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(1)
Tarikh : 25 Mei 2010

Semua Pengarah Ibu Pejabat

Semua Pengarah Kastam Negeri

Pengarah AKMAL

Pemungut Cukai Kastam Persekutuan, Singapura

SURAT PEKELILING ICT JABATAN KASTAM DIRAJA MALAYSIA
BILANGAN 1 TAHUN 2010

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 memenuhj keperluan penguatkuasaan, kawa!an dan langkah-langkah yang menyeluruh untuk melindungi aset ICT kerajaan. Semua agensi kerajaan, dipertanggungjawabkan untuk memastikan Rangka Dasar Keselamatan ICT Kerajaan di!aksana dan dipatuhi.

3. Selaras dengan pekeliling 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 1/2010 yang telah diadakan pada 22 Februari 2010 telah bersetuju untuk mengguna pakai dan menguatkuasakan peraturan-peraturan yang ditetapkan di dalam surat pekeliling 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(-)421/10(36) bertarikh 11 Januari 2007 adalah dibatalkan.

Sekian, terima kasih.

"BERKHIDMAT UNTUK NEGARA"

(DATO' SRI HJ IBRAHIM B HJ JAAPAR)
Ketua Pengarah Kastam
Malaysia.

s.k.

TKPK (Penguatkuasaan/Pematuhan)

TKPK (Perkastaman/Cukai Dalam Negeri)

TKPK (Pengurusan)

Pen. KPK (Bahagian Penguatkuasaan)

KERAJAAAN MALAYSIA

DASAR ICT

JABATAN KASTAM DIRAJA MALAYSIA

Jabatan Kastam Diraja Malaysia
Kementerian Kewangan
Mei 2010

Dikelilingkan kepada

Semua Pengarah Ibu Pejabat

Semua Pengarah Kastam Negeri

Pengarah AKMAL

Pemungut Cukai Kastam Persekutuan, Singapura

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*	-	Ketua Keselamatan ICT JKDM – Ketua Unit Teknikal CTM
JKDM	-	Jabatan Kastam Diraja Malaysia
Kehilangan	-	Aset yang tiada lagi dalam simpanan disebabkan oleh kecurian, kemalangan, kebakaran, bencana alam, kesusutan, penipuan atau kecuaian 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

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
Pelupusan	-	Satu proses untuk mengeluarkan aset dari milikan, kawalan, simpanan dan rekod mengikut kaedah yang ditetapkan
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 memberi perkhidmatan berpusat

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, menyedia, 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

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 Komputer, Pegawai Keselamatan ICT (ICTSO), semua Pengarah Bahagian serta semua Pengarah Kastam Negeri.	KPK
1.2 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna JKDM.	CTM
1.3 Penyelenggaraan Dasar	
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. Berikut adalah prosedur berhubung dengan penyelenggaraan Dasar ICT JKDM: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan untuk persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) JKDM; c. Perubahan yang telah dipersetujui oleh JPICT JKDM dimaklumkan kepada semua pengguna; dan d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.	CTM
1.4 Pengecualian	
Dasar ICT JKDM adalah terpakai kepada semua pengguna ICT JKDM dan tiada pengecualian diberikan	Semua

Perkara 2.0 - Organisasi ICT

Item/Aktiviti	Tanggungjawab
2.1 Ketua Pengarah Kastam Malaysia	
Peranan dan tanggungjawab KPK adalah seperti berikut: 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; dan d. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan dalam Dasar ICT JKDM.	KPK
2.2 Ketua Pegawai Maklumat (CIO)	
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.	CIO
2.3 Pengurus Komputer	
Timbalan Pengarah Cawangan Teknologi Maklumat (CTM) adalah merupakan Pengurus Komputer JKDM. Peranan dan tanggungjawab Pengurus Komputer adalah seperti berikut: a. Merangka, merumus dan menguatkuasa Dasar ICT JKDM; b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan JKDM; c. menentukan kawalan akses semua pengguna terhadap aset ICT JKDM; dan d. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT JKDM.	TPh CTM
2.4 Pegawai Keselamatan ICT (ICTSO)	
Ketua Unit Teknikal CTM adalah merupakan ICTSO JKDM. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Mengurus keseluruhan program-program keselamatan ICT	ICTSO

Item/Aktiviti	Tanggungjawab
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 memaklumkannya 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. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
2.5 Pentadbir Sistem ICT	
Pentadbir Sistem ICT terdiri daripada pegawai JKDM yang mengurus tadbir samaada sistem rangkaian atau sistem aplikasi (contoh: Sistem Maklumat Kastam, emel, laman web dan sebagainya). Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: 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 pencerobohan dan pengubahsuaian data tanpa kebenaran dan	CTM

Item/Aktiviti	Tanggungjawab
membatalkan atau memberhentikannya 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

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. b. Bahagian / Negeri hendaklah memohon secara rasmi kepada CTM 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.**	Semua
3.1.2 Pelupusan Perkakasan dan Perisian ICT	
a. Tatacara pelupusan perkakasan dan perisian ICT hendaklah merujuk kepada pekeliling yang sedang berkuatkuasa. b. Bahagian / Negeri hendaklah memohon secara rasmi kepada Unit Pengurusan Aset, 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”.	Semua
3.2 Peruntukan/Penggunaan Perkakasan dan Perisian ICT	
3.2.1 Pencetak	
Pencetak perlu diguna secara *‘pool’* dengan nisbah yang difikirkan sesuai untuk kelancaran kerja dan jenis kerja yang dilakukan seperti kerahsiaan maklumat, kedudukan tempat dan proses kerja.	Semua
3.2.2 Komputer	
a. Setiap pegawai kanan Gred 41 ke atas layak diperuntukkan 1 unit komputer mengikut keperluan dan tugasan yang sesuai. b. Pegawai JKDM yang bekerja mengikut syif hendaklah menggunakan komputer secara gunasama. c. Komputer riba (*Notebook)* yang dibekalkan oleh Ibu Pejabat	Semua

Item/Aktiviti	Tanggungjawab
JKDM hendaklah digunakan secara gunasama. d. Pegawai yang membuat peminjaman perkakasan ICT gunasama haruslah bertanggungjawab sepenuhnya terhadap keselamatan perkakasan ICT berkenaan.	
3.2.3 Penyelenggaraan Perkakasan dan Perisian ICT	
a. Penyelenggaraan perkakasan ICT yang dibekalkan oleh Ibu Pejabat JKDM ke Bahagian/Negeri perlulah diselaras oleh CTM bagi memudahkan pemantauan dan inventori. b. Aduan tentang masalah-masalah yang dihadapi dalam penggunaan ICT perlu diajukan kepada Meja Bantuan CTM melalui talian telefon 03-88822586 serta mengisi borang kerosakan atau emel kepada helpdesk@customs.gov.my. c. Senarai perisian ICT yang disokong oleh CTM bagi perkhidmatan pemasangan, penyelenggaraan dan latihan adalah seperti berikut: i. MS Office yang terdiri daripada: • MS Word • MS Excel • MS Powerpoint ii. Open Office yang terdiri daripada: • writer • calc • impress iii. Internet browser yang terdiri daripada: • Internet Explorer • Mozilla Firefox • Google Chrome iv. Emel d. Perkhidmatan bagi perisian ICT selain daripada yang tersebut di atas hanya akan diberikan sekiranya ada tenaga kepakaran di CTM.	Semua

Perkara 4.0 - Dasar Pengurusan Emel dan Penggunaan Internet

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

Item/Aktiviti	Tanggungjawab
n. Cawangan Perkhidmatan dan Latihan Ibu Pejabat hendaklah memaklumkan kepada pentadbir sistem emel dengan segera mengenai pegawai yang berpindah keluar dari JKDM atau pegawai yang telah tamat perkhidmatan dengan jabatan secara wajib/pilihan. o. Pengguna yang telah tidak wujud akan dihapus ID dan capaiannya kepada emel dalam masa 1 bulan. p. Pengguna hendaklah sentiasa mengimbas fail bagi memastikan fail yang akan dihantar melalui kepilan *(attachment)* bebas dari virus. q. Aktiviti *spamming*, penyebaran virus, bahan-bahan negatif, surat berantai dan promosi-promosi perniagaan adalah dilarang. Jika didapati aktiviti ini dilakukan oleh pengguna, akaun emel mereka akan dinyahaktifkan tanpa sebarang notis. r. Pentadbir Sistem berhak memasang sebarang jenis perisian atau perkakasan penapisan emel dan virus yang difikirkan sesuai dan boleh menggunakannya untuk mencegah, menapis, menyekat atau menghapuskan mana-mana emel yang disyaki mengandungi virus atau berunsur *spamming* daripada memasuki komputer. s. Menyebar perisian cetak rompak atau maklumat berbau politik, hasutan atau perkauman atau apa-apa maklumat yang menjejaskan reputasi JKDM dan Perkhidmatan Awam melalui kemudahan emel JKDM adalah dilarang. t. Pengguna dilarang melakukan pencerobohan atau percubaan untuk menceroboh masuk ke mana-mana akaun pengguna lain. u. Pihak KPK/CIO/Pengurus ICT/ICTSO/Pentadbir Sistem boleh memantau semua emel JKDM jika perlu tanpa mendapat kebenaran pengguna.	
4.2 Penggunaan Internet	
a. Pengguna yang menggunakan aplikasi atas talian dan laman web adalah bertanggung jawab sepenuhnya ke atas maklumat yang dikunci masuk *(key-in)* serta capaian yang dilakukan. b. Pengguna tidak dibenar menyumbangkan perkara-perkara bertentangan dengan Perintah Am Kerajaan kepada mana-mana laman web tanpa kebenaran Ketua Jabatan. c. Pengguna tidak dibenarkan membuat capaian kepada bahan-bahan terlarang dan menggunakan sebarang perisian judi atau	Semua

Item/Aktiviti	Tanggungjawab
seumpamanya dengan menggunakan kemudahan pejabat. d. Capaian laman web yang berbentuk hiburan, *chatting,* permainan komputer *online*, radio *online* dan *video streaming* yang membebankan rangkaian JKDM adalah tidak dibenarkan semasa waktu pejabat. e. Pengguna tidak dibenarkan melanggan kepada mana-mana *mailing list* dengan menggunakan emel rasmi jabatan yang tidak berkaitan dengan tugas. f. Pengguna tidak dibenarkan membuat capaian ke Laman Rangkaian Sosial seperti *Facebook* dan *Twitter* semasa waktu pejabat kecuali mendapat kelulusan pihak CTM/Pengarah Kastam Negeri. g. Capaian ke internet dimestikan melalui tapisan *firewall.* Pengguna tidak dibenarkan menginstalasi apa-apa perisian untuk melepasi tapisan *firewall*. h. Aktiviti *chatting* adalah tidak dibenarkan ketika waktu pejabat. i. Aktiviti muat turun (download) atau muat naik (upload) sebarang perisian cetak rompak adalah dilarang. j. Pengguna tidak dibenarkan melayari laman-laman yang tidak berkaitan dengan tugas di waktu pejabat. k. Pentadbir Sistem Rangkaian di JKDM adalah bertanggungjawab untuk menjana laporan capaian rangkaian dan internet setiap pengguna kepada pihak pengurusan. l. Pentadbir Sistem Rangkaian berhak menyediakan dan memasang perisian penapisan isi kandungan internet. m. Pentadbir Sistem Rangkaian berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yang tidak sesuai. 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.	
4.3 Laman dan Aplikasi Web	
a. Semua maklumat yang hendak dimuatkan ke dalam laman web JKDM mestilah mendapat kelulusan Ketua Bahagian/Negeri. b. Maklumat yang terkandung dalam laman web adalah di bawah tanggungjawab Bahagian/Negeri masing-masing.	Semua

Item/Aktiviti	Tanggungjawab
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.	

Perkara 5.0 - Dasar Sistem Aplikasi dan Pangkalan Data

Item/Aktiviti	Tanggungjawab
5.1 Pembangunan Sistem Aplikasi Dan Pangkalan Data	
a. Bahagian/Negeri hendaklah memohon secara rasmi kepada CTM untuk membangunkan sesuatu sistem aplikasi yang melibatkan kos, untuk tujuan mendapatkan kelulusan daripada jawatankuasa-jawatankuasa ICT yang berkaitan berdasarkan tatacara seperti di **Lampiran 1**. b. Pembangunan sistem aplikasi secara *in-house* dan tidak melibatkan kos perlu dimaklumkan kepada CTM. Maklumat yang perlu dikemukakan antara lain seperti: • Tajuk Projek • Tujuan Projek • Keterangan Projek • Tempoh Pembangunan (Tarikh mula dan akhir) • Sasaran Pengguna • Kaedah Pelaksanaan (*standalone, web-based* dan sebagainya) 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 digunapakai. d. Sebarang pembangunan sistem aplikasi mestilah menggunapakai kod-kod yang standard di bawah *Data Dictionary* Sektor Awam (DDSA). e. Garispanduan untuk pembangunan sistem aplikasi dan pangkalan data adalah seperti di **Lampiran 2.**	Semua
5.2 Pelaksanaan Sistem Aplikasi	
a. Sesuatu sistem aplikasi perlu dimiliki oleh sesuatu Bahagian/Negeri yang mempunyai kepentingan terhadap sistem yang dibangunkan. b. Pemilik sistem aplikasi tersebut hendaklah melantik *champion* bagi melancarkan pelaksanaan sistem. *Champion* sekurang-kurangnya di peringkat Ketua Bahagian/Negeri. c. Pemilik sistem aplikasi perlu membuat pelaporan kepada	

Item/Aktiviti	Tanggungjawab
JPICT JKDM secara berkala bagi kemajuan mengenai pembangunan atau pelaksanaan sistem aplikasi tersebut. d. Pemilik sistem aplikasi hendaklah melantik pentadbir sistem aplikasi untuk tujuan penyelenggaraan sistem aplikasi tersebut 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. f. Pengguna sistem aplikasi yang telah tidak wujud akan dihapus ID dan capaiannya ke aplikasi dalam masa 1 bulan.	

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 mengguna rangkaian JKDM. c. Pengguna luar yang hendak menggunakan kemudahan rangkaian JKDM hendaklah mendapat kebenaran CTM.	Semua
6.2 Pengurusan Alamat IP	
a. Sebarang permohonan untuk menggunakan *static* 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. *Static* IP yang diberikan kepada pengguna tidak boleh digunakan untuk kepentingan sendiri. Sekiranya pengguna didapati menyalahgunakan *static* IP dengan menukar konfigurasi komputer kepada *server* 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 peralatan peribadi ke dalam rangkaian JKDM. c. Pengguna tidak dibenarkan memasang sebarang *access point* untuk capaian secara *wireless* ke dalam rangkaian JKDM. d. Pengguna tidak dibenarkan memutuskan/ menyambung sambungan kabel UTP pada mana-mana *port* dalam rak peralatan rangkaian tanpa kebenaran dari pihak CTM. e. Pengguna tidak dibenarkan menukar maklumat yang terdapat	Semua

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

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. b. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Cawangan Logistik / Pegawai Aset 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: • Rahsia Besar; • Rahsia; • Sulit; atau • Terhad	Semua
7.2.2 Pengendalian Maklumat	
a. 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;	Semua

Item/Aktiviti	Tanggungjawab
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. b. 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 dan mempunyai ciri-ciri keselamatan; 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; 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, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT JKDM.	
7.3.1 Tanggungjawab Pengguna Terhadap Keselamatan ICT	
a. Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak.	Semua

Item/Aktiviti	Tanggungjawab
b. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyedia dan memastikan perlindungan ke atas semua 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: 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. bBerlaku kejadian sistem yang luar biasa seperti kehilangan fail atau sistem kerap kali gagal; dan e. berlaku percubaan menceroboh, menyeleweng atau insiden-insiden yang tidak diingini. <u>Nota:</u> Sila rujuk Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan ICT" untuk keterangan lanjut.	Semua
7.5 Pembudayaan Keselamatan ICT	
Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.	
7.5.1 Program Pembudayaan Keselamatan ICT	
a. Setiap pengguna di JKDM perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-	ICTSO

Item/Aktiviti	Tanggungjawab
tugas dan tanggungjawab mereka. b. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT JKDM.	
7.6 Tindakan Tatatertib	
Objektif: Meningkat kesedaran dan pematuhan ke atas Dasar ICT JKDM.	
7.6.1 Pelanggaran Dasar	
Pelanggaran Dasar ICT JKDM akan dikenakan tindakan tatatertib.	Semua
7.7 Keselamatan Kawasan	
Objektif: Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.	
7.7.1 Kawasan Larangan	
a. 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 JKDM adalah Pusat Data JKDM. Akses kepada kawasan tersebut hanya kepada pegawai-pegawai yang diberi kuasa sahaja. 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.	Semua
7.8 Keselamatan Perkakasan ICT	
Objektif: Melindung peralatan dan maklumat.	
7.8.1 Perkakasan ICT	
Secara umumnya perkakasan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu. Setiap pengguna	Semua

Item/Aktiviti	Tanggungjawab
hendaklah: 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.	
7.8.2 Media Storan	
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: 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; dan e. pengguna mesti memastikan peranti storan *(disket, cd* atau *thumb drive)* yang menyimpan dokumen terhad disimpan di tempat yang selamat.	Semua
7.8.3 Kabel Rangkaian	
Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; dan b. melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan.	Semua

Item/Aktiviti	Tanggungjawab
7.8.4 Penyelenggaraan Perkakasan ICT	
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
7.8.5 Peminjaman Perkakasan ICT untuk Kegunaan di Luar Pejabat	
a. Perkakasan ICT yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan: 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. 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: i. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan ii. penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
7.8.6 Pelupusan	
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: a. Semua kandungan di dalam perkakasan ICT khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding,*	Semua

Item/Aktiviti	Tanggungjawab
degauzing 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".	
7.8.7 *Clear Desk* dan *Clear Screen*	
a. Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. b. *Clear Desk dan Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada di atas meja atau di paparan skrin apabila anggota JKDM tidak berada di tempatnya. c. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: i. Gunakan kemudahan password screen saver (Sila rujuk **Lampiran 3** untuk clear screen setting) atau log keluar (logout) apabila meninggalkan komputer; dan ii. bahan-bahan sensitif hendaklah disimpan di dalam laci atau kabinet fail yang berkunci. Nota: Sumber Rujukan: "Dokumen Dasar Keselamatan ICT MAMPU Versi 5.3 bertarikh 13 Mei 2010".	Semua
7.9 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT JKDM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
7.9.1 Kawalan Persekitaran	
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	Semua

Item/Aktiviti	Tanggungjawab
persekitaran, langkah-langkah berikut hendaklah diambil: a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	
7.9.2 Bekalan Kuasa	
a. Semua perkakasan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan kuasa yang sesuai hendaklah disalurkan kepada perkakasan ICT. b. Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan. c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Penyenggara Bangunan/ CTM
7.9.3 Prosedur Kecemasan	
a. Keadaan kecemasan seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan JKDM.	Semua
7.10 Pengurusan Prosedur Operasi	

Item/Aktiviti	Tanggungjawab
Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.	
7.10.1 Pengendalian Prosedur	
a. Semua prosedur keselamatan ICT yang diwujudkan dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal. b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti. c. Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	Semua
7.10.2 Kawalan Perubahan	
a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu. b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan. c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja ataupun tidak.	Semua
7.10.3 Prosedur Pengurusan Insiden	
Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan, prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: a. Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti	ICTSO

Item/Aktiviti	Tanggungjawab
dan pengubahsuaian perisian tanpa kebenaran; b. menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c. menyimpan jejak audit dan memelihara bahan bukti; dan d. menyediakan tindakan pemulihan segera.	
7.11 Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
7.11.1 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 ICT dan ICTSO
7.11.2 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pemilik Sistem / CTM
7.12 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan.	
7.12.1 Perlindungan dari Perisian Berbahaya	
a. Memasang sistem keselamatan seperti antivirus dan *Intrusion Detection System* (IDS) untuk mengesan perisian atau program berbahaya, mengikut prosedur penggunaan yang	Semua

Item/Aktiviti	Tanggungjawab
betul dan selamat. b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997. c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya. d. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat. e. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya. f. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya. g. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan. h. Memberi notis amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
7.13 *Housekeeping*	
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.	
7.13.1 Penduaan	
a. Bagi memastikan sistem dapat beroperasi semula setelah berlakunya bencana, salinan penduaan hendaklah dilakukan setiap kali konfigurasi berubah. b. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru. c. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi. d. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan. e. Salinan penduaan hendaklah direkodkan dan di simpan di *off site*.	Semua

Item/Aktiviti	Tanggungjawab
7.13.2 Sistem Log	
a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna. b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera. c. Sekiranya wujud aktiviti-aktiviti tidak sah seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	CTM
7.14 Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
7.14.1 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: a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e. *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem; f. semua trafik rangkaian keluar dan masuk hendaklah melalui *firewall* di bawah kawalan JKDM; g. semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. memasang perisian *Intrusion Detection System* (IDS) bagi	CTM

Item/Aktiviti	Tanggungjawab
mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JKDM; i. 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"; j. sebarang penyambungan rangkaian yang bukan di bawah kawalan JKDM hendaklah mendapat kebenaran Pengurus ICT k. semua pengguna hanya dibenarkan menggunakan rangkaian JKDM sahaja. Penggunaan modem peribadi adalah dilarang sama sekali. l. memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	
7.15 Pengurusan Media Storan	
Objektif: Melindungi media storan dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.	
7.15.1 Penghantaran dan Pemindahan Media Storan	
Penghantaran atau pemindahan media storan ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Bahagian/Negeri terlebih dahulu.	Semua
7.15.2 Prosedur Pengendalian Media Storan	
a. Melabelkan semua media storan mengikut tahap sensitiviti sesuatu maklumat. b. Menghad dan menentukan capaian media storan kepada pengguna yang sah sahaja. c. Menghadkan pengedaran data atau media storan untuk tujuan yang dibenarkan. d. Mengawal dan merekodkan aktiviti penyelenggaraan media storan bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan. e. Menyimpan semua media storan di tempat yang selamat.	Semua

Item/Aktiviti	Tanggungjawab
f. Media storan yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	
7.16 Keselamatan Komunikasi	
Objektif: Melindungi aset ICT melalui sistem komunikasi yang selamat.	
7.16.1 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
7.16.2 Mel Elektronik	
a. Akaun atau alamat mel elektronik (emel) yang diperuntukkan oleh JKDM hanya boleh digunakan untuk urusan rasmi sahaja. b. Setiap akaun emel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh JKDM. c. Penggunaan akaun emel milik orang lain atau akaun emel yang dikongsi bersama adalah dilarang. d. Memastikan subjek dan kandungan emel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan.	Semua

Item/Aktiviti	Tanggungjawab
e. Pengguna hendaklah memastikan alamat emel penerima adalah betul sebelum penghantaran emel rasmi dibuat dan mengelak membuka emel daripada penghantar yang tidak diketahui atau diragui. f. Pengguna dinasihatkan menggunakan fail kepilan sekiranya perlu, tidak melebihi sepuluh (10) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan. g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui emel. h. Setiap emel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan. i. Emel yang telah diambil tindakan, tidak mempunyai nilai arkib dan tidak penting serta tidak diperlukan lagi bolehlah dihapuskan. j. Pengguna hendaklah memastikan tarikh dan masa sistem komputer adalah tepat. 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 emel.	
7.17 Kawalan Capaian	
Objektif: Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT JKDM.	
7.17.1 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
7.18 Pengurusan Capaian Pengguna	
Objektif: Mengawal capaian pengguna ke atas aset ICT JKDM.	

Item/Aktiviti	Tanggungjawab
7.18.1 Akaun Pengguna	
a. Semua pengguna baru hendaklah memohon akaun pengguna secara rasmi kepada Pemilik sistem /Pentadbir sistem. 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. c. Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan dan perlu mematuhi langkah-langkah berikut: i. Akaun pengguna mestilah unik; ii. akaun pengguna yang diwujud 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; dan iv. penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. d. Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Bertukar bidang tugas kerja; ii. bertukar ke agensi lain; iii. bersara; atau iv. ditamatkan perkhidmatan.	Semua
7.18.2 Pengurusan Kata laluan	
a. Amalan terbaik serta prosedur yang ditetapkan oleh JKDM dalam pengurusan kata laluan adalah seperti berikut: i. Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; ii. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; iii. Panjang kata laluan mestilah sekurang-kurangnya dua	Semua

Item/Aktiviti	Tanggungjawab
belas (12) aksara dengan gabungan alphanumeric dan simbol khas. Contoh kata laluan yang baik adalah "yw23#!y3ix8p". iv. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; v. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; vi. Kata laluan hendaklah tidak dipaparkan semasa *input*, 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 masa pengesahan ditentukan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; x. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan xi. Mengelakkan penggunaan semula kata laluan yang baru digunakan. <u>Nota:</u> Sumber Rujukan: "Dokumen Dasar Keselamatan ICT MAMPU Versi 5.3 bertarikh 13 Mei 2010".	
7.18.3 Jejak Audit	
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: 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	Pentadbir Sistem ICT

Item/Aktiviti	Tanggungjawab
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.	
7.19 Kawalan Capaian Sistem dan Aplikasi	
Objektif: Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.	
7.19.1 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: 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.	CTM
7.20 Perkakasan ICT Mudah Alih	
Objektif: Memastikan keselamatan maklumat apabila menggunakan kemudahan atau Perkakasan ICT mudah alih.	

Item/Aktiviti	Tanggungjawab
7.20.1 Penggunaan Perkakasan ICT Mudah Alih	
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. b. Pengguna adalah bertanggungjawab ke atas sebarang kehilangan atau kerosakan perkakasan ICT yang di pinjam. c. Perkakasan ICT mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. d. Untuk maklumat lanjut, sila rujuk: "Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan".	Semua
7.21 Keselamatan Dalam Membangunkan Sistem dan Aplikasi	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
7.21.1 Keperluan Keselamatan	
a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat. b. Ujian keselamatan hendaklah dijalankan ke atas: 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. c. Sebaiknya-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.	Pemilik Sistem dan CTM

Item/Aktiviti	Tanggungjawab
7.22 Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
7.22.1 Kawalan Sistem Fail	
a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan. b. Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji. c. Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT
7.23 Pembangunan dan Proses Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
7.23.1 Kawalan Perubahan	
Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum digunapakai.	Pentadbir Sistem ICT
7.24 Kesinambungan Perkhidmatan	
Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
7.24.1 Pelan Kesinambungan Perkhidmatan	
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	Pengurus ICT

Item/Aktiviti	Tanggungjawab
oleh JPICT dan perkara-perkara berikut perlu diberi perhatian: a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangkamasa yang telah ditetapkan; c. Mendokumentasikan proses dan prosedur yang telah dipersetujui; d. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; e. Membuat penduaan; dan f. Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.	

Perkara 8.0 - Pematuhan

Item/Aktiviti	Tanggungjawab
8.1 Pematuhan dan Keperluan Perundangan	
Objektif: Meningkatkan tahap penggunaan ICT bagi mengelak dari pelanggaran 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	
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di JKDM: a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”; c. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS); d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisma Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “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. Akta Tanda Tangan Digital 1997; h. Akta Jenayah Komputer 1997; i. Akta Hak cipta (Pindaan) Tahun 1997; j. Akta Komunikasi dan Multimedia 1998; dan k. Akta Aktiviti Kerajaan Elektronik 2007.	Semua

Lampiran 1

Garis Panduan Mengenai Tatacara Memohon Kelulusan Projek ICT

(Berdasarkan Surat Pekeliling Am Bil.1 Tahun 2009)

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 diperoleh 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.

(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 kurang daripada RM200,000 hendaklah mendapat kelulusan daripada JPICT di peringkat agensi sahaja;

ii. Semua Projek ICT melebihi RM200,000 dan telah diluluskan oleh JPICT Agensi hendaklah mendapatkan kelulusan teknikal daripada JPICT MOF; dan

iii. Hanya Projek ICT yang bernilai lebih daripada 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. Bagi projek ICT yang kurang daripada RM500,000 hendaklah mendapat kelulusan daripada JPICT di peringkat Ketua Agensi sahaja.

ii. Semua Projek ICT yang melebihi RM500,000 dan telah diluluskan oleh JPICT Agensi hendaklah mendapat kelulusan teknikal daripada JPICT MOF; dan

iii. Hanya Projek ICT bernilai lebih daripada RM3 juta dan telah diluluskan oleh JPICT MOF akan dikemukakan untuk kelulusan teknikal JTICT 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 hendaklah mematuhi garis panduan yang dikemukakan di dalam memohon kelulusan teknikal perolehan ICT daripada JPICT.

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.

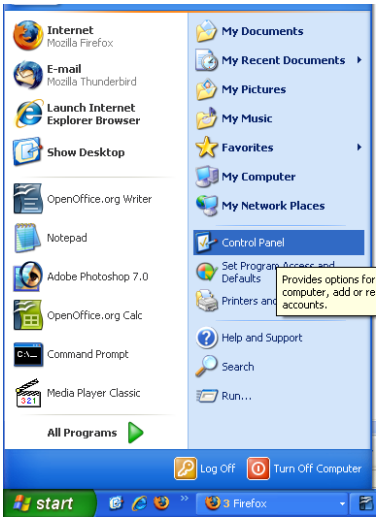
11. Bagi aplikasi yang dibangunkan oleh pembekal, klausa mengenai pemindahan teknologi *(Transfer of Technology)* hendaklah dinyatakan dalam dokumen kontrak.

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

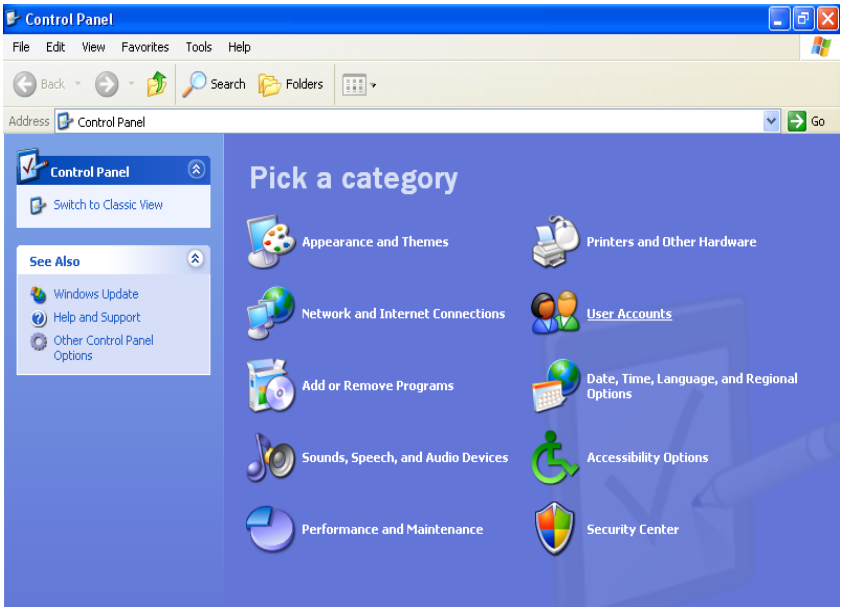
Lampiran 3

Garis Panduan untuk *Clear Screen Setting (Windows XP)*

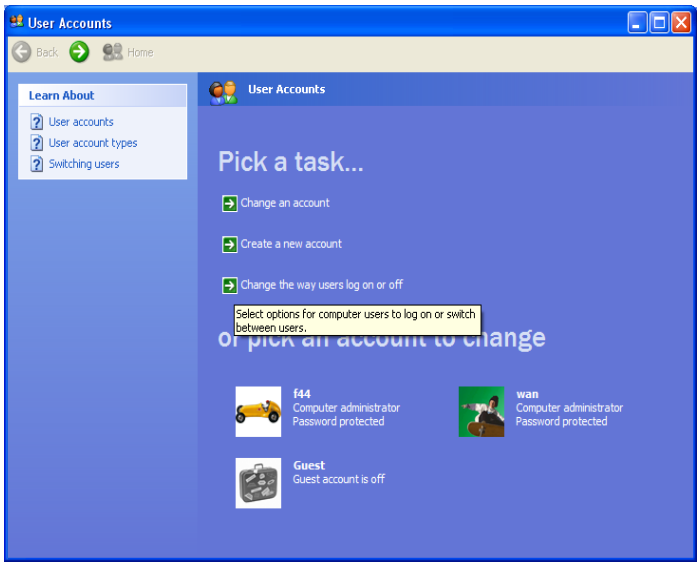
1. Click Start >> Control Panel



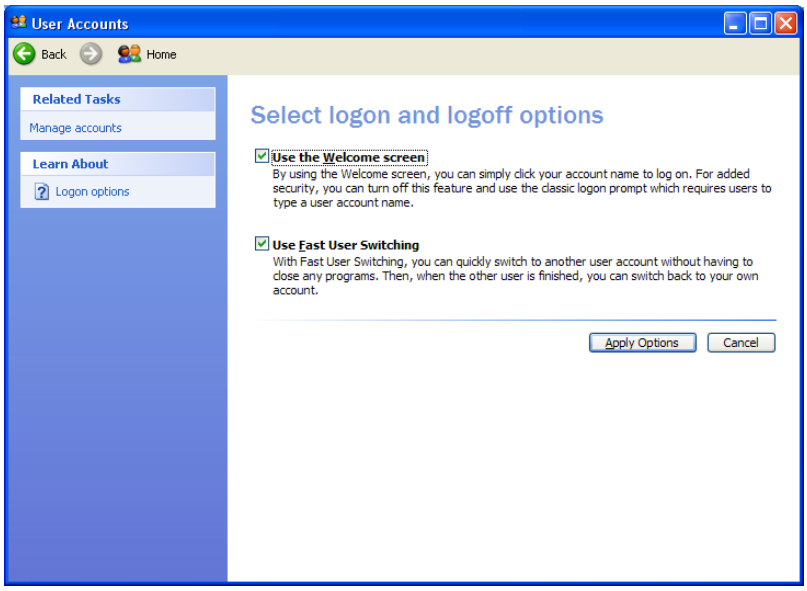
2. Click User Accounts



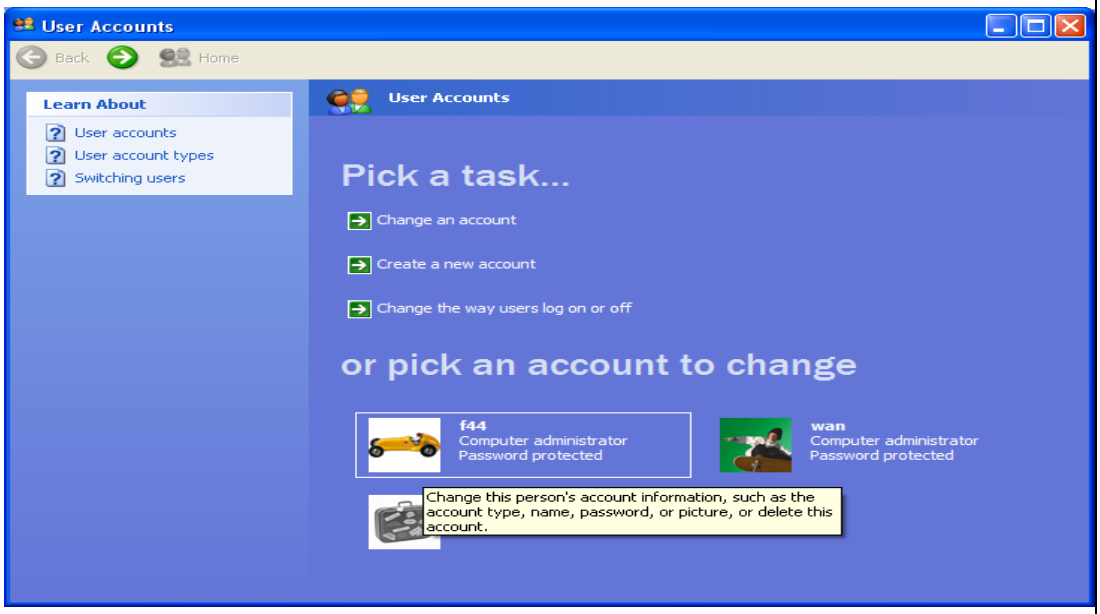
3. Click “Change the way users log on or off”



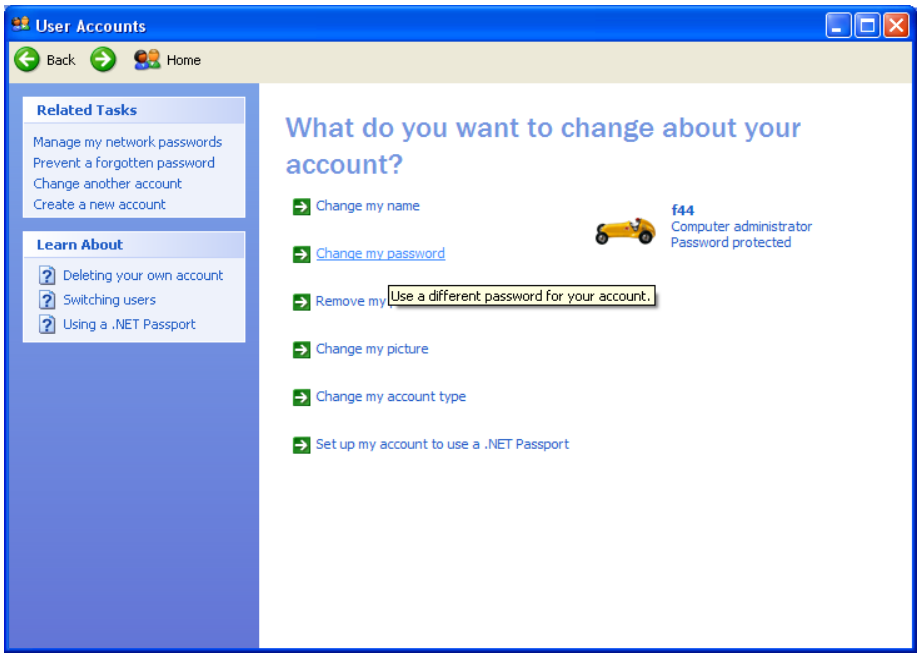
4. Tick (√) for “Use the Welcome screen”



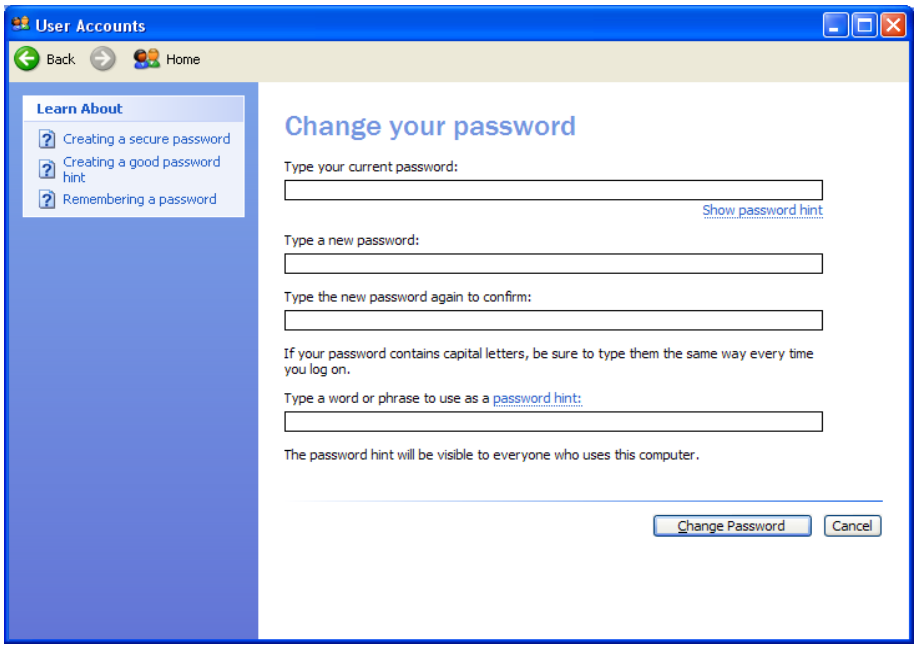
5. Pick an account to change / set password



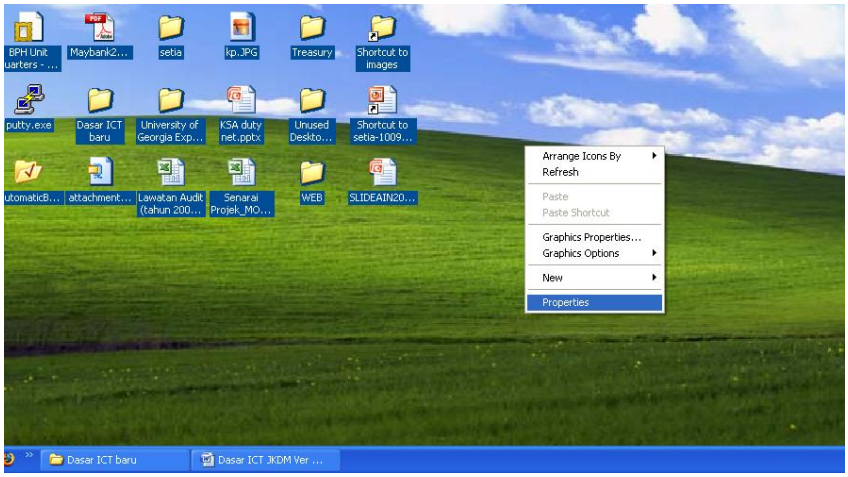
6. Click “Change my password”



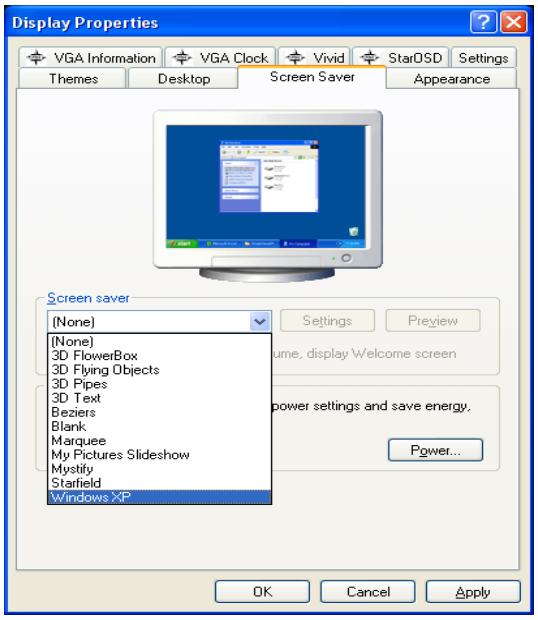
7. Type current password, new password and confirm new password. Click “Change password”.



8. Right Click at any desktop area. Click “Properties”



9. Click “Screen Saver” Tab, choose any screen saver.



10. Tick (√) “On resume, display Welcome screen”. Finally, click “OK”