Dasar Keselamatan Teknologi Maklumat & Komunikasi (ICT)

Institut Penyelidikan dan Kemajuan Pertanian Malaysia (MARDI)
Kementerian Pertanian dan Industri Asas Tani

Januari 2007

Versi 1.0

KANDUNGAN

PENGENALAN

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

OBJEKTIF

Dasar Keselamatan ICT MARDI diwujudkan untuk menjamin kesinambungan urusan MARDI dengan meminimumkan kesan insiden keselamatan ICT.

SKOP

Dasar Keselamatan ICT MARDI meliputi aset ICT yang berikut :-

a. Data dan maklumat – Semua data dan maklumat yang disimpan atau digunakan di pelbagai media atau peralatan ICT;

b. Peralatan ICT – Semua peralatan komputer dan periferal seperti komputer peribadi, stesen kerja, kerangka utama dan alat-alat prasarana seperti *Uninterrupted Power Supply* (UPS), punca kuasa dan pendingin hawa;

c. Media Storan – Semua media storan dan peralatan yang berkaitan seperti disket, kartrij, CD-ROM, pita, cakera, pemacu cakera dan pemacu pita;

d. Komunikasi dan Peralatan Rangkaian – Semua peralatan berkaitan komunikasi seperti komputer pelayan, *gateway*, *bridge*, *router, switches, access point* dan peralatan PABX;

e. Perisian – Semua perisian yang digunakan untuk mengendali, memproses, menyimpan, menjana dan mengirim maklumat. Ini meliputi semua perisian sistem, perisian utiliti, perisian rangkaian, program aplikasi, pangkalan data, fail program dan fail data;

f. Dokumentasi – Semua dokumen yang mengandungi maklumat berkaitan dengan penggunaan dan pemasangan peralatan dan perisian. Ia juga meliputi data dalam semua bentuk media seperti salinan kekal, salinan elektronik, *transparencies*, risalah dan *slides*;

g. Manusia – Semua pengguna yang dibenarkan termasuk pentadbir dan pengurus serta mereka yang bertanggungjawab terhadap keselamatan ICT; dan

h. Premis Komputer dan Komunikasi – Semua kemudahan serta premis yang diguna untuk menempatkan perkara a – g di atas.

Dasar ini adalah terpakai kepada semua pengguna di MARDI termasuk kakitangan, pembekal dan pakarunding yang mencapai, mengurus, menyelenggara, memproses, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT MARDI.

PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT MARDI dan perlu dipatuhi adalah seperti yang 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 khas ke atas maklumat MARDI 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 terhadap semua tindakannya terhadap aset ICT MARDI;

d. **Pengasingan**

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

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 mampu menjana dan menyimpan log tindakan keselamatan atau *pantomim trail*;

f. **Pematuhan**

Dasar Keselamatan ICT MARDI 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 mencorak sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

Perkara 01 Pembangunan dan Penyelenggaraan Dasar

Dasar Keselamatan ICT		
DM-010101	**Pelaksanaan Dasar**	
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah MARDI dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), dan semua Pengarah Pusat/Bahagian/Ketua Unit.	Ketua Pengarah
DM-010102	**Penyebaran Dasar**	
	Dasar ini perlu disebarkan kepada semua pengguna MARDI (termasuk kakitangan, pembekal, pakar runding dll.)	ICTSO
DM-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 MARDI: a. kenal pasti dan tentukan perubahan yang diperlukan; b. kemuka cadang pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Pengurusan MARDI (MPM); c. perubahan yang telah dipersetujui oleh JPKM dimaklumkan kepada semua pengguna; dan d. dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.	ICTSO
DM-010104	**Pengecualian Dasar**	
	Dasar Keselamatan ICT MARDI adalah terpakai kepada semua pengguna ICT MARDI dan **TIADA** pengecualian diberikan.	Semua

Perkara 02 Keselamatan Organisasi

Infrastruktur Keselamatan Organisasi		
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.		
DM-020101 Ketua Pengarah		
	Peranan dan tanggungjawab Ketua Pengarah adalah seperti yang berikut: a. memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT MARDI; b. memastikan semua pengguna mematuhi Dasar Keselamatan ICT MARDI; 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 MARDI.	Ketua Pengarah
DM-020102 Ketua Pegawai Maklumat (CIO)		
	Timbalan Ketua Pengarah (Penyelidikan) MARDI adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggung jawab beliau adalah seperti yang 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
DM-020103 Pegawai Keselamatan ICT (ICTSO)		
	Seorang Pegawai Kanan di Bahagian Pengurusan Sumber Maklumat MARDI yang dilantik sebagai ICTSO mempunyai peranan dan tanggungjawab seperti yang berikut: a. mengurus keseluruhan program keselamatan ICT MARDI; b. menguatkuasakan Dasar Keselamatan ICT MARDI; c. memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT MARDI kepada semua pengguna;	ICTSO

	d. mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT MARDI; e. menjalankan pengurusan risiko; f. menjalankan audit, mengkaji semula, merumus tindak balas pengurusan 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) MAMPU 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 terhadap pengguna yang melanggar Dasar Keselamatan ICT MARDI; dan k. menyediakan dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
DM-020104 Pengarah IS		
	Peranan dan tanggungjawab Pengarah IS adalah seperti yang berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT MARDI; b. mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan MARDI; c. menentukan kawalan akses semua pengguna terhadap aset ICT MARDI; d. melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan e. menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT MARDI.	Pengarah IS
DM-020105 Pentadbir Sistem ICT		
	Timbalan Pengarah Program Rangkaian Komputer di Bahagian Pengurusan Sumber Maklumat merupakan Pentadbir Sistem ICT MARDI. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti yang berikut:	Pentadbir Sistem ICT

	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 dalam Dasar Keselamatan ICT MARDI; c. memantau aktiviti capaian 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 mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	
DM-020106	**Pengguna**	
	Peranan dan tanggungjawab pengguna adalah seperti yang berikut: a. membaca, memahami dan mematuhi Dasar Keselamatan ICT MARDI; b. mengetahui dan memahami implikasi keselamatan ICT kesan daripada tindakannya; c. lulus tapisan keselamatan; d. melaksanakan prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat MARDI; e. melaksanakan langkah-langkah perlindungan seperti yang berikut :- 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 daripada diketahui umum. f. melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;	Pengguna

	g. menghadiri program kesedaran mengenai keselamatan ICT; dan h. menandatangani surat akuan pematuhan Dasar Keselamatan ICT MARDI.	
Pihak Ketiga Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.		
DM-020201	**Keperluan Keselamatan Kontrak dengan Pihak Ketiga**	
	Akses kepada aset ICT MARDI perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dimasukkan dalam perjanjian yang dimeterai. a. Dasar Keselamatan ICT MARDI; b. Tapisan Keselamatan; c. Perakuan Akta Rahsia Rasmi 1972; d. Hak Harta Intelek; Nota 1: 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.	CIO, ICTSO, Pengarah IS, Pentadbir Sistem ICT dan Pihak Ketiga

Perkara 03 Pengawalan dan Pengelasan Aset

Akauntabiliti Aset Objektif : Memberi dan menyokong perlindungan yang bersesuaian terhadap semua aset ICT MARDI.		
DM-030101 Inventori Aset		
	Semua aset ICT MARDI hendaklah direkodkan. Ini termasuklah mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Setiap pengguna adalah bertanggung jawab terhadap semua aset ICT di bawah tanggungjawabnya.	Pentadbir Sistem Semua
Pengendalian dan Pengelasan Maklumat Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.		
DM-030201 Pengelasan Maklumat		
	Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan dalam dokumen Arahan Keselamatan seperti yang berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	Semua
DM-030202 Pengendalian Maklumat		
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, pertukaran dan pemusnahan 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; d. menjaga kerahsiaan kata laluan;	Semua

	e. mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, menuukar dan memusnah; dan g. menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.	

Perkara 04 Keselamatan Sumber Manusia

Kawalan Dalam Definisi Tugas dan Kedapatan Sumber Objektif: Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT MARDI.		
DM-040101	**Tanggungjawab Keselamatan Semasa Dalam Perkhidmatan**	
	Peranan dan tanggungjawab keselamatan semasa dalam perkhidmatan bagi setiap pengguna MARDI mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan sama ada melalui fail meja atau termaktub dalam kontrak. Merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan terhadap semua aset atau sumber ICT yang dimiliki atau digunakan dalam melaksanakan pekerjaan.	Semua
DM-040102	**Terma dan Syarat Perkhidmatan**	
	Semua warga MARDI yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa.	Semua
DM-040103	**Perakuan Akta Rahsia Rasmi**	
	Warga MARDI yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua
Menangani Insiden Keselamatan ICT Objektif: Meminimumkan kesan insiden keselamatan ICT.		
DM-040201	**Pelaporan Insiden**	
	Insiden keselamatan ICT seperti yang berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada 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, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerapkali gagal dan komunikasi tersalah hantar; e. Berlaku percubaan menceroboh, penyelewengan dan insiden yang tidak diingini.	Semua

	Nota 2: Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan ICT" mengenainya bolehlah dirujuk.	
Pendidikan Objektif: Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.		
DM-040301 Program Kesedaran Keselamatan ICT-		
	Setiap pengguna di MARDI perlu diberikan latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT MARDI.	ICTSO
Tindakan Tatatertib Objektif: Meningkatkan kesedaran dan pematuhan terhadap Dasar Keselamatan ICT MARDI.		
DM-040401 Pelanggaran Dasar		
	Pelanggaran Dasar Keselamatan ICT MARDI akan dikenakan tindakan tatatertib.	Semua

Perkara 05 Keselamatan Fizikal

Keselamatan Kawasan Objektif : Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.		
DM-050101	**Perimeter Keselamatan Fizikal**	
	Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah yang berikut : a. 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; b. memperkukuh tingkap dan pintu serta dikunci untuk mengawal kemasukan; c. Memperkukuh dinding dan siling; d. Memasang alat penggera atau kamera; e. Mengehadkan jalan keluar masuk; f. Mengadakan kaunter kawalan; g. Menyediakan tempat atau bilik khas untuk pelawat; dan h. Mewujudkan perkhidmatan pengawalan keselamatan.	Pejabat Ketua Pegawai Keselamatan MARDI, CIO dan ICTSO
DM-050102	**Kawalan Masuk Fizikal**	
	a. Setiap pengguna MARDI hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; c. Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara; d. Setiap pelawat hendaklah mendaftar di pintu utama MARDI (Pintu 1,2 dan 3) terlebih dahulu; e. Kehilangan pas mestilah dilaporkan dengan segera; f. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT MARDI;	Semua dan pelawat

DM-050103	**Kawasan Larangan**	
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai yang tertentu sahaja, ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di MARDI ialah bilik Ketua Pengarah, bilik-bilik Timbalan Ketua Pengarah, bilik Pusat Data di tingkat bawah Blok C, bilik kemasukan data di Tingkat 1 Blok B. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja : a. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan apabila perlu. b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan c. Semua penggunaan peralatan yang melibatkan penghantaran, pengemas kinian dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Pengarah Pusat/Bahagian dan Ketua Unit.	Semua
	Keselamatan Peralatan	
Objektif : Melindung peralatan dan maklumat.		
DM-050201	**Perkakasan**	
	Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan apabila perlu: a. Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna; b. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; c. Setiap pengguna adalah bertanggungjawab terhadap kerosakan atau kehilangan perkakasan ICT di bawah kawalannya; dan d. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO.	Semua
DM-050202	**Dokumen**	
	Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti yang berikut hendaklah dipatuhi:	Semua

	a. memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b. menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; dan c. menggunakan penyulitan terhadap dokumen terperingkat yang disedia dan dihantar secara elektronik.	
DM-050203	**Media Storan**	
	Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti yang berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat : a. Menyediakan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; c. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan d. Media storan sebagai *backup* hendaklah direkodkan pergerakannya.	Semua
DM-050204	**Kabel**	
	Kabel komputer hendaklah dilindungi untuk mengelakkan pendedahan maklumat. Langkah-langkah keselamatan yang perlu diambil adalah seperti yang berikut : a. Menggunakan kabel mengikut spesifikasi yang telah ditetapkan; b. Kabel hendaklah dilindungi daripada kerosakan yang disengajakan atau tidak disengajakan; dan c. Laluan pemasangan kabel hendaklah dilindungi sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*.	IS & ICTSO
DM-050205	**Penyelenggaraan**	
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti. a. Semua perkakasan yang diselenggarakan hendaklah	Semua

	mematuhi spesifikasi pengeluar yang telah ditetapkan; b. Perkakasan 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 Pusat/Bahagian/Ketua Unit berkenaan.	
DM-050206	**Peminjaman Perkakasan Untuk Kegunaan di Luar Pejabat**	
	Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan : a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan Pengarah Pusat/Bahagian/Ketua Unit/Pengurus Stesen dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	Semua
DM-050207	**Peralatan di Luar Premis**	
	Bagi perkakasan yang dibawa keluar dari premis MARDI, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan MARDI: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan c. Semua peralatan di luar premis hendaklah direkod dan mendapat kebenaran daripada Pengarah Pusat/Bahagian/Ketua Unit/Pengurus Stesen berkenaan.	Semua
DM-050208	**Pelupusan**	
	Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan MARDI: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, disguising* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan	Semua

	c. Maklumat lanjut pelupusan bolehlah merujuk kepada Surat Pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk "Garis Panduan Pelupusan Peralatan Komputer".	
DM-050209	***Clear Desk* dan *Clear Screen***	
	Semua maklumat dalam apa jua bentuk media hendaklah di simpan 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 : a. Gunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; b. Bahan-bahan sensitif hendaklah disimpan di dalam laci atau kabinet fail yang berkunci; dan c. Dokumen yang mengandungi bahan-bahan sensitif hendaklah diambil segera dari pencetak.	Semua
	Keselamatan Persekitaran	
Objektif: Melindungi aset ICT MARDI daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.		
DM-050301	**Kawalan Persekitaran**	
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, mengubahsuai, membeli hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan MARDI. 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 perkomputeran 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 perkomputeran; 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	Semua

	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**	
	a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti UPS (*Uninterruptible Power Supply*) dan jana kuasa (*generator*) boleh digunakan bagi perkhidmatan kiritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan. c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	IS, ICTSO, KJ
DM-050303	**Prosedur Kecemasan**	
	a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MARDI 2006; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Pusat/Bahagian/Unit/Stesen yang dilantik.	Semua

Perkara 06 Pengurusan Operasi dan Komunikasi

Pengurusan Prosedur Operasi Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.		
DM-060101	**Pengendalian Prosedur**	
	a. Semua prosedur keselamatan ICT yang diwujudkan, dikenal pasti dan masih diguna pakai hendaklah didokumentasikan, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang lengkap, teratur dan jelas seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua
DM-060102	**Kawalan Perubahan**	
	a. Pengubahsuaian yang melibatkan perkakasan, sistem pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua
DM-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;	Jawatankuasa Pemandu ICT MARDI, CIO, ICTSO

	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.		
DM-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
DM-060202	**Penerimaan Sistem**	
	Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	IS, ICTSO
Perisian Berbahaya Objektif : Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan.		
DM-060301	**Perlindungan daripada 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 hak cipta terpelihara; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. Mengemas kini *pattern* anti virus dari semasa ke semasa; 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 dalam mana-mana	Semua

	kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini akan digunakan sekiranya perisian tersebut mengandungi program berbahaya; dan h. Mengadakan program dan prosedur jaminan kualiti terhadap semua prisian yang dibangunkan. (* g & h perlu dikajisemula) i. Mengedarkan amaran mengenai ancaman seperti serangan virus terhadap keselamatan aset ICT MARDI.	
Housekeeping Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.		
DM-060401 Penduaan		
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan backup hendaklah dilakukan setiap kali konfigurasi berubah. Salinan *backup* hendaklah direkodkan dan disimpan dalam lokasi yang selamat. a. Membuat salinan keselamatan bagi semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat salinan *backup* ke atas semua data dan maklumat mengikut kesesuaian operasi; dan c. Menguji sistem *backup* sedia ada bagi memastikan ia dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	Semua
DM-060402 Sistem Log		
	a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Pentadbir Sistem ICT dan ICTSO
Pengurusan Rangkaian Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.		
DM-060501 Kawalan Infrastruktur Rangkaian		
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan :- a. Tanggungjawab atau kerja-kerja operasi rangkaian dan	Pentadbir Sistem ICT

	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 daripada 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 yang dibenarkan sahaja; f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan MARDI; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer peribadi kecuali mendapat kebenaran ICTSO; h. Memasang perisian *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat MARDI; i. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti kemasukan dari atau capaian pada laman web/Internet yang mengandungi maklumat atau unsur-unsur tidak sihat dan berbahaya yang boleh menjejaskan integriti kakitangan, sistem dan maklumat; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan MARDI hendaklah mendapat kebenaran ICTSO; k. Semua pengguna hanya dibenarkan menggunakan rangkaian MARDI 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 daripada kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.

DM-060601	**Penghantaran dan Pemindahan**	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pengarah Pusat/Bahagian/Ketua Unit/Pengurus Stesen terlebih dahulu.	Semua

DM-060602	**Penghapusan**	
	Media yang mengandungi maklumat rahsia rasmi hedaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	Semua
DM-060603	**Prosedur Pengendalian Maklumat**	
	a. Semua media hendaklah dilabelkan mengikut tahap sensiviti sesuatu maklumat; b. Mengehadkan dan menentukan capaian kepada pengguna yang sah sahaja; c. Mengehadkan pengedaran data untuk tujuan yang dibenarkan; d. Penyelenggaraan media hendaklah dikawal dan direkodkan bagi mengelakkan sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan e. Semua media hendaklah disimpan di tempat yang selamat.	Semua
DM-060604	**Keselamatan Sistem Dokumentasi**	
	a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyediakan dan memantapkan lagi keselamatan sistem dokumentasi dalam rangkaian; dan c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	IS & ICTSO
	Keselamatan Komunikasi	
Objektif: Melindungi aset ICT melalui sistem komunikasi yang selamat.		
DM-060701	**Internet**	
	a. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan; b. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan; c. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet; d. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan	Semua

	oleh MARDI; f. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; dan 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".	
DM-060702	**Mel Elektronik**	
	a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh MARDI sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Dalam keadaan tidak boleh tidak, setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh MARDI; 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. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; f. Pengguna dinasihatkan tidak 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; dan k. Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada Pekeliling Kemajuan	Semua

	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 MARDI.		
DM-070101 Keperluan Dasar		
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkod, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	Pengarah IS, ICTSO
Pengurusan Capaian Pengguna Objektif : Mengawal capaian pengguna terhadap aset ICT MARDI.		
DM-070201 Akaun Pengguna		
	Pengguna adalah bertanggungjawab terhadap sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: a. akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b. akaun pengguna mestilah unik; c. akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. 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 yang berikut: i) Bertukar ke agensi lain; ii) Bersara; atau iii) Ditamatkan perkhidmatan.	Semua
DM-070202 Jejak Audit		
	Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi: a. maklumat identiti pengguna, sumber yang digunakan,	Pentadbir Sistem ICT

	perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b. aktiviti capaian pengguna terhadap sistem ICT sama ada secara sah atau sebaliknya; dan c. maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pentadbir sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
Kawalan Capaian Sistem dan Aplikasi Objektif: Melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.		
DM-070301	**Sistem Maklumat dan Aplikasi**	
	Capaian sistem dan aplikasi di MARDI adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: a. pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti yang tidak diingini; c. memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d. menghadekan 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.	IS & ICTSO
Peralatan Komputer Mudah Alih Objektif : Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.		
DM-070401	**Penggunaan Peralatan Komputer Mudah Alih**	
	a. Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; b. Komputer mudah alih hendaklah disimpan dan dikunci di	Semua

	tempat yang selamat apabila tidak digunakan; dan c. Capaian sistem dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimana pun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	

Perkara 08 Pembangunan dan Penyelenggaraan Sistem

Keselamatan Dalam Membangunkan Sistem dan Aplikasi Objektif : Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.		
DM-080101	**Keperluan Keselamatan**	
	a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan terhadap 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 c. Sebaiknya-baiknya, semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji dan diperakui terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Semua
Kriptografi Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat.		
DM-080201	**Penyulitan**	
	Setiap pengguna hendaklah membuat penyulitan terhadap semua sistem yang melibatkan maklumat sensitif atau kritikal bagi mengelakkan daripada pendedahan dan penyelewengan maklumat berlaku.	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 daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua

Sistem Fail		
Objektif: Memastikan supaya sistem fail dan aktiviti berkaitan beroperasi dengan baik dan selamat.		
DM-080301	**Kawalan Sistem Fail**	
	a. Menyediakan kawalan keselamatan yang kukuh semasa melaksanakan perisian atau sistem aplikasi bagi mengurangkan risiko kerosakan kepada sistem pengoperasian; b. Proses pengemas kini sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; c. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksana atau digunakan selepas diuji dan diperakui; d. Mengawal capaian terhadap kod atau atur cara program bagi mengelakkan kerosakan, pengubah suaian tanpa kebenaran, penghapusan dan kecurian program komputer; dan e. Mengaktifkan audit log bagi merekod semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	IS
Pembangunan dan Proses Sokongan		
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.		
DM-080401	**Kawalan Perubahan**	
	Perubahan atau pengubahsuaian sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod dan disahkan sebelum digunapakai.	IS

Perkara 09 Pengurusan Kesinambungan Perkhidmatan

Dasar Kesinambungan Perkhidmatan		
Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
DM-090101	**Pelan Kesinambungan Perkhidmatan**	
	Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan untuk memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diperakukan oleh Mesyuarat Pengurusan MARDI (JPKM) dan perkara-perkara yang berikut perlu diberi perhatian: a. mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; c. mendokumentasikan proses dan prosedur yang telah dipersetujui; d. mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; dan e. menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	Semua
DM-090102	**Penduaan**	
	a. Membuat penduaan sistem ICT sebagai kontigensi bagi memastikan pemulihan dapat dilaksanakan; b. Penduaan hendaklah dibuat secara berkala bagi mengurangkan beban pembangunan semula serta mempercepat proses pemulihan sistem; c. Salinan penduaan mesti disimpan dengan selamat dan dikawal; dan d. Prosedur pemulihan mestilah disemak dan diuji secara berjadual bagi memastikan prosedur berkenaan sentiasa boleh dipraktikkan.	Semua

Perkara 10 Pematuhan

Pematuhan dan Keperluan Perundangan		
Objektif: Meningkatkan tahap keselamatan ICT bagi mengelakkan pelanggaran kepada Dasar Keselamatan ICT MARDI.		
DM-100101	**Pematuhan Dasar**	
	Setiap pengguna di MARDI hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT MARDI dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di MARDI termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan bukannya di bawah kuasa mutlak individu.	Semua
DM-100102	**Keperluan Perundangan**	
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di MARDI: a. Arahan Keselamatan MARDI; b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"; c. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); d. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; e. Akta Tandatangan Digital 1997; f. Akta Jenayah Komputer 1997; g. Akta Hakcipta (Pindaan) Tahun 1997; h. Akta Komunikasi dan Multimedia 1998; dan i. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS).	Semua