



IBU PEJABAT KASTAM DIRAJA MALAYSIA,
BAHAGIAN KHIDMAT PENGURUSAN DAN SUMBER MANUSIA,
(CAWANGAN TEKNOLOGI MAKLUMAT)
ARAS 5 UTARA, KOMPLEKS KEMENTERIAN KEWANGAN,
NO. 3, PERSIARAN PERDANA,
PRESINT 2,
62596 PUTRAJAYA, MALAYSIA.



No. Tel : 03 - 88822100
No. Fax : 03 - 88822597
E - Mail : kastam@customs.gov.my

Ruj. Kami : KE.HK (-)646/04-1(2)

Tarikh : // Jun 2013

Semua Pengarah Ibu Pejabat

Semua Pengarah Kastam Negeri

Pengarah Kastam, Lapangan Terbang Antarabangsa Kuala Lumpur (KLIA)

Pengarah Kastam, Wilayah Persekutuan Labuan

Pengarah AKMAL

Pemungut Cukai Kastam Persekutuan, Singapura

SURAT PEKELILING ICT JABATAN KASTAM DIRAJA MALAYSIA BILANGAN 2 TAHUN 2013

DASAR ICT JABATAN KASTAM DIRAJA MALAYSIA

TUJUAN

Surat Pekeliling ICT ini bertujuan untuk menjelaskan Dasar Teknologi Maklumat dan Komunikasi (ICT) Jabatan Kastam Diraja Malaysia (JKDM) dan perkara-perkara berkaitan yang perlu dipatuhi dalam menggunakan aset ICT JKDM.

LATAR BELAKANG

2. Kerajaan telah mengeluarkan Pekeliling Am Bilangan 3 Tahun 2000 -"Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan" pada 1 Oktober 2000. Pekeliling tersebut dirumus untuk memenuhi keperluan penguatkuasaan, kawalan dan langkah-langkah yang menyeluruh untuk melindungi aset ICT kerajaan. Semua agensi kerajaan, dipertanggungjawabkan untuk memastikan Rangka Dasar Keselamatan ICT Kerajaan dilaksanakan dan dipatuhi.

3. Selaras dengan pekeliiling tersebut, Dasar ICT JKDM diwujudkan sebagai garis panduan kepada seluruh warga JKDM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT JKDM.

4. Sehubungan dengan itu, Mesyuarat Jawatankuasa Pemandu ICT (JPICT) JKDM Bil 1/2013 yang telah diadakan pada 11 April 2013 telah bersetuju untuk mengguna pakai dan menguatkuasakan peraturan-peraturan yang ditetapkan di dalam surat pekeliiling ini.

DASAR ICT JABATAN KASTAM DIRAJA MALAYSIA

5. Dasar ICT JKDM seperti di Lampiran adalah terpakai oleh semua pengguna di JKDM termasuk kakitangan, pembekal, pakar runding yang mengurus, menyenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT JKDM.

TANGGUNGJAWAB PENGGUNA

6. Semua pengguna JKDM adalah dikehendaki mematuhi Dasar ICT JKDM dan melaksanakan tanggungjawab yang ditetapkan di dalamnya.

PERANAN CAWANGAN TEKNOLOGI MAKLUMAT(CTM)

7. CTM bertanggungjawab dalam memastikan kepatuhan kepada Surat Pekeliling ICT ini di JKDM.

TARIKH KUATKUASA

8. Surat Pekeliling ICT ini adalah berkuat kuasa mulai tarikh ianya dikeluarkan.

PEMBATALAN

9. Dengan berkuat kuasanya Surat Pekeliling ICT ini, maka Dasar Keselamatan ICT yang diedarkan melalui surat rujukan KE.HK(-)646/04-1(1) bertarikh 25 Mei 2010 adalah dibatalkan.

Sekian, terima kasih.

"BERKHIDMAT UNTUK NEGARA"



(DATO' SRI KHAZALI BIN HJ. AHMAD)
Ketua Pengarah Kastam
Malaysia.

s.k.

TKPK (Penguatkuasaan/Pematuhan)

TKPK (Perkastaman/Cukai Dalam Negeri)

TKPK (Pengurusan)

Pen. KPK (Bahagian Penguatkuasaan)



KERAJAAN MALAYSIA

DASAR ICT

JABATAN KASTAM DIRAJA MALAYSIA



Jabatan Kastam Diraja Malaysia
Kementerian Kewangan
Jun 2013

Dikelilingkan kepada

Semua Pengarah Ibu Pejabat

Semua Pengarah Kastam Negeri

Pengarah Kastam, Lapangan Terbang Antarabangsa Kuala Lumpur (KLIA)

Pengarah Kastam, Wilayah Persekutuan Labuan

Pengarah AKMAL

Pemungut Cukai Kastam Persekutuan, Singapura



KANDUNGAN		MUKASURAT
Perkara 1.0	Pembangunan dan Penyelenggaraan Dasar	5
Perkara 2.0	Organisasi ICT	6
Perkara 3.0	Dasar Perkakasan dan Perisian ICT JKDM	9
Perkara 4.0	Dasar Pengurusan e-Mel dan Penggunaan Internet	12
Perkara 5.0	Dasar Sistem Aplikasi dan Pangkalan Data	16
Perkara 6.0	Dasar Pengurusan dan Penggunaan Rangkaian	18
Perkara 7.0	Dasar Keselamatan ICT	20
Perkara 8.0	Pematuhan	41



GLOSARI

- Aset - Harta benda kepunyaan atau milikan atau di bawah kawalan Kerajaan yang dibeli atau yang disewa beli dengan wang Kerajaan, yang diterima melalui sumbangan atau hadiah atau diperolehi melalui proses perundangan
- Aset ICT - Termasuk, tetapi tidak terhad kepada sistem komputer peribadi, terminal, alat-alat periferal komputer, peralatan komunikasi, rangkaian komunikasi, perisian komputer, dokumentasi bantuan, peralatan storan, kemudahan sokongan dan sumber tenaga. Kemudahan terhad kepada kemudahan yang dibeli, disewa, dipajak, dimiliki atau dipinjamkan kepada JKDM. Ia termasuk semua kemudahan, maklumat dan sistem aplikasi
- Bahagian - Bahagian-bahagian di Ibu Pejabat, JKDM
- CIO / *Chief Information Officer* - Ketua Pegawai Maklumat JKDM - Timbalan Ketua Pengarah Kastam (Pengurusan)
- CTM - Cawangan Teknologi Maklumat, Ibu Pejabat
- Hapuskira - Satu proses untuk membatalkan rekod aset yang hilang
- ICT - Teknologi Maklumat dan Komunikasi
- ICTSO / *ICT Security Officer* - Pegawai Keselamatan ICT JKDM
- JKDM - Jabatan Kastam Diraja Malaysia
- JPICT - Jawatankuasa Pemandu ICT
- Kehilangan - Aset yang tiada lagi dalam simpanan disebabkan oleh kecurian, kemalangan, kebakaran, bencana alam, kesusutan, penipuan atau kecuaiian pegawai awam
- KPK - Ketua Pengarah Kastam Malaysia
- Negeri - Negeri dan stesen-stesen JKDM di bawah kawalan negeri
- Pakar Perunding - Seseorang atau kumpulan orang yang dipilih untuk memberi perkhidmatan dalam bentuk khidmat nasihat ICT di JKDM

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	1 daripada 49



- Pegawai JKDM - Seseorang yang dilantik untuk sesuatu jawatan sama ada secara tetap, sambilan, sementara atau kontrak yang berkhidmat di JKDM, sama ada di negeri atau di Ibu Pejabat
- Pegawai keselamatan - Seseorang yang dilantik untuk menjaga keselamatan mengikut skop atau ruang lingkup yang telah dipertanggungjawabkan.
- Pelupusan - Satu proses untuk mengeluarkan aset dari milikan, kawalan, simpanan dan rekod mengikut kaedah yang ditetapkan
- Pemilik sumber maklumat - pihak yang bertanggungjawab ke atas maklumat di dalam sesuatu sistem
- Pembekal - Seseorang atau kumpulan orang yang dibenarkan membekal sama ada perkhidmatan atau barangan ICT di JKDM
- Pengguna - Warga JKDM yang dibenarkan menggunakan kemudahan ICT JKDM
- Pengurus ICT - Timbalan Pengarah Cawangan Teknologi Maklumat (TPh CTM) yang mengetuai CTM
- Pentadbir Sistem - Pegawai CTM yang dilantik oleh Pengurus ICT JKDM bagi mengetuai sesuatu sistem atau sistem aplikasi
- Peralatan rangkaian - Peralatan dan komponen yang digunakan dalam sistem rangkaian seperti *switch*, *hub*, *router* dan sebagainya
- Perisian ICT - Merangkumi semua jenis perisian sistem dan perisian aplikasi. Perisian sistem merangkumi sistem operasi, pangkalan data dan perisian bagi membangunkan sistem. Perisian aplikasi adalah sistem aplikasi yang dibangunkan ataupun pakej sedia ada (*off-the-shelf*) untuk kegunaan tertentu (contoh: Sistem Perakaunan, Sistem Personel dan Sistem Pengurusan Inventori) dan perisian yang digunakan untuk menyokong kerja-kerja harian seperti penyediaan dokumentasi
- Perkakasan ICT - Peralatan dan komponen ICT seperti *server*, komputer, *notebook*, pencetak dan sebagainya
- Pihak Ketiga - Pembekal atau pakar perunding
- Server* - Komputer yang mempunyai keupayaan tinggi yang

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	2 daripada 49



memberi perkhidmatan berpusat

Masa sistem tidak aktif (idle time) - Masa sesuatu sumber komputer yang sepatutnya digunakan tetapi tidak menjalankan sebarang pengendalian atau tugas berguna bagi pengguna
(Sumber rujukan : Kamus Komputer, Dewan Bahasa dan Pustaka)

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	3 daripada 49



PENGENALAN

Dasar ICT Jabatan Kastam Diraja Malaysia (JKDM) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) JKDM. Dasar ini juga menerangkan kepada semua pengguna di JKDM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT JKDM.

OBJEKTIF

Dasar ICT JKDM diwujudkan untuk menjamin kesinambungan urusan JKDM melalui kemudahan ICT dengan meminimumkan kesan insiden keselamatan ICT.

SKOP

Dasar ini meliputi semua sumber atau aset ICT yang digunakan seperti:

- i. maklumat (contoh: fail, dokumen dan data elektronik)
- ii. perisian (contoh: aplikasi dan sistem perisian)
- iii. perkakasan (contoh: komputer, peralatan komunikasi dan media magnet).

Dasar ini adalah terpakai untuk semua pengguna di JKDM termasuk pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyediakan, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT JKDM.

PRINSIP-PRINSIP

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

a. Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya ke atas aset ICT JKDM; dan

b. Pematuhan

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

Perkara 1.0 - Pembangunan dan Penyelenggaraan Dasar

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	4 daripada 49



Item/Aktiviti	Tanggungjawab
1.1 Pelaksanaan Dasar	
Pelaksanaan Dasar ini akan dijalankan oleh Ketua Pengarah Kastam Malaysia (KPK) dibantu oleh Pasukan Pengurusan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pengurus ICT, Pegawai Keselamatan ICT (ICTSO), semua Pengarah Bahagian serta semua Pengarah Kastam Negeri.	KPK
1.2 Penyebaran Dasar	
Dasar ini perlu disebar kepada semua pengguna JKDM dan pihak ketiga.	CTM
1.3 Penyelenggaraan Dasar	
<p>Dasar ICT JKDM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan arahan serta keperluan semasa.</p> <p>Berikut adalah prosedur berhubung dengan penyelenggaraan Dasar ICT JKDM:</p> <ol style="list-style-type: none">Kenal pasti dan tentukan perubahan yang diperlukan;Kemuka cadangan pindaan untuk persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) JKDM;Perubahan yang telah dipersetujui oleh JPICT JKDM dimaklumkan kepada semua pengguna; danDasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	CTM
1.4 Pengecualian	
Dasar ICT JKDM adalah terpakai kepada semua pengguna ICT JKDM dan tiada pengecualian diberikan.	Semua

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	5 daripada 49



Perkara 2.0 - Organisasi ICT

Item/Aktiviti		Tanggungjawab	
2.1 Ketua Pengarah Kastam Malaysia			
<p>Peranan dan tanggungjawab KPK adalah seperti berikut:</p> <ul style="list-style-type: none">a. Memastikan semua pengguna memahami peraturan-peraturan di bawah Dasar ICT JKDM;b. memastikan semua pengguna mematuhi Dasar ICT JKDM;c. memastikan semua keperluan ICT JKDM disokong dengan sumber kewangan, sumber manusia serta perkakasan ICT yang mencukupi; dand. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan dalam Dasar ICT JKDM.e. Mepengerusikan mesyuarat Jawatankuasa Pemandu ICT (JPICT), JKDM.	KPK		
2.2 Ketua Pegawai Maklumat (CIO)			
<p>Timbalan Ketua Pengarah Kastam (Pengurusan) telah dilantik sebagai Ketua Pegawai Maklumat (CIO) JKDM. CIO bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di JKDM.</p>	CIO		
2.3 Pengurus ICT			
<p>Timbalan Pengarah Cawangan Teknologi Maklumat (CTM) adalah merupakan Pengurus ICT JKDM. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut:</p> <ul style="list-style-type: none">a. Merangka, merumus dan menguatkuasa Dasar ICT JKDM;b. mengkaji semula dan melaksanakan Dasar ICT JKDM selaras dengan keperluan JKDM;c. menentukan kawalan akses semua pengguna terhadap aset ICT JKDM; dand. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT JKDM.	TPh CTM		
2.4 Pegawai Keselamatan ICT (ICTSO)			
<p>Ketua Unit Teknikal CTM adalah merupakan ICTSO JKDM. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti</p>	ICTSO		
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	6 daripada 49



Item/Aktiviti	Tanggungjawab
<p>berikut:</p> <ul style="list-style-type: none"> a. Mengurus keseluruhan program-program keselamatan ICT JKDM; b. menguatkuasakan Dasar Keselamatan ICT JKDM; c. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT JKDM; d. menjalankan pengurusan risiko; e. menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; f. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; g. melaporkan insiden keselamatan ICT kepada Pasukan Tindakbalas Insiden Keselamatan ICT (GCERT) dan memaklukkannya kepada CIO; h. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; i. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar ICT JKDM; dan j. menyediakan dan melaksanakan program-program kesedaran mengenai keselamatan ICT. 	

2.5 Pentadbir Sistem

<p>Pentadbir Sistem terdiri daripada pegawai JKDM yang mengurus tadbir samaada sistem rangkaian atau sistem aplikasi (contoh: Sistem Maklumat Kastam, e-mel, laman web dan sebagainya). Peranan dan tanggungjawab Pentadbir Sistem adalah seperti berikut:</p> <ul style="list-style-type: none"> a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas; b. menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar ICT JKDM; c. memantau aktiviti capaian harian pengguna; d. mengenal pasti aktiviti-aktiviti tidak normal seperti 	CTM
--	-----

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	7 daripada 49



Item/Aktiviti	Tanggungjawab
penceroobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikanannya dengan serta merta; e. menyimpan dan menganalisis rekod jejak audit; dan f. menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	
2.6 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar ICT JKDM; b. lulus tapisan keselamatan; c. melaksanakan prinsip-prinsip Dasar ICT JKDM dan menjaga kerahsiaan maklumat JKDM; d. melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. memeriksa maklumat dan menentukan maklumat tersebut adalah 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. e. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan f. menghadiri program-program pembudayaan dan kesedaran ICT.	Pengguna

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	8 daripada 49



Perkara 3.0 - Dasar Perkakasan dan Perisian ICT JKDM

Item/Aktiviti		Tanggungjawab	
3.1 Perolehan/Pelupusan Perkakasan dan Perisian ICT			
3.1.1 Perolehan Perkakasan dan Perisian ICT			
a. Tatacara perolehan perkakasan dan perisian ICT hendaklah merujuk kepada pekeliling yang sedang berkuatkuasa.		Semua	
b. Bahagian/Negeri hendaklah memohon secara rasmi kepada Urusetia JPICT JKDM untuk kelulusan JPICT JKDM bagi sebarang perolehan baru / peningkatan perkakasan, perisian dan perkhidmatan ICT.			
c. Garis panduan untuk perolehan perkakasan dan perisian ICT JKDM adalah seperti di Lampiran 1 .			
d. Perolehan bagi perkakasan ICT bernilai kurang daripada RM1000 adalah dibenarkan dibuat sendiri oleh pihak negeri setelah mendapat kelulusan JPICT JKDM.			
3.1.2 Pelupusan Perkakasan dan Perisian ICT			
a. Tatacara pelupusan perkakasan dan perisian ICT hendaklah merujuk kepada pekeliling yang sedang berkuatkuasa.		Semua	
b. Bahagian/Negeri hendaklah memohon secara rasmi kepada Cawangan Logistik, Ibu Pejabat bagi sebarang pelupusan perkakasan ICT.			
c. Untuk maklumat lanjut, sila rujuk: "Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan".			
3.2 Peruntukan/Penggunaan Perkakasan dan Perisian ICT			
3.2.1 Pencetak			
Pencetak perlu diguna secara 'pool' dengan nisbah yang difikirkan sesuai oleh Bahagian/Negeri untuk kelancaran kerja dan jenis kerja yang dilakukan seperti kerahsiaan maklumat, kedudukan tempat dan proses kerja.		Semua	
3.2.2 Komputer			
a. Warga JKDM yang berkelayakan akan diperuntukkan komputer mengikut keperluan dan kesesuaian tugas.		Semua	
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	9 daripada 49



Item/Aktiviti	Tanggungjawab
b. Pegawai JKDM yang bekerja mengikut syif hendaklah menggunakan komputer secara gunasama. c. Komputer riba (<i>Notebook</i>) yang dibekalkan oleh Ibu Pejabat JKDM hendaklah digunakan secara gunasama.	
3.2.3 Komputer Riba	
Komputer riba (<i>Notebook</i>) yang dibekalkan oleh Ibu Pejabat JKDM hendaklah digunakan secara gunasama oleh Bahagian/ Negeri.	Semua
3.3 Penyelenggaraan Perkakasan dan Perisian ICT	
a. Penyelenggaraan perkakasan ICT yang dibekalkan oleh Ibu Pejabat JKDM ke Bahagian/Negeri perlulah diselaras oleh Bahagian/Negeri sendiri bagi memudahkan pemantauan dan inventori. b. Aduan tentang masalah-masalah yang dihadapi dalam penggunaan ICT perlu diajukan kepada Meja Bantuan CTM Ibu Pejabat / Negeri seperti di Lampiran 3. c. Senarai perisian ICT yang disokong oleh CTM bagi perkhidmatan pemasangan, penyelenggaraan dan latihan adalah seperti berikut: i. MS Office yang terdiri daripada: <ul style="list-style-type: none">• MS Word• MS Excel• MS Powerpoint ii. Open Office yang terdiri daripada: <ul style="list-style-type: none">• writer• calc• impress iii. Internet browser yang terdiri daripada: <ul style="list-style-type: none">• Internet Explorer• Mozilla Firefox• Google Chrome iv. E-mel d. Perkhidmatan bagi perisian ICT selain daripada yang tersebut di atas hanya akan diberikan sekiranya ada tenaga kepakaran	Semua

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	10 daripada 49



Item/Aktiviti	Tanggungjawab
di CTM.	

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	11 daripada 49



Perkara 4.0 - Dasar Pengurusan E-mel dan Penggunaan Internet

Item/Aktiviti	Tanggungjawab
4.1 Pengurusan E-mel	
<p>a. Akaun e-mel bukanlah hak mutlak seseorang. Ia adalah kemudahan yang tertakluk kepada peraturan jabatan dan boleh ditarik balik jika penggunaannya melanggar peraturan.</p> <p>b. Semua pengguna adalah bertanggungjawab kepada e-mel masing-masing. JKDM tidak akan bertanggungjawab ke atas sebarang kesalahan jenayah dan seumpamanya berkaitan e-mel.</p> <p>c. Pengguna hendaklah menggunakan e-mel sebagai saluran rasmi dalam urusan rasmi dan urusan pentadbiran harian.</p> <p>d. Pengguna dikehendaki merahsiakan kata laluan daripada pengetahuan orang lain.</p> <p>e. Pengguna diminta menukarkan kata laluan masing-masing sekurang-kurangnya sebulan sekali bagi mengelakkan akaun mereka dicerobohi.</p> <p>f. Pegawai JKDM tidak dibenarkan menggunakan kemudahan e-mel percuma seperti <i>Hotmail</i>, <i>Yahoo mail</i>, <i>Gmail</i> dan lain-lain untuk tujuan rasmi.</p> <p>g. Setiap alamat e-mel yang disediakan adalah untuk kegunaan individu berkenaan sahaja dan tidak boleh digunakan oleh pihak lain sama ada dengan kebenaran atau tanpa kebenaran.</p> <p>h. Pengguna adalah dinasihatkan menggunakan kemudahan e-mel secara rutin sekurang-kurangnya sekali sehari.</p> <p>i. Mana-mana e-mel rasmi yang dihantar dan diterima perlu di <i>archive</i> sendiri oleh pengguna.</p> <p>j. Pengguna mesti melakukan <i>housekeeping</i> sekiranya petunjuk kuota telah mencapai 80% kegunaannya. Ini adalah bagi memastikan kotak mel tidak penuh dan seterusnya menjamin kelancaran penggunaan sistem e-mel.</p> <p>k. Elakkan membuka e-mel sekiranya identiti penghantar tidak diketahui dan diragui. Pengguna perlulah memadam terus e-mel tersebut.</p> <p>l. Had penghantaran bahan kepilang (<i>attachment</i>) tidak melebihi 10 MB dalam satu masa.</p> <p>m. Bagi pengguna yang bertukar tempat kerja secara dalaman hendaklah memaklumkan kepada pentadbir sistem e-mel dengan segera supaya pengemaskinian akaun e-mel dapat dilaksanakan.</p> <p>n. Cawangan Perkhidmatan dan Latihan Ibu Pejabat hendaklah</p>	Semua

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	12 daripada 49



Item/Aktiviti	Tanggungjawab
<p>mengemaskini akaun e-mel dengan segera pegawai yang berpindah keluar dari JKDM atau pegawai yang telah tamat perkhidmatan dengan jabatan secara wajib/pilihan.</p> <p>o. Pengguna yang telah tidak wujud akan dihapus ID dan capaiannya kepada e-mel dalam masa 1 bulan.</p> <p>p. Pengguna hendaklah sentiasa mengimbas fail bagi memastikan fail yang akan dihantar melalui kepilang (<i>attachment</i>) bebas dari virus.</p> <p>q. Aktiviti <i>spamming</i>, penyebaran virus, bahan-bahan negatif, surat berantai dan promosi-promosi perniagaan adalah dilarang. Jika didapati aktiviti ini dilakukan oleh pengguna, akaun e-mel mereka akan dinyahaktifkan tanpa sebarang notis.</p> <p>r. Pentadbir Sistem berhak memasang sebarang jenis perisian atau perkakasan penapisan e-mel dan virus yang difikirkan sesuai dan boleh menggunakannya untuk mencegah, menapis, menyekat atau menghapuskan mana-mana e-mel yang disyaki mengandungi virus atau berunsur <i>spamming</i> daripada memasuki komputer.</p> <p>s. Menyebar perisian cetak rompak atau maklumat berbaur politik, hasutan atau perkauman atau apa-apa maklumat yang menjejaskan reputasi JKDM dan Perkhidmatan Awam melalui kemudahan e-mel JKDM adalah dilarang.</p> <p>t. Pengguna dilarang melakukan pencerobohan atau percubaan untuk mencerooboh masuk ke mana-mana akaun pengguna lain.</p> <p>u. Pihak KPK/CIO/Pengurus ICT/ICTSO/Pentadbir Sistem boleh memantau semua e-mel JKDM jika perlu tanpa mendapat kebenaran pengguna.</p>	

4.2 Penggunaan Internet

<p>a. Pengguna yang menggunakan aplikasi atas talian dan laman web adalah bertanggung jawab sepenuhnya ke atas maklumat yang dikunci masuk (<i>key-in</i>) serta capaian yang dilakukan.</p> <p>b. Pengguna tidak dibenar menyumbangkan perkara-perkara bertentangan dengan Perintah Am Kerajaan kepada mana-mana laman web tanpa kebenaran Ketua Jabatan.</p> <p>c. Pengguna tidak dibenarkan membuat capaian kepada bahan-bahan terlarang dan menggunakan sebarang perisian judi atau seumpamanya dengan menggunakan kemudahan</p>	Semua
--	-------

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	13 daripada 49



Item/Aktiviti	Tanggungjawab
<p>pejabat.</p> <p>d. Capaian laman web yang berbentuk hiburan, <i>chatting</i>, permainan komputer <i>online</i>, radio <i>online</i> dan <i>video streaming</i> yang membebankan rangkaian JKDM adalah tidak dibenarkan semasa waktu pejabat.</p> <p>e. Pengguna tidak dibenarkan melanggan kepada mana-mana <i>mailing list</i> dengan menggunakan e-mel rasmi jabatan yang tidak berkaitan dengan tugas.</p> <p>f. Pengguna tidak dibenarkan membuat capaian ke Laman Rangkaian Sosial seperti <i>Facebook</i> dan <i>Twitter</i> semasa waktu pejabat kecuali mendapat kelulusan pihak CTM/Pengarah Kastam Negeri.</p> <p>g. Capaian ke internet dimestikan melalui tapisan <i>firewall</i>. Pengguna tidak dibenarkan menginstalasi apa-apa perisian untuk melepasi tapisan <i>firewall</i>.</p> <p>h. Aktiviti <i>chatting</i> adalah tidak dibenarkan ketika waktu pejabat.</p> <p>i. Aktiviti muat turun (download) atau muat naik (upload) sebarang perisian cetak rompak adalah dilarang.</p> <p>j. Pengguna tidak dibenarkan melayari laman-laman yang tidak berkaitan dengan tugas di waktu pejabat.</p> <p>k. Pentadbir Sistem Rangkaian di JKDM adalah bertanggungjawab untuk menjana laporan capaian rangkaian dan internet setiap pengguna kepada pihak pengurusan.</p> <p>l. Pentadbir Sistem Rangkaian berhak menyediakan dan memasang perisian penapisan isi kandungan internet.</p> <p>m. Pentadbir Sistem Rangkaian berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yang tidak sesuai.</p> <p>n. Pengguna-pengguna yang didapati tidak mematuhi arahan dan larangan yang telah ditetapkan, Pentadbir Sistem Rangkaian berhak menarik balik kemudahan internet yang diberikan tanpa sebarang notis.</p>	

4.3 Laman dan Aplikasi Web

a. Semua maklumat yang hendak dimuatkan ke dalam laman web JKDM mestilah mendapat kelulusan Ketua Bahagian/Negeri.	Semua
b. Maklumat yang terkandung dalam laman web adalah di	

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	14 daripada 49



Item/Aktiviti	Tanggungjawab
bawah tanggungjawab Bahagian/Negeri masing-masing. c. Pencerobohan atau percubaan untuk menggodam laman web JKDM adalah dilarang. d. Aspek keselamatan laman web yang dipaut ke laman web JKDM menjadi tanggungjawab pemilik laman web sendiri.	

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	15 daripada 49



Perkara 5.0 - Dasar Sistem Aplikasi dan Pangkalan Data

Item/Aktiviti		Tanggungjawab	
5.1 Pembangunan Sistem Aplikasi Dan Pangkalan Data			
<p>a. Bahagian/Negeri hendaklah memohon secara rasmi kepada Urusetia JPICT untuk membangunkan sesuatu sistem aplikasi yang melibatkan kos, untuk tujuan mendapatkan kelulusan JPICT JKDM berdasarkan tatacara seperti di Lampiran 1.</p> <p>b. Pembangunan sistem aplikasi secara <i>in-house</i> dan tidak melibatkan kos perlu dimaklumkan kepada Urusetia JPICT. Maklumat yang perlu dikemukakan antara lain seperti:</p> <ul style="list-style-type: none"> • Tajuk Projek • Tujuan Projek • Keterangan Projek • Tempoh Pembangunan (Tarikh mula dan akhir) • Sasaran Pengguna • Kaedah Pelaksanaan (<i>standalone, web-based</i> dan sebagainya) <p>c. Pembangunan sistem aplikasi hendaklah mengambil kira sistem sedia ada di JKDM dan agensi lain bagi mengelakkan pertindihan pembangunan sistem aplikasi yang sama. Sebagai contoh pembangunan sistem yang berkaitan sumber manusia hendaklah dielakkan kerana HRMIS telah sedia untuk digunakan.</p> <p>d. Sebarang pembangunan sistem aplikasi mestilah menggunakan kod-kod yang standard di bawah <i>Data Dictionary</i> Sektor Awam (DDSA).</p> <p>e. Garis panduan untuk pembangunan sistem aplikasi dan pangkalan data adalah seperti di Lampiran 2.</p>		Semua	
5.2 Pelaksanaan Sistem Aplikasi			
<p>a. Sesuatu sistem aplikasi perlu dimiliki oleh sesuatu Bahagian/Negeri yang mempunyai kepentingan terhadap sistem yang dibangunkan.</p> <p>b. Pemilik sistem aplikasi tersebut hendaklah melantik <i>champion</i> bagi melancarkan pelaksanaan sistem. <i>Champion</i> sekurang-kurangnya di peringkat Ketua Bahagian/Negeri.</p> <p>c. Pemilik sistem aplikasi perlu membuat pelaporan kepada Urusetia JPICT secara berkala bagi kemajuan mengenai pembangunan atau pelaksanaan sistem aplikasi tersebut.</p>			
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	16 daripada 49



Item/Aktiviti	Tanggungjawab
<p>d. Pemilik sistem aplikasi hendaklah melantik pentadbir sistem untuk tujuan penyelenggaraan sistem tersebut.</p> <p>e. Bahagian/Negeri hendaklah memaklumkan kepada pentadbir sistem aplikasi dengan segera mengenai pegawai yang berpindah keluar dari JKDM/Bahagian/Negeri atau pegawai yang telah tamat perkhidmatan dengan jabatan secara wajib/pilihan supaya pengemaskinian/penghapusan ID pengguna dapat dilaksanakan.</p> <p>f. Pengguna sistem aplikasi yang telah tidak wujud akan dihapus ID dan capaiannya ke aplikasi dalam masa 1 bulan.</p>	

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	17 daripada 49



Perkara 6.0 - Dasar Pengurusan dan Penggunaan Rangkaian

Item/Aktiviti		Tanggungjawab	
6.1 Infrastruktur Rangkaian			
a. Semua komunikasi antara sistem ICT dengan sistem luar hendaklah melalui mekanisma pusat untuk mengurus, menguatkuasa dan mengawasi sebarang bahaya keselamatan. b. Hanya pengguna JKDM sahaja yang dibenarkan menggunakan rangkaian JKDM. c. Pengguna luar yang hendak menggunakan kemudahan rangkaian JKDM hendaklah mendapat kebenaran CTM.		Semua	
6.2 Pengurusan Alamat <i>Internet Protocol</i> (IP)			
a. Sebarang permohonan untuk menggunakan <i>static</i> IP bagi tujuan capaian ke rangkaian Kastam*Net, pengujian dan capaian ke atas aplikasi tertentu hendaklah melalui CTM secara rasmi. b. Pengguna adalah dilarang sama sekali untuk menukar atau menggunakan Alamat IP selain yang ditetapkan oleh CTM dalam komputer masing-masing tanpa kebenaran. c. <i>Static</i> IP yang diberikan kepada pengguna tidak boleh digunakan untuk kepentingan sendiri. Sekiranya pengguna didapati menyalahgunakan <i>static</i> IP dengan menukar konfigurasi komputer kepada <i>server</i> tanpa memaklumkan kepada CTM, komputer pengguna berkenaan akan dikeluarkan dari rangkaian.		Semua	
6.3 Sambungan Rangkaian			
a. Semua permohonan baru untuk mendapatkan sambungan rangkaian mestilah melalui CTM. b. Pengguna tidak dibenarkan menyambung sebarang perkakasan peribadi ke dalam rangkaian JKDM. c. Pengguna tidak dibenarkan memasang sebarang <i>access point</i> untuk capaian secara <i>wireless</i> ke dalam rangkaian JKDM. d. Pengguna tidak dibenarkan memutuskan/ menyambung sambungan kabel UTP pada mana-mana <i>port</i> dalam rak peralatan rangkaian tanpa kebenaran dari pihak CTM. e. Pengguna tidak dibenarkan menukar maklumat yang terdapat pada <i>faceplate</i> (UTP port).		Semua	
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	18 daripada 49



Item/Aktiviti	Tanggungjawab
<p>f. Perbuatan yang boleh merosakkan UTP port, kabel UTP atau rak perkakasan rangkaian serta perkakasan adalah dilarang.</p> <p>g. Sebarang kerosakan pada kabel UTP, <i>network point</i> dan <i>network port</i> pada mana-mana <i>switch/hub</i> hendaklah dilaporkan kepada CTM.</p>	
6.4 Muat turun (<i>Download</i>)/ Muat naik (<i>Upload</i>)	
Fail-fail yang bersaiz besar yang dimuat turun/dimuat naik hendaklah dilakukan selepas waktu pejabat.	Semua
6.5 Penyahvirus (<i>Antivirus</i>)	
<p>a. Kesemua perkakasan seperti komputer yang bersambung ke rangkaian JKDM mesti dipasang dan diaktifkan dengan perisian antivirus. Pengguna perlu memastikan perisian antivirus sentiasa dikemaskini dengan <i>virus pattern</i> terkini.</p> <p>b. Pengguna tidak dibenarkan memasang lebih daripada satu (1) jenis perisian antivirus.</p> <p>c. Sebarang perkakasan yang didapati menyebarkan virus dan setara dengannya, akan diputuskan hubungan ke rangkaian JKDM sehinggalah virus berkenaan dihapuskan.</p> <p>d. Semua pengguna hendaklah membuat <i>scanning</i> semua fail yang telah dimuat turun/dimuat naik dari mana-mana sumber termasuklah e-mel.</p> <p>e. Sebarang media seperti disket, <i>thumb drive</i>, CD dan lain-lain perlu diimbis sebelum sebarang fail dibaca atau disalin ke komputer masing-masing.</p> <p>f. Mana-mana pegawai yang didapati menjadi pembawa atau pembuat virus akan dilaporkan terus kepada Pengurus ICT.</p>	Semua

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	19 daripada 49



Perkara 7.0 - Dasar Keselamatan ICT

Item/Aktiviti		Tanggungjawab	
7.1 Akauntabiliti Aset ICT			
Objektif: Memberi perlindungan yang bersesuaian ke atas semua aset ICT JKDM.			
7.1.1 Inventori Aset ICT			
a. Semua aset ICT JKDM hendaklah direkodkan termasuk mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya.		Cawangan Logistik / Pegawai Aset	
b. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.		Semua	
7.2 Pengelasan dan Pengendalian Maklumat			
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.			
7.2.1 Pengelasan Maklumat			
Maklumat hendaklah dikelas dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mesti mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut:		Semua	
<ul style="list-style-type: none">• Rahsia Besar;• Rahsia;• Sulit; atau• Terhad			
7.2.2 Pengendalian Maklumat			
a. Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampaikan, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut:		Semua	
i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;			
ii. memeriksa maklumat dan menentukan ia tepat dan lengkap			
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	20 daripada 49



Item/Aktiviti	Tanggungjawab
<p>dari semasa ke semasa;</p> <ul style="list-style-type: none"> 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. <p>b. Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:</p> <ul style="list-style-type: none"> i. memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin dan mempunyai ciri-ciri keselamatan; ii. menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; iii. menggunakan penyulitan (<i>encryption</i>) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik; iv. memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak; dan v. mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada. 	

7.3 Keselamatan ICT dalam Tugas Harian

Objektif: Meminimumkan risiko seperti kesilapan, kecuaiian, kecurian, penipuan dan penyalahgunaan aset ICT JKDM.

7.3.1 Tanggungjawab Pengguna Terhadap Keselamatan ICT

<p>a. Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak.</p>	Semua
<p>b. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua</p>	

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	21 daripada 49



Item/Aktiviti		Tanggungjawab	
aset atau sumber ICT yang digunakan dalam melaksanakan tugas harian.			
7.4 Menangani Insiden Keselamatan ICT			
Objektif: Meminimumkan kesan insiden keselamatan ICT.			
7.4.1 Pelaporan Insiden			
Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera:		Semua	
<ul style="list-style-type: none"> a. Maklumat didapati hilang atau 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 didapati hilang, dicuri atau didedahkan; atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail atau sistem kerap kali gagal; dan e. berlaku percubaan mencero boh, menyeleweng atau insiden-insiden yang tidak diinginkan. <p><u>Nota:</u> Sila rujuk Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan ICT" untuk keterangan lanjut.</p>			
7.5 Pembudayaan Keselamatan ICT			
Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.			
7.5.1 Program Pembudayaan Keselamatan ICT			
<ul style="list-style-type: none"> a. Setiap pengguna di JKDM perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. b. Program kesedaran keselamatan ICT juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman 		ICTSO	
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	22 daripada 49



Item/Aktiviti		Tanggungjawab	
keselamatan ICT JKDM.			
7.6 Keselamatan Kawasan			
Objektif: Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.			
7.6.1 Kawasan Larangan			
a. Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kepada kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di JKDM adalah Pusat Data JKDM. Akses kepada kawasan tersebut hanya kepada pegawai-pegawai yang diberi kuasa sahaja.		Semua	
b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal. Mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.			
7.7 Keselamatan Perkakasan ICT			
Objektif: Melindung perkakasan dan maklumat.			
7.7.1 Perkakasan ICT			
Secara umumnya perkakasan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu. Setiap pengguna hendaklah:		Semua	
a. menyemak dan memastikan semua perkakasan ICT di bawah kawalannya dapat berfungsi dengan sempurna;			
b. menyimpan atau meletakkan perkakasan ICT di tempat yang bersih secara teratur dan mempunyai ciri-ciri keselamatan;			
c. bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan			
d. melapor sebarang bentuk penyelewengan atau salah guna perkakasan ICT kepada ICTSO.			
7.7.2 Media Storan			
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	23 daripada 49



Item/Aktiviti	Tanggungjawab
<p>Keselamatan media storan perlu diberi perhatian yang khusus. Langkah-langkah keselamatan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat:</p> <ul style="list-style-type: none">a. Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;b. akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja;c. penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu;d. pergerakan media storan hendaklah direkodkan; dane. pengguna mesti memastikan peranti storan (<i>disket, cd</i> atau <i>thumb drive</i>) yang menyimpan dokumen terhad disimpan di tempat yang selamat.	Semua
7.7.3 Kabel Rangkaian	
<p>Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:</p> <ul style="list-style-type: none">a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; danb. melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan.c. c. Setiap pemasangan kabel rangkaian perlu dilabelkan dan kemas.	Semua
7.7.4 Penyelenggaraan Perkakasan ICT	
<ul style="list-style-type: none">a. Perkakasan ICT hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti.b. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan.c. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja.d. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan.	Semua

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	24 daripada 49



Item/Aktiviti			Tanggungjawab
7.7.5 Peminjaman Perkakasan ICT untuk Kegunaan di Luar Pejabat			
<p>a. Perkakasan ICT yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan:</p> <ul style="list-style-type: none"> i. Perkakasan ICT, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan Ketua Bahagian/Negeri dan tertakluk kepada tujuan yang dibenarkan; dan ii. aktiviti peminjaman dan pemulangan perkakasan ICT mesti direkodkan. <p>b. Bagi perkakasan ICT yang dibawa keluar dari premis JKDM, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan JKDM:</p> <ul style="list-style-type: none"> i. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan ii. penyimpanan atau penempatan perkakasan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian. 			Semua
7.7.6 Pelupusan			
<p>Aset ICT yang hendak dilupuskan perlu melalui tatacara pelupusan yang berkuatkuasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan JKDM:</p> <ul style="list-style-type: none"> a. Semua kandungan di dalam perkakasan ICT khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui <i>shredding</i>, <i>grinding</i>, <i>degauzing</i> atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c. Untuk maklumat lanjut, sila rujuk: "Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan". 			Semua
7.7.7 Clear Desk dan Clear Screen			
<ul style="list-style-type: none"> a. Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. b. <i>Clear Desk dan Clear Screen</i> bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada di atas meja 			Semua
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	25 daripada 49



Item/Aktiviti	Tanggungjawab
<p>atau di paparan skrin apabila anggota JKDM tidak berada di tempatnya.</p> <p>c. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:</p> <ul style="list-style-type: none">i. Gunakan kemudahan kata laluan <i>screen saver</i> atau log keluar (logout) apabila meninggalkan komputer; danii. bahan-bahan sensitif hendaklah disimpan di dalam laci atau kabinet fail yang berkunci.	
7.8 Keselamatan Persekitaran	
<p>Objektif: Melindungi aset ICT JKDM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan.</p>	
7.8.1 Kawalan Persekitaran	
<p>Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, mengubahsuai atau pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil:</p> <ul style="list-style-type: none">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; dang. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan	Semua

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	26 daripada 49



Item/Aktiviti	Tanggungjawab
dan tindakan sekiranya perlu.	
7.8.2 Bekalan Kuasa	
<p>a. Semua perkakasan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan kuasa yang sesuai hendaklah disalurkan kepada perkakasan ICT.</p> <p>b. Peralatan sokongan seperti UPS (<i>Uninterruptable Power Supply</i>) dan penjana (<i>generator</i>) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan.</p> <p>c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.</p>	Penyenggara Bangunan/ CTM
7.8.3 Prosedur Kecemasan	
<p>a. Keadaan kecemasan seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan JKDM yang dilantik.</p>	Semua
7.9 Pengurusan Prosedur Operasi	
Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.	
7.9.1 Pengendalian Prosedur	
<p>a. Semua prosedur keselamatan ICT yang diwujudkan dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal.</p> <p>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.</p> <p>c. Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.</p>	Semua
7.9.2 Kawalan Perubahan	
<p>a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik</p>	Semua

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	27 daripada 49



Item/Aktiviti	Tanggungjawab
<p>sistem/aset ICT terlebih dahulu.</p> <p>b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan.</p> <p>c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan.</p> <p>d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja ataupun tidak.</p>	

7.9.3 Prosedur Pengurusan Insiden

<p>a. Langkah kawalan berikut hendaklah dilakukan bagi memastikan insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan. Prosedur pelaporan insiden keselamatan ICT berdasarkan :</p> <ul style="list-style-type: none">i. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; danii. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam <p>b. Mengenal pasti semua jenis insiden keselamatan ICT seperti:</p> <ul style="list-style-type: none">i. Percubaan (samada gagal atau berjaya) untuk mencapai sistem atau data tanpa kebenaran (probing);ii. Serangan kod jahat (malicious code) seperti virus, trojan horse, worms dan sebagainya;iii. Gangguan yang disengajakan (unwanted disruption) atau halangan pemberian perkhidmatan (denial of service);iv. Menggunakan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran (unauthorised access); danv. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak.vi. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar.vii. Maklumat dan kata laluan didapati hilang, disyaki hilang,	ICTSO
---	-------

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	28 daripada 49



Item/Aktiviti		Tanggungjawab	
dicuri, didedahkan kepada pihak-pihak yang tidak diberi kuasa. c. menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; d. menyimpan jejak audit dan memelihara bahan bukti; dan e. menyediakan tindakan pemulihan segera.			
7.10 Perancangan dan Penerimaan Sistem			
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.			
7.10.1 Perancangan Kapasiti			
a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.		Pentadbir Sistem dan ICTSO	
7.10.2 Penerimaan Sistem			
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.		Pemilik Sistem / CTM	
7.11 Perisian Berbahaya			
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan.			
7.11.1 Perlindungan dari Perisian Berbahaya			
a. Memasang sistem keselamatan seperti antivirus dan <i>Intrusion Detection System</i> (IDS) untuk mengesan perisian atau program berbahaya, mengikut prosedur penggunaan yang		Semua	
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	29 daripada 49



Item/Aktiviti	Tanggungjawab
<p>betul dan selamat.</p> <p>b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997.</p> <p>c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya.</p> <p>d. Mengemaskini antivirus dengan pattern antivirus yang terkini.</p> <p>e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diinginkan seperti kehilangan dan kerosakan maklumat.</p> <p>f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya.</p> <p>g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya.</p> <p>h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan.</p> <p>i. Memberi notis amaran mengenai ancaman keselamatan ICT seperti serangan virus.</p>	

7.12 Housekeeping

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

7.12.1 Penduaan (Backup)

<p>a. Bagi memastikan sistem dapat beroperasi semula setelah berlakunya bencana, salinan penduaan (<i>backup</i>) hendaklah dilakukan setiap kali konfigurasi berubah.</p> <p>b. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru.</p> <p>c. Membuat salinan penduaan (<i>backup</i>) ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan penduaan (<i>backup</i>) bergantung pada tahap kritikal maklumat.</p> <p>d. Menguji sistem penduaan (<i>backup</i>) sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.</p> <p>e. Salinan penduaan (<i>backup</i>) hendaklah direkodkan dan di</p>	<p>Semua</p>
---	--------------

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	30 daripada 49



Item/Aktiviti		Tanggungjawab	
simpan di lokasi yang berlainan dan selamat.			
7.12.2 Sistem Log			
a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna.		CTM	
b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera.			
c. Sekiranya wujud aktiviti-aktiviti tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.			
7.13 Pengurusan Rangkaian			
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.			
7.13.1 Kawalan Infrastruktur Rangkaian			
Infrastruktur rangkaian mesti dikawal dan diuruskan sebaik mungkin demi menjamin kelancaran sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu diambil tindakan:		CTM	
a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;			
b. perkakasan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;			
c. capaian kepada perkakasan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja;			
d. semua perkakasan mestilah melalui proses <i>Factory Acceptance Check</i> (FAC) semasa pemasangan dan konfigurasi;			
e. <i>Firewall</i> hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem;			
f. semua trafik rangkaian keluar dan masuk hendaklah melalui <i>firewall</i> di bawah kawalan JKDM;			
g. semua perisian <i>sniffer</i> atau <i>network analyser</i> adalah dilarang dipasang pada komputer pengguna kecuali mendapat			
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	31 daripada 49



Item/Aktiviti		Tanggungjawab	
<p>kebenaran ICTSO;</p> <p>h. memasang perisian <i>Intrusion Detection System</i> (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JKDM;</p> <p>i. memasang <i>Web Content Filter</i> pada <i>Internet Gateway</i> untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”;</p> <p>j. sebarang penyambungan rangkaian yang bukan di bawah kawalan JKDM hendaklah mendapat kebenaran Pengurus ICT</p> <p>k. semua pengguna hanya dibenarkan menggunakan rangkaian JKDM sahaja. Penggunaan modem peribadi adalah dilarang sama sekali.</p> <p>l. memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.</p>			
7.14 Pengurusan Media Storan			
Objektif: Melindungi media storan dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.			
7.14.1 Penghantaran dan Pemindahan Media Storan			
Penghantaran atau pemindahan media storan ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Bahagian/Negeri terlebih dahulu.		Semua	
7.14.2 Prosedur Pengendalian Media Storan			
<p>a. Melabelkan semua media storan mengikut tahap sensitiviti sesuatu maklumat seperti dalam Arahan Keselamatan.</p> <p>b. Menghad dan menentukan capaian media storan kepada pengguna yang sah sahaja.</p> <p>c. Menghadkan pengedaran data atau media storan untuk tujuan yang dibenarkan.</p> <p>d. Mengawal dan merekodkan aktiviti penyelenggaraan media storan bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan.</p>		Semua	
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	32 daripada 49



Item/Aktiviti	Tanggungjawab
e. Menyimpan semua media storan di tempat yang selamat. f. Media storan yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	
7.15 Keselamatan Komunikasi	
Objektif: Melindungi aset ICT melalui sistem komunikasi yang selamat.	
7.15.1 Internet	
a. Laman web yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan. b. Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan. c. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian/Negeri masing-masing sebelum dimuat naik ke Laman Web JKDM. d. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara. e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh JKDM. f. Pengguna boleh merujuk Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" untuk maklumat lanjut mengenai keselamatan Internet.	Semua
7.15.2 Mel Elektronik	
a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh JKDM hanya boleh digunakan untuk urusan rasmi sahaja. b. Setiap akaun e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh JKDM. c. Penggunaan akaun e-mel individu milik orang lain dan perkongsian akaun e-mel individu adalah dilarang. d. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum	Semua

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	33 daripada 49



Item/Aktiviti	Tanggungjawab
<p>penghantaran dilakukan.</p> <p>e. Pengguna hendaklah memastikan alamat e-mel penerima adalah betul sebelum penghantaran e-mel rasmi dibuat dan mengelak membuka e-mel daripada penghantar yang tidak diketahui atau diragui.</p> <p>f. Pengguna dinasihatkan menggunakan fail keipilan sekiranya perlu, tidak melebihi sepuluh (10) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan.</p> <p>g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel.</p> <p>h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan.</p> <p>i. E-mel yang telah diambil tindakan, tidak mempunyai nilai arkib dan tidak penting serta tidak diperlukan lagi bolehlah dihapuskan.</p> <p>j. Pengguna hendaklah memastikan tarikh dan masa sistem komputer adalah tepat.</p> <p>k. Pengguna boleh merujuk Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" untuk maklumat lanjut mengenai keselamatan e-mel.</p>	
7.16 Kawalan Capaian	
Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT JKDM.	
7.16.1 Keperluan Polisi	
Setiap capaian kepada sistem dan maklumat hendaklah direkod dan dikemaskinikan mengikut polisi yang telah ditetapkan dan dikawal mengikut keperluan keselamatan serta fungsi kerja pengguna yang berbeza.	CTM

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	34 daripada 49



Item/Aktiviti		Tanggungjawab
7.17 Pengurusan Capaian Pengguna		
Objektif: Mengawal capaian pengguna ke atas aset ICT JKDM.		
7.17.1 Akaun Pengguna		
<p>a. Semua pengguna baru hendaklah memohon akaun pengguna secara rasmi kepada Pemilik sistem /Pentadbir sistem.</p> <p>b. Akaun pengguna yang tidak aktif selama 3 bulan akan dibekukan dan dimansuhkan selepas bulan keempat. Pengecualian akan diberikan kepada pengguna yang memaklumkan kepada Pemilik sistem/Pentadbir sistem berkenaan keperluan akaun masing-masing.</p> <p>c. Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan dan perlu mematuhi langkah-langkah berikut:</p> <ul style="list-style-type: none">i. Akaun pengguna mestilah unik;ii. akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian berdasarkan keperluan pengguna tersebut yang telah ditentukan oleh Ketua Bahagian/Negeri masing-masing. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;iii. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; daniv. penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. <p>d. Pentadbir sistem boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:</p> <ul style="list-style-type: none">i. Bertukar bidang tugas kerja;ii. bertukar ke agensi lain;iii. bersara; atauiv. ditamatkan perkhidmatan.	Semua	
7.17.2 Pengurusan Kata laluan		
<p>a. Amalan terbaik serta prosedur yang ditetapkan oleh JKDM dalam pengurusan kata laluan adalah seperti berikut:</p> <ul style="list-style-type: none">i. Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun;	Semua	

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	35 daripada 49



Item/Aktiviti	Tanggungjawab
<ul style="list-style-type: none"> ii. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; iii. Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan alphanumeric dan simbol khas. Contoh kata laluan yang baik adalah “yw23#!y3ix8p”. iv. Kata laluan hendaklah diingat dan tidak didedahkan dengan apa cara sekalipun; v. Kata laluan <i>windows</i> dan <i>screen saver</i> hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; vi. Kata laluan hendaklah tidak dipaparkan semasa <i>input</i>, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; vii. Pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan disetkan semula perlu dikuatkuasakan; viii. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; ix. Had maksima masa sesi tidak aktif (<i>idle time</i>) selepas login sistem sah adalah ditetapkan selama tiga puluh (30) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; x. Kata laluan hendaklah ditukar selepas 6 bulan atau selepas tempoh masa yang bersesuaian; dan xi. Mengelakkan penggunaan semula kata laluan yang baru digunakan. 	

7.17.3 Jejak Audit

<ul style="list-style-type: none"> a. Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. b. Aktiviti jejak audit mengandungi: <ul style="list-style-type: none"> 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 	<p>Pentadbir Sistem</p>
--	-------------------------

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	36 daripada 49



Item/Aktiviti		Tanggungjawab	
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.			
7.18 Kawalan Capaian Sistem dan Aplikasi			
Objektif: Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.			
7.18.1 Sistem Maklumat dan Aplikasi			
Capaian sistem dan aplikasi di JKDM adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi:		CTM	
<ul style="list-style-type: none"> a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; c. memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d. menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; dan e. memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah. 			
7.19 Perkakasan ICT Mudah Alih			
Objektif: Memastikan keselamatan maklumat apabila menggunakan kemudahan atau perkakasan ICT mudah alih.			
20.1 Penggunaan Perkakasan ICT Mudah Alih			
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	37 daripada 49



Item/Aktiviti	Tanggungjawab
<p>a. Aktiviti keluar masuk penggunaan Perkakasan ICT mudah alih hendaklah direkodkan mengikut tatacara pengurusan aset yang sedang berkuatkuasa. Ini bertujuan bagi mengesan kehilangan atau pun kerosakan perkakasan ICT mudah alih.</p> <p>b. Pengguna adalah bertanggungjawab ke atas sebarang kehilangan atau kerosakan perkakasan ICT yang di pinjam.</p> <p>c. Perkakasan ICT mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.</p> <p>d. Untuk maklumat lanjut, sila rujuk: “Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk “Tatacara Pengurusan Aset Alih Kerajaan”.</p>	Semua

7.20 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

7.20.1 Keperluan Keselamatan

<p>a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat.</p> <p>b. Ujian keselamatan hendaklah dijalankan ke atas:</p> <ul style="list-style-type: none"> i. Sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan; ii. sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan tanpa ralat; dan iii. sistem output untuk memastikan data yang telah diproses adalah tepat. <p>c. 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.</p>	Pemilik Sistem dan CTM
---	------------------------

7.21 Fail Sistem

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	38 daripada 49



Item/Aktiviti		Tanggungjawab	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.			
7.21.1 Kawalan Fail Sistem			
<p>a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh pentadbir sistem atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan.</p> <p>b. Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji.</p> <p>c. Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan</p> <p>d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.</p>		Pentadbir Sistem	
7.22 Pembangunan dan Proses Sokongan			
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.			
7.22.1 Kawalan Perubahan			
Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum digunakan.		Pentadbir Sistem	
7.23 Kesenambungan Perkhidmatan			
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.			
7.23.1 Pelan Kesenambungan Perkhidmatan			
<p>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 dan perkara-perkara berikut perlu diberi perhatian:</p> <p>a. Mengenal pasti semua tanggungjawab dan prosedur</p>		Pengurus ICT	
CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	39 daripada 49



Item/Aktiviti	Tanggungjawab
<p>kecemasan atau pemulihan;</p> <p>b. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangkamasa yang telah ditetapkan;</p> <p>c. Mendokumentasikan proses dan prosedur yang telah dipersetujui;</p> <p>d. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;</p> <p>e. Membuat penduaan; dan</p> <p>f. Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.</p>	

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 2.0	11/06/2013	40 daripada 49



Perkara 8.0 - Pematuhan

Item/Aktiviti	Tanggungjawab
8.1 Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan pematuhan kepada Dasar ICT JKDM.	
8.1.1 Pematuhan Dasar	
a. Setiap pengguna di JKDM hendaklah membaca, memahami dan mematuhi Dasar ICT JKDM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. b. Semua aset ICT di JKDM termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	Semua
8.1.2 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di JKDM adalah seperti di Lampiran 4.	Semua
8.2 Tindakan Tatatertib	
Objektif: Meningkatkan kesedaran dan pematuhan ke atas Dasar ICT JKDM.	
8.2.1 Pelanggaran Dasar	
Pelanggaran Dasar ICT JKDM akan dikenakan tindakan tatatertib.	Semua

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 1.0	11/06/2013	41 daripada 49



Garis Panduan Mengenai Tatacara Memohon Kelulusan Projek ICT Jabatan Kastam Diraja Malaysia

(Berdasarkan Surat Pekeliling Am Bil 1 Tahun 2009 - Garis Panduan Mengenai Tatacara Memohon Kelulusan Teknikal Projek ICT Agensi Kerajaan dan Surat Pekeliling ICT JKDM Bil 1 Tahun 2013 - Garis Panduan Mengenai Tatacara Memohon Kelulusan Projek ICT Jabatan Kastam Diraja Malaysia)

1. Skop projek ICT yang perlu mendapatkan kelulusan JPICT adalah seperti berikut:

(a) Projek Baru

Projek baru bermaksud projek pengkomputeran yang melibatkan salah satu **atau** gabungan aktiviti-aktiviti perolehan perkakasan, perisian dan/atau perkhidmatan ICT, untuk membangunkan projek ICT agensi.

- i. Perkakasan komputer yang dimaksudkan merangkumi semua jenis alat-alat input/output (contoh: pencetak dan pengimbas), pemprosesan, storan data, peralatan rangkaian dan multimedia (contoh: persidangan video (*video conferencing*)) kecuali alat-alat seperti komponen alat ganti, barang pakai habis (*consumable item*), aksesori dan perabut komputer.
- ii. Perisian komputer yang dimaksudkan merangkumi semua jenis perisian sistem dan perisian aplikasi. Perisian sistem merangkumi sistem operasi, pangkalan data dan perisian bagi membangunkan sistem. Perisian aplikasi adalah sistem aplikasi yang dibangunkan ataupun pakej sedia ada (off-the-shelf) untuk kegunaan tertentu (contoh: Sistem Perakaunan, Sistem Personel dan Sistem Pengurusan Inventori) dan perisian yang digunakan untuk menyokong kerja-kerja harian seperti penyediaan dokumen.
- iii. Perkhidmatan ICT yang dimaksudkan merangkumi semua jenis perkhidmatan teknikal yang diperolehi daripada syarikat perunding swasta, kontraktor dan syarikat-syarikat lain yang berkaitan seperti pembangunan sistem, pemasangan sistem, infrastruktur rangkaian, talian internet, web hosting, kemasukan data, pemindahan data, migrasi sistem, pemulihan data, langganan maklumat dalam talian dan seumpamanya.

(b) Peningkatan Sistem

Peningkatan sistem bermaksud mempertingkatkan keupayaan perkakasan, perisian, rangkaian dan/atau perkhidmatan ICT. Contoh peningkatan sistem adalah seperti peningkatan perkakasan dari segi konfigurasi dan kapasiti. Peningkatan perisian merangkumi pengemaskinian fungsi-fungsi di dalam sistem ICT sedia ada kepada tahap yang lebih baik. Contoh peningkatan rangkaian adalah seperti peningkatan saiz jalur lebar (*bandwidth*), peluasan rangkaian dan seumpamanya. Peningkatan perkhidmatan pula merangkumi pertambahan skop perkhidmatan yang sedia ada.

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 1.0	11/06/2013	42 daripada 49



(c) Pertambahan Peralatan

Pertambahan peralatan bermaksud menambahkan bilangan bagi mana-mana perkara di bawah kategori perkakasan, perisian dan/atau rangkaian bagi projek ICT sedia ada.

(d) Perluasan Sistem

Perluasan (*roll-out*) sistem bermaksud memperkembangkan pelaksanaan projek ICT daripada lokasi sedia ada ke lokasi-lokasi lain atau dengan menambah bilangan pengguna di lokasi yang sama ataupun kedua-duanya sekali.

2. Had nilai projek ICT yang memerlukan kelulusan JPICT adalah seperti berikut:

(a) Bagi Permohonan Projek ICT yang **MELIBATKAN** pembangunan Sistem Aplikasi :-

- i. Semua projek ICT yang bernilai hingga RM50,000.00 hendaklah mendapat kelulusan daripada JPICT JKDM sahaja dan kelulusan boleh dipertimbangkan secara luar mesyuarat;
- ii. Semua projek ICT yang bernilai melebihi RM50,000.00 hingga RM200,000.00 hendaklah mendapat kelulusan daripada JPICT JKDM sahaja;
- iii. Semua projek ICT yang bernilai melebihi RM200,000.00 hingga RM500,000.00 hendaklah mendapat kelulusan daripada JPICT JKDM dan akan dikemukakan untuk mendapat kelulusan teknikal daripada JPICT Kementerian Kewangan (MoF); dan
- iv. Hanya projek ICT yang bernilai melebihi RM500,000 dan telah diluluskan oleh JPICT MOF akan dikemukakan untuk kelulusan teknikal JTICT MAMPU.

(b) Bagi Permohonan Projek ICT yang TIDAK MELIBATKAN pembangunan Sistem Aplikasi :-

- i. Semua projek ICT yang bernilai hingga RM50,000.00 hendaklah mendapat kelulusan daripada JPICT Jabatan sahaja dan kelulusan boleh dipertimbangkan secara luar mesyuarat;
- ii. Semua projek ICT yang bernilai melebihi RM50,000.00 hingga RM500,000.00 hendaklah mendapat kelulusan daripada JPICT Jabatan sahaja;
- iii. Semua projek ICT yang bernilai melebihi RM500,000.00 hingga RM3 juta hendaklah mendapat kelulusan daripada JPICT JKDM dan akan dikemukakan untuk mendapat kelulusan teknikal daripada JPICT MoF; dan
- iv. Hanya projek ICT yang bernilai melebihi RM3 juta dan telah diluluskan oleh JPICT MOF akan dikemukakan untuk kelulusan teknikal JTICT

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 1.0	11/06/2013	43 daripada 49



MAMPU.

3. Semua perolehan ICT hendaklah berdasarkan kepada Pelan Strategik ICT (ISP). JTICT MAMPU dan JPICT MOF akan memberi keutamaan kepada projek ICT yang telah dirancang di dalam ISP.
4. Untuk projek-projek yang diluluskan oleh JPICT, Bahagian/Negeri yang memohon perlu mengemukakan laporan kemajuan kepada Urusetia JPICT setiap enam (6) bulan dari tarikh kelulusan sehingga projek selesai.
5. Tempoh sah laku kelulusan JPICT adalah selama tiga (3) tahun dari tarikh surat kelulusan. Sekiranya projek yang diluluskan tidak dilaksanakan dalam tempoh tersebut, Bahagian/Negeri hendaklah memohon semula kelulusan JPICT sebelum melaksanakan projek ICT tersebut.
6. Semua Bahagian/Negeri hendaklah mematuhi garis panduan yang dikemukakan di dalam memohon kelulusan teknikal perolehan ICT daripada JPICT.

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 1.0	11/06/2013	44 daripada 49



Lampiran 2

Garis panduan untuk Pembangunan Sistem Aplikasi dan Pangkalan Data

1. Keperluan pengguna secara terperinci daripada pengguna adalah perlu disediakan sebelum proses pembangunan sistem aplikasi dapat dimulakan.
2. Bahagian (pengguna utama) hendaklah memperuntukkan seorang atau lebih kakitangan sebagai wakil tetap yang dapat meluangkan masa yang cukup sepanjang proses pembangunan dan kerja-kerja berkaitan dengan projek.
3. Bagi aplikasi yang besar (projek pengkomputeran Bahagian), Jawatankuasa Teknikal dan Jawatankuasa Pemandu di peringkat Bahagian perlu diwujudkan.
4. Bagi sistem aplikasi yang melibatkan pelbagai Bahagian, maka setiap Bahagian perlu mempunyai wakil tetap bagi menganggotai Jawatankuasa Teknikal dan Jawatankuasa Pemandu.
5. Cadangan Sistem (*System Proposal*) perlu dibentangkan kepada pengguna untuk ulasan dan persetujuan serta ditandatangani oleh pengguna.
6. Bagi sistem yang melibatkan fungsi dan prosedur tertentu, *subject matter expert* perlu dilibatkan dalam merekabentuk kawalan yang berkaitan dengan *subject matter* (contoh: Bagi sistem yang melibatkan fungsi dan prosedur kewangan, Akauntan perlu dilibatkan dalam merekabentuk kawalan yang berkaitan dengan perakaunan).
7. Pengujian dan prosedur penerimaan sistem di setiap peringkat (*unit test*, *component test* dan *integration test*) perlu dibuat.
8. Pengguna perlu menandatangani Penerimaan Sementara dan Penerimaan Akhir sistem aplikasi.
9. Pelaksanaan kawalan keselamatan ICT dalam aplikasi adalah perlu bagi menghalang capaian yang tidak sah, ubahsuaian, penyebaran maklumat dan kerosakan maklumat.
10. *Source code* dan hak cipta bagi sesuatu aplikasi yang dibangunkan secara dalaman ataupun secara bersama dengan pembekal perlu dinyatakan dalam kontrak sebagai Hak Kerajaan Malaysia.

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 1.0	11/06/2013	45 daripada 49



11. Bagi aplikasi yang dibangunkan oleh pembekal, klausa mengenai pemindahan teknologi (*Transfer of Technology*) hendaklah dinyatakan dalam dokumen kontrak.

12. Pengarah setiap Bahagian yang terlibat akan mempengerusikan mesyuarat kemajuan projek bagi tujuan pemantauan.

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 1.0	11/06/2013	46 daripada 49



Lampiran 3

Bil	Nama	Alamat Pejabat	No Tel
1	Cawangan Teknologi Maklumat Putrajaya	Jabatan Kastam Diraja Malaysia, Cawangan Tekonologi Maklumat, Aras 5 Utara, 62596 Putrajaya.	No. Tel: 03-88822586/2589 E-mel: teknikal.ctmhq@customs.gov.my.
2	Cawangan Teknologi Maklumat KLIA	Cawangan Teknologi Maklumat, Aras 3, Kompleks Kastam Kargo, Jalan KLIA S3, 64000 KLIA, Sepang, Selangor	03-87874906
3	Cawangan Teknologi Maklumat Selangor	1) Aras 3, Wisma Kastam Pelabuhan Utara, Pelabuhan Klang, 42000 Selangor	03-31761375
		2) Aras Bawah, Wisma Kastam Pelabuhan Barat, P44&45, Kompleks Kastam, Jalan Perigi Nanas 7/2, Taman Perindustrian Pulau Indah, 42920 Pulau Indah, Selangor	03-31693606 (Direct Line) 03-31693607 (En. Saad) 03-31693610 (Cik Faizah) 03-31693611 (En. Rizal)
5	Unit Teknologi Maklumat, Johor	Bangunan KSAB, Gelang Patah, Johor	07-5133008

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 1.0	11/06/2013	47 daripada 49



SENARAI PERUNDANGAN DAN PERATURAN

- (a) Arahan Keselamatan;
- (b) Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
- (c) Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002;
- (d) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
- (e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
- (f) Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
- (g) Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
- (h) Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006;
- (i) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
- (j) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
- (k) Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
- (l) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
- (m) Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
- (n) Akta Tandatangan Digital 1997;
- (o) Akta Rahsia Rasmi 1972;
- (p) Akta Jenayah Komputer 1997;
- (q) Akta Hak Cipta (Pindaan) Tahun 1997;
- (r) Akta Komunikasi dan Multimedia 1998;
- (s) Perintah-Perintah Am;

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 1.0	11/06/2013	48 daripada 49



- (t) Arahan Perbendaharaan;
- (u) Arahan Teknologi Maklumat 2007;
- (v) Garis Panduan Keselamatan MAMPU 2004;
- (w) Standard Operating Procedure (SOP) ICT MAMPU;
- (x) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
- (y) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesenambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.

CETAKAN	REVISI	TARIKH	M/SURAT
PERTAMA	Versi 1.0	11/06/2013	49 daripada 49