Dasar Keselamatan ICT

Lembaga Getah Malaysia (LGM)

Oktober 2010

KANDUNGAN

PENGENALAN

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

OBJEKTIF

Dasar Keselamatan ICT LGM diwujudkan untuk menjamin kesinambungan urusan LGM 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 LGM termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT LGM.

PRINSIP-PRINSIP

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

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

b. **Hak akses minimum**
   Hak akses pengguna hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses 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 LGM;

d. Pengasingan

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

e. Pengauditan

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

f. Pematuhan

Dasar Keselamatan ICT LGM 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 kepada sistem tersebut. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/kesinambungan perkhidmatan; dan

h. Saling Bergantungan

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

PERKARA 01

PEMBANGUNAN DAN PENYELENGGARAAN DASAR

Kandungan Dasar		Tanggungjawab
0101 Dasar Keselamatan ICT		
010101 Pelaksanaan Dasar		
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah LGM dibantu oleh Jawatankuasa Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), dan semua Pengarah Bahagian .	Ketua Pengarah
010102 Penyebaran Dasar		
	Dasar ini perlu disebarkan kepada semua pengguna ICT LGM (termasuk kakitangan, pembekal, pakar runding dan lain-lain.)	ICTSO
010103 Penyelenggaraan Dasar		
	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 LGM: a. kenal pasti dan tentukan perubahan yang diperlukan; b. kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Teknikal LGM; c. perubahan yang telah dipersetujui oleh Jawatankuasa Teknikal LGM dimaklumkan kepada semua pengguna; dan d. dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.	ICTSO

Kandungan Dasar		Tanggungjawab
010104 Pengecualian Dasar		
	Dasar Keselamatan ICT LGM adalah terpakai kepada semua pengguna ICT LGM dan tiada pengecalian diberikan.	Semua

PERKARA 02

ORGANISASI KESELAMATAN

Kandungan Dasar		Tanggungjawab
0201 Infrastruktur Organisasi Keselamatan Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi keselamatan.		
020101 Ketua Pengarah		
	Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut: a. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT LGM; b. memastikan semua pengguna mematuhi Dasar Keselamatan ICT LGM; c. memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan d. memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT LGM.	Ketua Pengarah
020102 Ketua Pegawai Maklumat (CIO)		
	Timbalan Ketua Pengarah (Dasar dan Operasi) LGM adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut: a. membantu Ketua Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. menentukan keperluan keselamatan ICT; dan c. membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.	CIO

Kandungan Dasar		Tanggungjawab
020103 Pegawai Keselamatan ICT (ICTSO)		
	Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. mengurus keseluruhan program-program keselamatan ICT LGM; b. menguatkuasakan Dasar Keselamatan ICT LGM; c. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT LGM kepada semua pengguna; d. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT LGM; e. menjalankan pengurusan risiko; f. menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h. melaporkan insiden keselamatan ICT kepada Pasukan Tindak Balas Insiden Keselamatan ICT (GCERT) dan memaklumkannya kepada CIO; i. bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j. memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT LGM; dan k. menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	ICTSO

Kandungan Dasar		Tanggungjawab
020104 Pengurus ICT		
	Ketua Unit Teknologi Maklumat(UTM) adalah merupakan Pengurus ICT LGM. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT LGM; b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan LGM; c. menentukan kawalan akses semua pengguna terhadap aset ICT LGM; d. melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan e. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT LGM.	Pengurus ICT
020105 Pentadbir Sistem ICT		
	Ketua Kumpulan Pembangunan Aplikasi atau mana-mana pegawai yang dilantik oleh LGM untuk mentadbir sesuatu sistem di LGM adalah merupakan Pentadbir Sistem ICT LGM. Peranan dan tanggungjawab adalah seperti berikut: a. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti 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 Keselamatan ICT LGM; c. memantau aktiviti capaian sistem dan rangkaian harian pengguna; d. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. menyimpan dan menganalisis rekod jejak audit; dan	Pentadbir Sistem ICT, UTM

Kandungan Dasar		Tanggungjawab
	f. menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	
020106 Pentadbir Rangkaian		
	Ketua Kumpulan Rangkaian dan Penyenggaraan ICT atau mana-mana pegawai yang dilantik oleh LGM untuk mentadbir rangkaian ICT di LGM adalah merupakan Pentadbir Rangkaian ICT LGM. Peranan dan tanggungjawab adalah seperti berikut: a. mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. menentukan ketepatan dan kesempurnaan sesuatu tahap capaian di dalam rangkaian; c. memantau aktiviti rangkaian harian pengguna; d. mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. menyimpan dan menganalisis rekod jejak audit; dan f. menyediakan laporan akses rangkaian secara berkala.	Pentadbir Rangkaian, UTM
020107 Pengguna		
	Peranan dan tanggungjawab pengguna adalah seperti berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT LGM; b. mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat LGM; d. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;	Pengguna

Kandungan Dasar		Tanggungjawab
	e. menghadiri program-program kesedaran mengenai keselamatan ICT; dan	
020108 Jawatankuasa Keselamatan ICT LGM		
	Jawatankuasa Keselamatan ICT (JKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT LGM. Keanggotaan JKICT LGM adalah seperti berikut: **Pengerusi :** Ketua Pengarah LGM **Ahli :** (1) CIO LGM (2) Semua Pengarah Bahagian (4) ICTSO LGM **Bidang kuasa:** a. Memperakukan/meluluskan dokumen DKICT LGM; b. Memantau tahap pematuhan keselamatan ICT; c. Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam LGM yang mematuhi keperluan DKICT LGM; d. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; e. Memastikan DKICT LGM selaras dengan dasar-dasar ICT kerajaan semasa; f. Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; g. Membincang tindakan yang melibatkan pelanggaran DKICT LGM; dan h. Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	JKICT LGM

Kandungan Dasar		Tanggungjawab
0202 Pihak Ketiga Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga		
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga		
	Ini bertujuan bagi memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi adalah: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT LGM; b. Mengenalpasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. Mengenalpasti keperluan keselamatan sebelum memberi kebenaran capaian atau kepenggunaan kepada pihak ketiga; d. Akses kepada aset ICT LGM perlu berlandaskan kepada perjanjian kontrak; e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai: i. Dasar Keselamatan ICT LGM; ii. Perakuan Akta Rahsia Rasmi 1972; iii. Hak Harta Intelek;	CIO, ICTSO, Pengurus Komputer, Pentadbir Sistem ICT, Pentadbir Rangkaian dan Pihak Ketiga

PERKARA 03

KAWALAN DAN PENGELASAN ASET

Kandungan Dasar		Tanggungjawab
0301 Akauntabiliti Aset Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT LGM.		
030101 Aset ICT		
	Semua aset ICT LGM hendaklah direkodkan di dalam Sistem My1Asset mengikut Tatacara Pengurusan Aset Alih Kerajaan dari Pekeliling Perbendaharaan Bil 5 Tahun 2007. Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Semua
0302 Pengelasan dan Pengendalian Maklumat Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.		
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
030202 Pengendalian Maklumat		
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;	Semua

Kandungan Dasar		Tanggungjawab
	b. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. menentukan maklumat sedia untuk digunakan; d. menjaga kerahsiaan kata laluan; e. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

PERKARA 04

KESELAMATAN SUMBER MANUSIA

Kandungan Dasar		Tanggungjawab
0401 Keselamatan Sumber Manusia Dalam Tugas Harian Objektif: Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan LGM, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga LGM hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.		
040101 Sebelum Perkhidmatan		
	Perkara-perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan LGM serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pegawai dan kakitangan LGM serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan.	Semua
040102 Dalam Perkhidmatan		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan pegawai dan kakitangan LGM serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh LGM ;	Semua

Kandungan Dasar		Tanggungjawab
	b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT LGM secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; c. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan LGM serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh LGM ; dan d. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Unit Pengurusan Sumber Manusia.	
040103 Bertukar atau Tamat Perkhidmatan		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Memastikan semua aset ICT dikembalikan kepada LGM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh LGM dan/atau terma perkhidmatan.	Semua

PERKARA 05

KESELAMATAN FIZIKAL DAN PERSEKITARAN

Kandungan Dasar		Tanggungjawab
0501 Keselamatan Kawasan Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.		
050101 Kawalan Kawasan		
	Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Kawasan keselamatan fizikal hendaklah dikenalpasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c. Menghadkan jalan keluar masuk; d. Mewujudkan perkhidmatan kawalan keselamatan; e. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; f. Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; g. Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; h. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan i. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Pegawai Keselamatan LGM, CIO dan ICTSO

	Kandungan Dasar	Tanggungjawab
050102	**Kawalan Masuk Fizikal**	
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Setiap warga LGM hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Semua pas keselamatan hendaklah diserahkan balik kepada LGM apabila pengguna berhenti atau bersara; c. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter pengawal di Bangunan Getah Asli (Menara). Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan d. Kehilangan pas mestilah dilaporkan dengan segera.	Semua
050103	**Kawasan Larangan**	
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di LGM adalah bilik Ketua Pengarah, bilik-bilik Timbalan Ketua Pengarah, bilik-bilik Pengarah dan bilik server. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja: a. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja; dan b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai;	Semua

	Kandungan Dasar	Tanggungjawab
	0502 Keselamatan Peralatan Objektif: Melindungi peralatan ICT LGM dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
	050201 Peralatan ICT	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d. Pengguna dilarang membuat sebarang instalasi perisian tambahan tanpa kebenaran Pengurus ICT; e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemaskini disamping melakukan imbasan ke atas media storan yang digunakan; g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); j. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; k. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; l. Peralatan ICT yang hendak dibawa keluar dari premis LGM, perlulah mendapat kelulusan Pengurus ICT dan direkodkan bagi tujuan pemantauan;	Semua

Kandungan Dasar		Tanggungjawab
	m. Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; n. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuatkuasa; o. Sebarang kerosakan peralatan ICT hendaklah dilaporkan melalui Sistem Pengurusan Aduan UTM untuk dibaikpulih; p. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; q. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; r. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; s. Sebarang bentuk penyelewengan atau salahguna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan t. Memastikan plag dicabut daripada suis utama (*main switch)* bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
050202 Media Storan		
	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk, flash disk*, *thumb drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja;	Semua

Kandungan Dasar		Tanggungjawab
	c. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; d. Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; e. Akses dan pergerakan media storan hendaklah direkodkan; f. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; g. Mengadakan *backup* pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan i. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
050203 Media Tandatangan Digital		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital dan dilindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b. Media ini tidak boleh dipindah milik atau dipinjamkan; dan c. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Semua
050204 Media Perisian dan Aplikasi		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan LGM; b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran ICTSO;	Semua

Kandungan Dasar		Tanggungjawab
	c. Lesen perisian (*registration code, serials, CD-key*) perlu disimpan berasingan daripada *CD-rom*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d. *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	
050205 Penyelenggaraan Perkakasan		
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti terjamin. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b. Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap penyelenggaraan perkakasan sama ada masih dalam tempoh jaminan atau telah tamat tempoh jaminan; d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	Semua Pegawai Aset dan Kumpulan Pengurusan Infrastrutur ICT UTM
050206 Peralatan di Luar Premis		
	Perkakasan yang dibawa keluar dari premis LGM adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua

Kandungan Dasar		Tanggungjawab
050207 Pelupusan Perkakasan		
	Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh LGM dan ditempatkan di LGM. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan LGM. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat *backup*; c. Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; e. Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; f. Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem My1Asset; g. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan h. Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan	Pegawai Aset Setiap Unit, Kumpulan Pengurusan Infrastruktur ICT

Kandungan Dasar		Tanggungjawab
	menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran computer seperti *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di LGM; iii. Memindah keluar dari LGM mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab LGM; dan v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
0503 Keselamatan Persekitaran Objektif: Melindungi aset ICT LGM dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.		
050301 Kawalan Persekitaran		
	Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil: 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;	Semua

Kandungan Dasar		Tanggungjawab
	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.	
050302 Bekalan Kuasa		
	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti 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.	UTM, ICTSO
050303 Kabel		
	Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya	Kumpulan Pengurusan Infrastrutur ICT UTM

Kandungan Dasar		Tanggungjawab
	bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	
050304 Prosedur Kecemasan		
	a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan Perlindungan LGM; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan yang dilantik;	Semua

PERKARA 06

PENGURUSAN OPERASI DAN KOMUNIKASI

Kandungan Dasar		Tanggungjawab
0601 Pengurusan Prosedur Operasi Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.		
060101 Pengendalian Prosedur Operasi		
	a. Semua prosedur keselamatan ICT yang wujud, dikenalpasti dan masih digunapakai hendaklah didokumenkan, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap; dan c. Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	Semua
060102 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. Aktivit-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; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua

Kandungan Dasar		Tanggungjawab
060103 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 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.	ICTSO dan Pengurus Komputer

Kandungan Dasar		Tanggungjawab
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.		
060201 Perkhidmatan Penyampaian		
	Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dari semasa ke semasa; dan c. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Semua
0603 Perancangan dan Penerimaan Sistem Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.		
060201 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; 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.	Pentadbir Sistem ICT, ICTSO

Kandungan Dasar		Tanggungjawab
060202 Penerimaan Sistem		
	Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT , ICTSO
0603 Perisian Berbahaya Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus , Trojan dan sebagainya.		
060301 Perlindungan dari Perisian Berbahaya		
	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 mana-mana undang-undang bertulis yang sedang berkuatkuasa; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. Mengemas kini *pattern* 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

Kandungan Dasar		Tanggungjawab
0604 *Housekeeping*		
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.		
060401 *Backup*		
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Data yang ditempatkan di server-server LGM adalah di bawah tanggungjawab UTM dan backup dijalankan sepertimana yang ditetapkan di dalam Arahan Kerja AK/IT/01/01. Data yang disimpan di dalam komputer-komputer adalah tanggungjawab pemilik data tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat *backup* ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c. Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d. Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan e. Merekod dan menyimpan salinan backup di lakosi yang berlainan dan selamat. f.	Semua
0605 Pengurusan Rangkaian		
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.		
060501 Kawalan Infrastruktur Rangkaian		
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. a. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir dan gegaran;	Pentadbir Rangkaian dan Pentadbir Sistem ICT

Kandungan Dasar		Tanggungjawab
	b. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; c. Semua peralatan mestilah melalui proses *User Acceptance Test* (UAT) semasa pemasangan dan konfigurasi; d. *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem; e. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan LGM; f. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; g. Memasang perisian *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat LGM; h. Memasang *Web Content Filter* pada Internet Gateway untuk menyekat aktiviti yang dilarang; i. Sebarang penyambungan rangkaian yang bukan di bawah kawalan LGM hendaklah mendapat kebenaran ICTSO; j. Semua pengguna hanya dibenarkan menggunakan rangkaian LGM sahaja. Penggunaan modem hendaklah mendapat kebenaran ICTSO; dan k. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	

Kandungan Dasar		Tanggungjawab
0606 Pengurusan Media Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan		
060601 Penghantaran dan Pemindahan		
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pegawai Atasan terlebih dahulu.	Semua
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
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.	Pentadbir Sistem ICT, ICTSO

Kandungan Dasar		Tanggungjawab
0607 Pengurusan Pertukaran Maklumat Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara LGM dan agensi luar terjamin.		
060701 Pertukaran Maklumat		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara LGM dengan agensi luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari LGM; dan d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua
060702 Pengurusan Mel Elektronik (E-mel)		
	Penggunaan e-mel di LGM hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh LGM sahaja boleh digunakan. Penggunaan akaun milik orang lain bersama adalah dilarang; b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh LGM; c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;	Semua

Kandungan Dasar		Tanggungjawab
	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 yang tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; f. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; h. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; i. Mengambil tindakan dan memberi maklumbalas terhadap e-mel dengan cepat dan mengambil tindakan segera; dan j. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbo*x* masing-masing.	

PERKARA 07

KAWALAN CAPAIAN

Kandungan Dasar		Tanggungjawab
0701 Dasar Kawalan Capaian Objektif: Mengawal capaian ke atas maklumat		
070101 Keperluan Kawalan Capaian		
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d. Kawalan ke atas kemudahan pemprosesan maklumat.	UTM, ICTSO
0702 Pengurusan Capaian Pengguna Objektif: Mengawal capaian pengguna ke atas aset ICT LGM.		
070201 Akaun Pengguna		
	Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenalpasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh LGM sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;	Semua

Kandungan Dasar		Tanggungjawab
	c. Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan LGM. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
070202 Hak Capaian		
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
070203 Pengurusan Kata Laluan		
	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh LGM seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi;	Pentadbir Sistem ICT

Kandungan Dasar		Tanggungjawab
	c. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara; d. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g. Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan j. Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
070204 Clear Desk dan Clear Screen		
	Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; b. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Semua

Kandungan Dasar		Tanggungjawab
0703 Kawalan Capaian Sistem dan Aplikasi Objektif: Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.		
070301 Sistem Maklumat dan Aplikasi		
	Capaian sistem dan aplikasi di LGM adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah di patuhi: 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.	Pentadbir Sistem ICT, ICTSO
0704 Peralatan Komputer Mudah Alih dan Kerja Jarak Jauh Objektif: Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.		
070401 Peralatan Komputer Mudah Alih		
	Perkara yang perlu dipatuhi adalah seperti berikut: a. Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan	Semua

Kandungan Dasar		Tanggungjawab
	b. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	
070401 Kerja Jarak Jauh		
	Perkara yang perlu dipatuhi adalah seperti berikut: a. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

PERKARA 08

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Kandungan Dasar		Tanggungjawab
0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
080101 Keperluan Keselamatan		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna, dan sistem *output* untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. 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, Pentadbir Sistem ICT, ICTSO

Kandungan Dasar		Tanggungjawab
080102 Pengesahan Data Input dan Output		
	a. Data *input* bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b. Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem ICT
0802 Kriptografi Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat.		
080201 Enkripsi		
	Pengguna hendaklah membuat enkripsi ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
080202 Tandatangan Digital		
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
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

Kandungan Dasar		Tanggungjawab
0803 Keselamatan Fail Sistem Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.		
080301 Kawalan Fail Sistem		
	a. Proses mengemaskini 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 dikemas kini 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

Kandungan Dasar		Tanggungjawab
0804 Keselamatan Dalam Pembangunan dan Proses Sokongan Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.		
080401 Kawalan Perubahan		
	a. Perubahan atau pengubahsuaian ke atas sistem maklumat aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e. Menghalang sebarang peluang untuk membocorkan maklumat.	Pentadbir Sistem ICT
080401 Pembangunan Sistem Secara *Outsource*		
	Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code)* bagi semua aplikasi dan perisian adalah menjadi hak milik LGM.	Semua

PERKARA 09

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

Kandungan Dasar		Tanggungjawab
0901 Mekanisme Pelaporan Insiden Keselamatan ICT Objektif: Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.		
090101 Mekanisme Pelaporan		
	Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan GCERT dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	Semua

Kandungan Dasar		Tanggungjawab
0902 Pengurusan Maklumat Insiden Keselamatan ICT Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.		
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT		
	Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenalpasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada LGM. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; d. Menyediakan tindakan pemulihan segera; dan e. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO

PERKARA 10

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Kandungan Dasar		Tanggungjawab
1001 Dasar Kesinambungan Perkhidmatan Objektif: Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
100101 Pelan Kesinambungan Perkhidmatan		
	Pelan Kesinambungan Perkhidmatan (*Business Continuity Management - BCM*) 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 JKICT LGM. Perkara-perkara berikut perlu diberi perhatian: a. Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Mengenalpasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; c. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; d. Mendokumentasikan proses dan prosedur yang telah dipersetujui; e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; f. Membuat *backup*; dan g. Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali. Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;	Semua

Kandungan Dasar		Tanggungjawab
	b. Senarai personel LGM dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; c. Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; d. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan e. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. LGM hendaklah memastikan salinan pelan BCM sentiasa dikemaskini dan dilindungi seperti di lokasi utama.	

PERKARA 11

PEMATUHAN

Kandungan Dasar		Tanggungjawab
1101 Pematuhan dan Keperluan Perundangan Objektif: Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT LGM.		
110101 Pematuhan Dasar		
	Setiap pengguna di LGM hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT LGM dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di LGM 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. Sebarang penggunaan aset ICT LGM selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber LGM.	Semua
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal		
	ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO

Kandungan Dasar		Tanggungjawab
110103 Pematuhan Keperluan Audit		
	Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
110104 Pelanggaran Dasar		
	Pelanggaran Dasar Keselamatan ICT LGM boleh dikenakan tindakan tatatertib.	Semua