b.p Ketua Pegawai Eksekutif
Majlis Agama Islam dan 'Adat Melayu Perak

Tarikh :

RUJUKAN	VERSI	TARIKH	MUKASURAT
DKICT MAIPK	1.0	20 NOV 2015	55/55