



Dasar Keselamatan ICT

**Unit ePerolehan
Perbendaharaan Malaysia**



PERKARA 04 KESELAMATAN SUMBER MANUSIA.....	19
Keselamatan ICT Dalam Tugas Harian.....	19
DM-040101 Tanggungjawab Keselamatan.....	19
DM-040102 Terma dan Syarat Perkhidmatan.....	19
DM-040103 Perakuan Akta Rahsia Rasmi.....	19
Menangani Insiden Keselamatan ICT.....	19
DM-040201 Pelaporan Insiden.....	19
Pendidikan.....	20
DM-040301 Program Kesedaran Keselamatan ICT.....	20
Tindakan Tatatertib.....	20
DM-040401 Pelanggaran Dasar.....	20
PERKARA 05 KESELAMATAN FIZIKAL.....	21
Keselamatan Kawasan.....	21
DM-050101 Perimeter Keselamatan Fizikal.....	21
DM-050102 Kawalan Masuk Fizikal.....	21
DM-050103 Kawasan Larangan.....	22
Keselamatan Peralatan.....	22
DM-050201 Perkakasan.....	22
DM-050202 Dokumen.....	23
DM-050203 Media Storan.....	23
DM-050204 Kabel.....	23
DM-050205 Penyelenggaraan	24
DM-050206 Peminjaman Perkakasan Untuk Kegunaan di Luar Pejabat.....	24
DM-050207 Peralatan di Luar Premis.....	24
DM-050208 Pelupusan.....	25
DM-050209 <i>Clear Desk dan Clear Screen</i>	25
Keselamatan Persekitaran.....	25
DM-050301 Kawalan Persekitaran.....	25
DM-050302 Bekalan Kuasa.....	26
DM-050303 Prosedur Kecemasan.....	26

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI.....	27
Pengurusan Prosedur Operasi.....	27
DM-060101 Pengendalian Prosedur.....	27
DM-060102 Kawalan Perubahan.....	27
DM-060103 Prosedur Pengurusan Insiden.....	27
Perancangan dan Penerimaan Sistem.....	28
DM-060201 Perancangan Kapasiti.....	28
DM-060202 Penerimaan Sistem.....	28
Perisian Berbahaya.....	29
DM-060301 Perlindungan dari Perisian Berbahaya	29
<i>Housekeeping</i>.....	30
DM-060401 Penduaan.....	30
DM-060402 Sistem Log.....	30
Pengurusan Rangkaian.....	30
DM-060501 Kawalan Infrastruktur Rangkaian.....	30
Pengurusan Media.....	32
DM-060601 Penghantaran dan Pemindahan.....	32
DM-060602 Prosedur Pengendalian Media.....	32
DM-060603 Keselamatan Sistem Dokumentasi.....	32
Keselamatan Komunikasi.....	33
DM-060701 Internet.....	33
DM-060702 Mel Elektronik.....	33
PERKARA 07 KAWALAN CAPAIAN.....	35
Dasar Kawalan Capaian.....	35
DM-070101 Keperluan Dasar.....	35
Pengurusan Capaian Pengguna.....	35
DM-070201 Akaun Pengguna.....	35
DM-070202 Jejak Audit.....	36
Kawalan Capaian Sistem dan Aplikasi.....	37
DM-070301 Sistem Maklumat dan Aplikasi.....	37

Peralatan Komputer Mudah Alih.....	38
DM-070401 Penggunaan Peralatan Komputer Mudah Alih.....	38
PERKARA 08 PEMBANGUNAN DAN PENYELENGGARAAN SISTEM.....	39
Keselamatan Dalam Membangunkan Sistem dan Aplikasi.....	39
DM-080101 Keperluan Keselamatan.....	39
Kriptografi.....	39
DM-080201 Penyulitan.....	39
DM-080202 Tandatangan Digital.....	39
DM-080203 Pengurusan Kunci.....	40
Fail Sistem.....	40
DM-080301 Kawalan Fail Sistem.....	40
Pembangunan dan Proses Sokongan.....	40
DM-080401 Kawalan Perubahan.....	40
PERKARA 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN..	41
DM-090101 Mekanisme Pengurusan Pengendalian Insiden Keselamatan ICT.....	41
DM-090102 Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT.....	42
PERKARA 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN.....	43
DM-100101 Pelan Kesyinambungan Perkhidmatan.....	43
DM-100102 Pengurusan Kesyinambungan Perkhidmatan.....	44
PERKARA 11 PEMATUHAN.....	45
Pematuhan dan Keperluan Perundangan.....	45
DM-110101 Pematuhan Dasar.....	45
DM-110102 Keperluan Perundangan.....	45
DM-110103 Pematuhan Dengan Dasar, Piawaian dan Keperluan Teknikal.....	46
DM-110104 Pematuhan Keperluan Audit.....	46
DM-110105 Pelanggaran Dasar.....	46

PENGENALAN

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Unit ePerolehan (eP) dan Projek ePerolehan. Dasar ini juga menerangkan kepada semua pengguna di Unit ePerolehan dan di Pusat Tanggungjawab-Pusat Tanggungjawab (PTJ) mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT Unit dan Projek ePerolehan.

OBJEKTIF

Dasar Keselamatan ICT Unit ePerolehan diwujudkan untuk menjamin kesinambungan urusan Unit dan Projek ePerolehan dengan meminimumkan kesan insiden keselamatan ICT.

SKOP

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

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan dan melibatkan aktiviti berkala bagi menjamin keselamatan. Keselamatan ICT adalah bermaksud keadaan bagi urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan lancar tanpa gangguan yang boleh menjejaskan keselamatan termasuklah perlindungan kepada aset ICT.

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

- (a) Kerahsiaan — Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
- (b) Integriti — Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan; dan
- (c) Kebolehsediaan — Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

PRINSIP-PRINSIP

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

a. **Akses atas dasar "perlu mengetahui"**

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

b. **Hak akses minimum**

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

c. **Akauntabiliti**

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT Unit ePerolehan;

d. **Pengasingan**

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

e. **Pengauditan**

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

f. **Pematuhan**

Dasar Keselamatan ICT Unit ePerolehan hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang

boleh membawa ancaman kepada keselamatan ICT;

g. **Pemulihan**

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

h. **Saling Bergantungan**

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

Perkara 01 Pembangunan dan Penyelenggaraan Dasar

Dasar Keselamatan ICT

Objektif:

DKICT Unit ePerolehan diwujudkan untuk melindungi aset ICT bagi memastikan kelancaran operasi secara berterusan, meminimumkan kerosakan atau kemusnahan aset-aset ICT melalui usaha pencegahan atau mengurangkan kesan kejadian yang tidak diingini berdasarkan kepada ciri-ciri keselamatan iaitu kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan.

Perkara		Tanggungjawab
DM-010101 Pelaksanaan Dasar		
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha Perbendaharaan dibantu oleh Pasukan Pemandu Projek ePerolehan, Pasukan Pengurusan Keselamatan ICT Unit ePerolehan (PKICTeP) yang terdiri daripada Pengarah Projek ePerolehan, Timbalan Pengarah Projek ePerolehan, Ketua Bahagian Teknikal 2 Unit eP dan semua pegawai Seksyen Pengurusan Operasi Unit eP.	Ketua Setiausaha Perbendaharaan
DM-010102 Penyebaran Dasar		
	Dasar ini perlu disebar kepada semua pengguna Unit ePerolehan dan pengguna sistem ePerolehan (termasuk kakitangan, pembekal, pakar runding dan lain-lain)	PKICTeP
DM-010103 Penyelenggaraan Dasar		
	<p>Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT Unit ePerolehan:</p> <ol style="list-style-type: none"> Kenal pasti dan tentukan perubahan yang diperlukan; Kemuka cadangan pindaan secara bertulis kepada PKICTeP untuk pembentangan dan persetujuan Mesyuarat Jawatan Kuasa Pemandu eP (ePSC); Perubahan yang telah dipersetujui oleh ePSC dimaklumkan kepada semua pengguna; dan Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun. 	PKICTeP

DM-010104 Pengecualian Dasar		
	Dasar Keselamatan ICT Unit ePerolehan adalah terpakai kepada semua pengguna ICT Unit ePerolehan serta pengguna di Pusat Tanggungjawab dan tiada pengecualian diberikan.	Semua

Perkara 02 Organisasi Keselamatan

Infrastruktur Organisasi Keselamatan

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.

Perkara		Tanggungjawab
DM-020101 Ketua Setiausaha Perbendaharaan		
	<p>Peranan dan tanggungjawab Ketua Setiausaha Perbendaharaan adalah seperti berikut:</p> <ol style="list-style-type: none"> Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT Unit ePerolehan; Memastikan semua pengguna mematuhi Dasar Keselamatan ICT Unit ePerolehan; Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT Unit ePerolehan. 	Ketua Setiausaha Perbendaharaan
DM-020102 Pengarah Projek ePerolehan		
	<p>Peranan dan tanggung jawab Pengarah Projek eP (PeP) adalah seperti berikut:</p> <ol style="list-style-type: none"> Membantu Ketua Setiausaha Perbendaharaan dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; Menentukan keperluan keselamatan ICT; dan Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT. 	PeP

DM-020103 Pasukan Keselamatan ICT Unit eP (PKICTeP)		
	<p>PKICTeP diketuai oleh Timbalan Pengarah Projek ePerolehan. Peranan dan tanggungjawab PKICTeP yang dilantik adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Membantu Pengarah Projek dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Mengurus keseluruhan program-program keselamatan ICT Unit ePerolehan; c. Menguatkuasakan Dasar Keselamatan ICT Unit ePerolehan; d. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT Unit ePerolehan kepada semua pengguna; e. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT Unit ePerolehan; f. Menjalankan pengurusan risiko; g. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; h. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; i. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT), MAMPU dan memaklukkannya kepada PeP; j. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; k. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT Unit ePerolehan; dan l. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT. 	PKICTeP

DM-020104 Ketua Bahagian Teknikal 2		
	<p>Ketua Bahagian Teknikal 2 (KB(T2)) berperanan adalah seperti berikut:</p> <ol style="list-style-type: none"> Membaca, memahami dan mematuhi Dasar Keselamatan ICT Unit ePerolehan; Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Unit ePerolehan; Menentukan kawalan akses semua pengguna terhadap aset ICT Unit ePerolehan; Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada PKICTeP; dan Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT Unit ePerolehan. 	KB(T2)
DM-020105 Ketua Seksyen TO (Pengurusan Operasi)		
	<p>Ketua Penolong Pengarah Seksyen Teknikal Operasi (KPP(TO)) adalah merupakan Pentadbir Sistem ICT Unit ePerolehan. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut:</p> <ol style="list-style-type: none"> Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT Unit ePerolehan; Memantau aktiviti capaian harian pengguna; Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikanannya dengan serta merta; Menyimpan dan menganalisis rekod jejak audit; dan Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala. 	KPP(TO)

DM-020106	Pegguna	
	<p>Peranan dan tanggungjawab pengguna di Unit eP adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT Unit ePerolehan; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Lulus tapisan keselamatan; d. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat Unit ePerolehan; e. Melaksanakan langkah-langkah perlindungan seperti berikut :- <ol style="list-style-type: none"> 1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; 2. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; 3. Menentukan maklumat sedia untuk digunakan; 4. Menjaga kerahsiaan kata laluan; 5. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; 6. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan 7. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada PKICTeP dengan segera; g. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan h. Menandatangani surat akuan pematuhan Dasar Keselamatan ICT Unit ePerolehan. <p>Peranan dan tanggungjawab pengguna Sistem eP adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT Unit ePerolehan; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Melaksanakan prinsip-prinsip Dasar Keselamatan 	<p>Pegguna Sistem dan Pengguna Unit eP</p>

	<p>ICT dan menjaga kerahsiaan maklumat transaksi;</p> <p>d. Melaksanakan langkah-langkah perlindungan seperti berikut:-</p> <ol style="list-style-type: none"> 1. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; 2. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; 3. Menentukan maklumat sedia untuk digunakan; 4. Menjaga kerahsiaan kata laluan; 5. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; 6. Memberi perhatian kepada maklumat terperinci terutama semasa pewujudan, pemrosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan 7. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. <p>e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada PKICTeP dengan segera.</p>	
--	---	--

Pihak Ketiga

Objektif:

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.

	Perkara	Tanggungjawab
DM-020201	Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
	<p>Akses kepada aset ICT Unit ePerolehan perlu berlandaskan kepada perjanjian kontrak.</p> <p>Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan.</p> <ol style="list-style-type: none"> a. Dasar Keselamatan ICT Unit ePerolehan; b. Tapisan Keselamatan; c. Perakuan Akta Rahsia Rasmi 1972; d. Hak Harta Intelek; <p>Nota 1:</p> <p>Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk "Tatacara Penyediaan, Penilaian dan Penerimaan Tender" dan Surat Pekeliling Perbendaharaan Bilangan 3 Tahun 1995 bertajuk "Peraturan Perolehan Perkhidmatan Perundingan" yang berkaitan juga boleh dirujuk.</p>	<p>PeP, PKICTeP, KB(T2), KPP(TO) dan Pihak Ketiga</p>

Perkara 03 Pengurusan Aset

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT Unit ePerolehan.

Perkara		Tanggungjawab
DM-030101 Inventori Aset		
	Semua aset ICT Unit ePerolehan dan Projek ePerolehan hendaklah direkodkan. Ini termasuklah mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya.	Bahagian Pengurusan & KPP(TO)
	Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Semua

Pengelasan dan Pengendalian Maklumat

Objektif:

Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

Perkara		Tanggungjawab
DM-030201 Pengelasan Maklumat		
	Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	Semua
DM-030202 Pengendalian Maklumat		
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampaikan, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan;	Semua

	<ul style="list-style-type: none">d. Menjaga kerahsiaan kata laluan;e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dang. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.	
--	---	--

Perkara 04 Keselamatan Sumber Manusia

Keselamatan ICT Dalam Tugas Harian

Objektif:

Memastikan semua pihak yang terlibat termasuk pegawai dan kakitangan Unit ePerolehan, pembekal, pakar runding dan pihak-pihak yang terlibat memahami tanggungjawab dan peranan mereka dalam keselamatan aset ICT.

Perkara		Tanggungjawab
DM-040101	Tanggungjawab Keselamatan	
	<p>Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak.</p> <p>Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.</p>	Semua
DM-040102	Terma dan Syarat Perkhidmatan	
	Semua warga Unit ePerolehan yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	Semua
DM-040103	Perakuan Akta Rahsia Rasmi	
	Warga Unit ePerolehan yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua

Menangani Insiden Keselamatan ICT

Objektif:

Meminimumkan kesan insiden keselamatan ICT.

Perkara		Tanggungjawab
DM-040201	Pelaporan Insiden	
	<p>Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada PKICTeP dengan kadar segera:</p> <ol style="list-style-type: none"> Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; 	Semua

	<p>c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;</p> <p>d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar;</p> <p>e. Berlaku percubaan mencero boh, penyelewengan dan insiden-insiden yang tidak diingini.</p> <p>Nota 2:</p> <p>Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan ICT” mengenainya bolehlah dirujuk.</p>	
--	---	--

Pendidikan

Objektif:

Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.

	Perkara	Tanggungjawab
DM-040301	Program Kesedaran Keselamatan ICT	
	<p>Setiap pengguna di Unit ePerolehan perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka.</p> <p>Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT Unit ePerolehan.</p>	PKICTeP & Bahagian Pengurusan

Tindakan Tatatertib

Objektif:

Meningkat kesedaran dan pematuhan ke atas Dasar Keselamatan ICT Unit ePerolehan.

	Perkara	Tanggungjawab
DM-040401	Pelanggaran Dasar	
	<p>Pelanggaran Dasar Keselamatan ICT Unit ePerolehan akan dikenakan tindakan tatatertib.</p>	Semua

Perkara 05 Keselamatan Fizikal dan Persekitaran

Keselamatan Kawasan

Objektif:

Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.

Perkara		Tanggungjawab
DM-050101	Perimeter Keselamatan Fizikal	
	<p>Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk mencero boh. Langkah-langkah fizikal tidak terhad kepada langkah-langkah keselamatan berikut:</p> <ol style="list-style-type: none"> Kawasan keselamatan fizikal hendaklah di kenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; Memperkukuhkan dinding dan siling; Memasang alat penggera atau kamera; Menghadkan jalan keluar masuk; Mengadakan kaunter kawalan; Menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan Mewujudkan perkhidmatan kawalan keselamatan. 	Pejabat Ketua Pegawai Keselamatan Kerajaan, PeP dan PKICTeP
DM-050102	Kawalan Masuk Fizikal	
	<ol style="list-style-type: none"> Setiap pengguna Unit ePerolehan hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; Setiap pelawat hendaklah mendaftar dan mendapat Pas Keselamatan Pelawat di pintu utama Unit ePerolehan dan hendaklah dikembalikan semula selepas tamat lawatan; Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara; Kehilangan pas mestilah dilaporkan dengan segera; Hanya pengguna yang diberi kebenaran sahaja 	Semua dan pelawat

	boleh mencapai atau menggunakan aset ICT Unit ePerolehan;	
DM-050103	Kawasan Larangan	
	<p>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 Unit ePerolehan adalah semua bilik pegawai dan bilik server. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja:</p> <ol style="list-style-type: none"> Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu; Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan Semua penggunaan peralatan yang melibatkan penghantaran, kemas kini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Pengarah Projek. 	Semua

Keselamatan Peralatan

Objektif:

Melindung peralatan dan maklumat.

Perkara		Tanggungjawab
DM-050201	Perkakasan	
	<p>Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu:</p> <ol style="list-style-type: none"> Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna; Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan Sebarang bentuk penyelewengan atau salah guna 	Semua

	perkakasan hendaklah dilaporkan kepada PKICTeP.	
DM-050202 Dokumen		
	<p>Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi:</p> <ol style="list-style-type: none"> Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; Menggunakan penyulitan (encryption) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik; dan Memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak. 	Semua
DM-050203 Media Storan		
	<p>Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat:</p> <ol style="list-style-type: none"> Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan Pergerakan media storan hendaklah direkodkan. 	Semua
DM-050204 Kabel		
	Kabel komputer hendaklah dilindung kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut:	Bahagian Teknologi Maklumat dan PKICTeP

	<ul style="list-style-type: none"> a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; dan c. Melindung laluan pemasangan kabel sepenuhnya. 	
DM-050205 Penyelenggaraan		
	<p>Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti.</p> <ul style="list-style-type: none"> a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b. Perakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan d. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengarah Bahagian berkenaan. 	Semua
DM-050206 Peminjaman Perakasan Untuk Kegunaan Di Luar Pejabat		
	<p>Perkakasan 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"> a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan. 	Semua
DM-050207 Peralatan di Luar Premis		
	<p>Bagi perkakasan yang dibawa keluar dari premis Unit ePerolehan, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan Unit ePerolehan:</p> <ul style="list-style-type: none"> a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian. 	Semua

DM-050208 Pelupusan		
	<p>Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan Unit ePerolehan:</p> <ol style="list-style-type: none"> Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui <i>shredding</i>, <i>grinding</i>, <i>degauzing</i> atau pembakaran; Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan Maklumat lanjut pelupusan bolehlah merujuk kepada Surat Pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk "Garis Panduan Pelupusan Peralatan Komputer". 	Semua
DM-050209 Clear Desk dan Clear Screen		
	<p>Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Clear Desk bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja warga atau di paparan skrin apabila warga tidak berada di tempatnya:</p> <ol style="list-style-type: none"> Gunakan kemudahan <i>password screen saver</i> atau log keluar apabila meninggalkan komputer atau tidak; Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci. 	Semua

Keselamatan Persekitaran

Objektif:

Melindungi aset ICT Unit ePerolehan daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuiaan atau kemalangan.

Perkara		Tanggungjawab
DM-050301 Kawalan Persekitaran		
	<p>Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil:</p>	Semua

	<ul style="list-style-type: none"> a. Merancang dan menyediakan pelan keseluruhan susun atur bilik server (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu. 	
DM-050302 Bekalan Kuasa		
	<ul style="list-style-type: none"> a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti UPS (Uninterruptable Power Supply) dan penjana (generator) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual. 	<p>Teknikal Operasi, PKICTeP</p>
DM-050303 Prosedur Kecemasan		
	<ul style="list-style-type: none"> a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan Unit ePerolehan 2004; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik mengikut aras; 	<p>Semua</p>

Perkara 06 Pengurusan Operasi dan Komunikasi

Pengurusan Prosedur Operasi

Objektif:

Memastikan perkhidmatan dan pemprosesan maklumat dan komunikasi dapat berfungsi dengan betul dan selamat dari sebarang ancaman atau gangguan.

Perkara		Tanggungjawab
DM-060101	Pengendalian Prosedur	
	<p>a. Semua prosedur keselamatan ICT yang di wujud, dikenal pasti 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; dan</p> <p>c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.</p>	Semua
DM-060102	Kawalan Perubahan	
	<p>a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik 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; dan</p> <p>d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.</p>	Semua
DM-060103	Prosedur Pengurusan Insiden	
	<p>Bagi memastikan tindakan menangani insiden keselamatan ICT, diambil dengan cepat, teratur dan berkesan; prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut:</p>	ePSC, PKICTeP

	<ul style="list-style-type: none"> a. Mengetahui pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c. Menyimpan jejak audit dan memelihara bahan bukti; dan d. Menyediakan tindakan pemulihan segera. 	
--	---	--

Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

Perkara		Tanggungjawab
DM-060201	Perancangan Kapasiti	
	<ul style="list-style-type: none"> 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; dan 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. 	KPP(TO), PKICTeP
DM-060202	Penerimaan Sistem	
	Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	KPP(TO), PKICTeP

Perisian Berbahaya

Objektif:

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

Perkara	Tanggungjawab
DM-060301 Perlindungan dari Perisian Berbahaya	
<ul style="list-style-type: none"> a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan Intrusion Detection System (IDS) dan mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. Mengemas kini paten anti virus setiap minggu; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus. 	Semua

Housekeeping

Objektif:

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

Perkara		Tanggungjawab
DM-060401	Penduaan	
	<p>Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan di off site.</p> <ol style="list-style-type: none"> Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan. 	Semua
DM-060402	Sistem Log	
	<ol style="list-style-type: none"> Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada PKICTeP. 	Teknikal Operasi

Pengurusan Rangkaian

Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

Perkara		Tanggungjawab
DM-060501	Kawalan Infrastruktur Rangkaian	
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada	Teknikal Operasi

	<p>sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan:-</p> <ol style="list-style-type: none">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 keluar dan masuk hendaklah melalui firewall di bawah kawalan Unit ePerolehan;g. Semua perisian sniffer atau network analyser adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran PKICTeP;h. Memasang perisian Intrusion Detection System (IDS) bagi mengesan sebarang cubaan menceroth dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat Unit ePerolehan;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 Unit ePerolehan hendaklah mendapat kebenaran PKICTeP;k. Semua pengguna hanya dibenarkan menggunakan rangkaian Unit ePerolehan sahaja. Penggunaan modem adalah dilarang sama sekali; dan	
--	--	--

	l. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	
--	---	--

Pengurusan Media

Objektif:

Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.

Perkara		Tanggungjawab
DM-060601	Penghantaran dan Pemindahan	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Semua
DM-060602	Prosedur Pengendalian Media	
	a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	Semua
DM-060603	Keselamatan Sistem Dokumentasi	
	a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan. b. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	KPP(TO), PKICTeP

Keselamatan Komunikasi

Objektif:

Melindungi aset ICT melalui sistem komunikasi yang selamat.

Perkara		Tanggungjawab
DM-060701 Internet		
	<p>a. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan;</p> <p>b. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan;</p> <p>c. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet;</p> <p>d. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara;</p> <p>e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh Unit ePerolehan;</p> <p>f. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti newsgroup dan bulletin board. Walaubagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; dan</p> <p>g. Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".</p>	Semua
DM-060702 Mel Elektronik		
	<p>a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh Unit ePerolehan sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;</p> <p>b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh Unit ePerolehan;</p>	Semua

	<ul style="list-style-type: none">c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul;e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi dua (2) megabait semasa penghantaran. Ini adalah untuk mengelakkan kesesakan di dalam rangkaian apabila fail terlalu besar dihantar. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dank. Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".	
--	--	--

Perkara 07 Kawalan Capaian

Dasar Kawalan Capaian

Objektif :

Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT Unit ePerolehan.

Perkara		Tanggungjawab
DM-070101 Keperluan Dasar		
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	Teknikal Operasi, PKICTeP

Pengurusan Capaian Pengguna

Objektif :

Mengawal capaian pengguna ke atas aset ICT Unit ePerolehan.

Perkara		Tanggungjawab
DM-070201 Akaun Pengguna		
	<p>Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi:</p> <ol style="list-style-type: none"> Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; Akaun pengguna mestilah unik; Akaun pengguna yang di wujud pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab 	Semua

	<p>berikut:</p> <ul style="list-style-type: none"> i) Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu; ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan. 	
DM-070202 Jejak Audit		
	<p>Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi:</p> <ul style="list-style-type: none"> a. Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan c. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. <p>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 pengubah suaian yang tidak dibenarkan.</p>	<p>KPP(TO), Penolong Pengarah Kanan (Juruaudit)</p>

Kawalan Capaian Sistem dan Aplikasi

Objektif:

Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.

Perkara	Tanggungjawab
DM-070301 Sistem Maklumat dan Aplikasi	
<p>Capaian sistem dan aplikasi di Unit ePerolehan adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan Sistem, kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi:</p> <ol 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; e. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan f. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walaubagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja. 	<p>KPP(TO), PKICTeP</p>

Peralatan Komputer Mudah Alih

Objektif :

Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.

Perkara		Tanggungjawab
DM-070401 Penggunaan Peralatan Komputer Mudah Alih		
	<p>a. Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan</p> <p>b. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.</p>	Semua

Perkara 08 Pembangunan dan Penyelenggaraan Sistem

Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif:

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

Perkara		Tanggungjawab
DM-080101	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 sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; dan</p> <p>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.</p>	KPP(TO), PKICTeP

Kriptografi

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat.

Perkara		Tanggungjawab
DM-080201	Penyulitan	
	Pengguna hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
DM-080202	Tandatangan Digital	
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua

DM-080203 Pengurusan Kunci		
	Pengurusan kunci hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua

Fail Sistem

Objektif:

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

Perkara		Tanggungjawab
DM-080301 Kawalan Fail Sistem		
	<ul style="list-style-type: none"> a. Proses pengemas kini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubah suaian tanpa kebenaran, penghapusan dan kecurian; dan d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemas kinian untuk tujuan statistik, pemulihan dan keselamatan. 	KPP(TO)

Pembangunan dan Proses Sokongan

Objektif:

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

Perkara		Tanggungjawab
DM-080401 Kawalan Perubahan		
	Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai.	KPP(TO)

Perkara 09 Pengurusan Pengendalian Insiden Keselamatan

Objektif:

Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan dan memastikan sistem ICT dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej.

Perkara	Tanggungjawab
DM-090101 Mekanisme Pelaporan Insiden Keselamatan ICT	
<p>Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera:</p> <ol style="list-style-type: none"> a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisma kawalan akses, hilang, dicuri atau didedahkan disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan mencerooboh, penyelewengan dan insiden-insiden yang tidak diingini. <p>Sekiranya berlaku insiden keselamatan ICT, maka mekanisme pelaporan adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Pelaporan Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan kepada CERTeP untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. b. CERTeP Pasukan CERTeP akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai <i>input</i> atau untuk tindakan seterusnya. c. Tanggungjawab Pengguna Semua kakitangan, pembekal, pakar runding dan pihak-pihak lain yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan secara sendiri, tetapi sebaliknya perlu terus melaporkan dengan segera sebarang kejadian insiden keselamatan ICT kepada 	<p>KPP(TO), PKICTeP</p>

	<p>ICTSO, kerentanan (<i>vulnerability</i>) yang diperhatikan atau disyaki terdapat dalam sistem maklumat menerusi mekanisme pelaporan ini. Ini adalah bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan mencerooboh.</p> <p>d. Tindakan Dalam Keadaan Berisiko Tinggi Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak.</p>	
DM-090201 Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT		
	<p>Semua pegawai pasukan pengendali insiden keselamatan ICT atau CERTeP perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur operasi standard keselamatan CERTeP dan GCERT.</p> <p>CERTeP menerima aduan atau laporan daripada pengguna, laporan yang dikesan dari PRISMA atau laporan dari sumber luar. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden kemudiannya dimaklumkan kepada GCERT MAMPU. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguatkuasa undang-undang.</p> <p>CERTeP yang diketuai oleh ICTSO akan menjalankan tindakan pengendalian secara capaian jarak jauh (<i>remote</i>) atau <i>on-site</i>. Sekiranya laporan tersebut memerlukan bantuan GCERT MAMPU, permohonan akan dihantar bagi mendapatkan maklum balas GCERT MAMPU.</p> <p>Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan akan dihantar melalui GCERT MAMPU dan khidmat nasihat akan disalurkan. CERTeP seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya Pelan Kesenambungan Perkhidmatan / <i>Business Resumption Plan (BRP)</i> perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada CIO bagi mengaktifkan <i>BRP</i>.</p> <p>Laporan insiden yang tidak memerlukan <i>BRP</i> akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan.</p>	CERTeP

Perkara 10 Pengurusan Kesenambungan Perkhidmatan

Dasar Kesenambungan Perkhidmatan

Objektif:

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

Perkara	Tanggungjawab
DM-100101 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 ePSC dan perkara-perkara berikut perlu diberi perhatian:</p> <ol style="list-style-type: none"> a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa 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 mengemas kini pelan sekurang-kurangnya setahun sekali. 	PKICTeP

DM-100102 Pengurusan Kesenambungan Perkhidmatan		
	<p>Pengurusan Kesenambungan Perkhidmatan adalah mekanisme bagi mengurus dan memastikan kepentingan <i>stakeholder</i> sistem penyampaian perkhidmatan dilindungi dan imej terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan.</p> <p>Unit eP adalah bertanggungjawab untuk memastikan operasi sistem disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT eP.</p>	Semua

Perkara 11 Pematuhan

Pematuhan dan Keperluan Perundangan

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT Unit ePerolehan.

Perkara	Tanggungjawab
DM-110101 Pematuhan Dasar	
<p>Setiap pengguna di Unit ePerolehan hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT Unit ePerolehan dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa.</p> <p>Semua aset ICT di Unit ePerolehan 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.</p>	Semua
DM-110102 Keperluan Perundangan	
<p>Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di Unit ePerolehan adalah seperti berikut:</p> <ol style="list-style-type: none"> a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”; c. <i>Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS)</i>; d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme 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. Surat Pekeliling Am Bil. 4 Tahun 2006 – “Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor 	Semua

	<p>Awam”;</p> <p>h. Surat Pekeliling Perbendaharaan Bil. 2/1995 (Tambahan pertama) - “Tatacara Penyediaan, Penilaian dan Penerimaan Tender”;</p> <p>i. Surat Pekeliling Perbendaharaan Bil. 3/1995 - “Peraturan Perolehan Perkhidmatan Perundingan”;</p> <p>j. Akta Tandatangan Digital 1997;</p> <p>k. Akta Rahsia Rasmi 1972;</p> <p>l. Akta Jenayah Komputer 1997;</p> <p>m. Akta Hak cipta (Pindaan) Tahun 1997;</p> <p>n. Akta Komunikasi dan Multimedia 1998;</p> <p>o. Perintah-Perintah Am;</p> <p>p. Arahan Perbendaharaan;</p> <p>q. Arahan Teknologi Maklumat 2007; dan</p> <p>r. <i>Standard Operating Procedure (SOP) ICT eP.</i></p>	
DM-110103 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal		
	<p>ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal.</p> <p>Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan.</p>	ICTSO
DM-110104 Pematuhan Keperluan Audit		
	<p>Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat.</p> <p>Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan.</p> <p>Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.</p>	Semua
DM-110105 Pelanggaran Dasar		
	Pelanggaran Dasar Keselamatan ICT Unit ePerolehan boleh dikenakan tindakan tatatertib.	Semua

Disediakan oleh:

**Unit ePerolehan
Perbendaharaan Malaysia**