DASAR KESELAMATAN ICT

KEMENTERIAN KESIHATAN MALAYSIA

13 Februari 2013

No Semakan 4.0

RUJUKAN	NO SEMAKAN	M/SURAT
DKICT KKM	4.0	1

SEJARAH DOKUMEN

TARIKH	NO SEMAKAN	KELULUSAN	TARIKH KUAT KUASA
9 Februari 2010	Versi 2.0	JPICT	23 April 2010
16 Ogos 2011	Versi 3.0	JPICT	20 September 2011
4 Disember 2012	No Semakan 4.0	JPICT	13 Februari 2013

KANDUNGAN — MUKA SURAT

PENGENALAN

Dasar Keselamatan ICT Kementerian Kesihatan Malaysia (DKICT KKM) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) KKM. Dasar ini juga menerangkan kepada semua pengguna di KKM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KKM.

OBJEKTIF

DKICT KKM diwujudkan untuk memastikan tahap keselamatan ICT KKM terurus dan menjamin kesinambungan urusan KKM dengan meminimumkan kesan insiden keselamatan ICT.

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi KKM. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT KKM adalah seperti berikut:

(a) Memastikan kelancaran operasi KKM dan meminimumkan kerosakan atau kemusnahan;
(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan
(c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

SKOP

Dasar ini meliputi pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut :

(a) Peralatan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan KKM.

Contoh: komputer, pelayan, peralatan komunikasi, media magnetik dan sebagainya;

(b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT.

Contoh: perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada KKM;

(c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya.

Contoh:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

(d) Data atau Maklumat

Koleksi fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat untuk digunakan bagi mencapai misi dan objektif KKM.

Contoh: sistem dokumentasi, prosedur operasi, rekod KKM, profil pelanggan, pangkalan data, maklumat arkib dan lain-lain;

(e) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian KKM bagi mencapai misi dan objektif fasiliti. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan;

(f) Premis Komputer Dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara **(a) - (e)** di atas; dan

(g) Dokumentasi

Semua dokumentasi 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*.

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran DKICT KKM.

Dasar ini adalah terpakai oleh semua pengguna di KKM termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT KKM.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT KKM 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 dan 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, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu 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 KKM.

Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

(d) Pengasingan

Tugas mewujud, memadam, kemaskini, 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 ICT.

Dengan itu, aset ICT seperti komputer, pelayan *(server), router, firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

(f) Pematuhan

DKICT KKM hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk perlanggaran 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 *(backup)* 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 kaedah keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

PENILAIAN RISIKO KESELAMATAN ICT

Pegawai Keselamatan ICT (ICTSO) hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu ICTSO perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

ICTSO hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan Keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat KKM termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

ICTSO bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: GarisPanduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

ICTSO perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

(a) mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
(b) menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan agensi;
(c) mengelak dan/atau mencegah risiko dari terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
(d) memindahkan risiko ke pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

PERKARA 01

PEMBANGUNAN DAN PENGEMASKINIAN DASAR

Dasar Keselamatan ICT KKM		
Objektif:	Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan KKM dan perundangan yang berkaitan.	
	01-01 Pelaksanaan Dasar	**T/jawab**
Tanggungjawab melaksanakan dasar	Ketua Setiausaha KKM adalah bertanggungjawab ke atas pelaksanaan arahan dengan dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), dan lain-lain pegawai yang dilantik. CIO bertanggungjawab memastikan hala tuju pengurusan organisasi untuk melindungi aset ICT selaras dengan keperluan pentadbiran.	Ketua Setiausaha KKM,CIO,ICTSO CIO
	01-02 Penyebaran Dasar	
Sebaran	Dasar ini perlu disebarkan kepada semua pengguna KKM (termasuk kakitangan, pembekal dan pakar runding yang berurusan dengan KKM).	ICTSO
	01-03 Pengemaskinian Dasar	
Penyelarasan mengikut perubahan dan keperluan semasa	DKICT KKM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Prosedur penyelenggaraan DKICT KKM adalah seperti berikut: (a) Mengkaji semula dasar ini sekurang-kurangnya sekali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan; (b) Mengemukakan cadangan perubahan secara bertulis kepada **CIO** untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KKM; dan (c) Memaklumkan perubahan dasar yang telah dipersetujui oleh JPICT kepada semua pengguna KKM.	ICTSO
	01-04 Pemakaian Dasar	
Pemakaian dan tiada pengecualian	DKICT KKM ini hendaklah dibaca, difahami dan dipatuhi oleh semua warga KKM. DKICT KKM adalah terpakai kepada semua pengguna ICT KKM dan tiada pengecualian diberikan.	Semua Pengguna KKM,

PERKARA 02

ORGANISASI KESELAMATAN

Organisasi Keselamatan		
Objektif :	Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT KKM.	
	02-01 Ketua Setiausaha KKM	**T/jawab**
Peranan dan tanggungjawab Ketua Setiausaha KKM	Peranan dan tanggungjawab Ketua Setiausaha KKM adalah seperti berikut: (a) Memastikan pelaksanaan peranan pasukan penyelaras keselamatan ICT KKM; (b) Memastikan semua pengguna KKM mematuhi DKICT; (c) Memastikan semua keperluan KKM (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT KKM; dan (e) Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), KKM.	Ketua Setiausaha KKM
	02-02 Struktur Dalaman Organisasi	
	Struktur formal dalam KKM diwujudkan untuk mengurus keselamatan ICT organisasi. Perkara yang perlu dipatuhi termasuk yang berikut: (a) Komitmen pengurusan ke atas keselamatan ICT dilaksanakan dengan aktif dan telus; (b) Aktiviti pengurusan keselamatan ICT diselaraskan oleh wakil dari semua peringkat KKM berdasarkan peranan masing-masing; (c) Tanggungjawab semua yang terlibat dalam pengurusan keselamatan ICT adalah jelas; (d) Proses kebenaran menggunakan kemudahan proses maklumat dikenal pasti dan dilaksana; (e) Keperluan untuk pengurusan kerahsiaan maklumat dikenal pasti, dilaksanakan dan dikaji secara berkala; (f) Memastikan jalinan perhubungan/komunikasi dengan pihak yang relevan dipelihara; dan (g) Memastikan kajian semula ke atas keselamatan maklumat dijalankan mengikut peraturan yang ditetapkan.	CIO dan ICTSO

PERKARA 02

ORGANISASI KESELAMATAN

	02-03 Peranan Ahli Pasukan Penyelaras Keselamatan ICT	
Objektif :	Menerangkan peranan dan tanggungjawab ahli pasukan penyelaras keselamatan ICT KKM.	
	02-03-01 Ketua Pegawai Maklumat (CIO)	
Peranan dan tanggungjawab CIO	Peranan dan tanggungjawab adalah termasuk seperti berikut: (a) Mewujud dan mengetuai pasukan penyelaras keselamatan ICT KKM; (b) Menasihati Ketua Setiausaha KKM dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (c) Menentukan keperluan keselamatan ICT; (d) Menyelaras pembangunan dan pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan (e) Memastikan semua pengguna KKM memahami peruntukan di bawah DKICT KKM.	CIO
	02-03-02 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO	**(i) Pegawai Keselamatan ICT Ibu Pejabat KKM (ICTSO IP KKM)** Peranan dan tanggungjawab adalah termasuk seperti berikut: (a) Mengurus, menyedia dan melaksanakan keseluruhan program-program keselamatan ICT KKM; (b) Menguatkuasa DKICT KKM; (c) Memberi penerangan dan pendedahan berkenaan DKICT KKM kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur atau tatacara selaras dengan keperluan DKICT KKM; (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 CIO dan Pasukan Pengendalian Insiden Keselamatan ICT MAMPU (GCERT);	ICTSO IP KKM

		(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 gagal mematuhi DKICT KKM; (k) Memantau pematuhan DKICT KKM; (l) Memperakukan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan dan pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan (m) Menyelaras Pengurusan Kesinambungan Perkhidmatan KKM	
	(ii)	**Pegawai Keselamatan ICT Negeri (ICTSO Negeri)** Peranan dan tanggungjawab adalah termasuk seperti berikut: (a) Memberi penerangan dan pendedahan berkenaan DKICT KKM kepada semua pengguna; (b) Menjalankan pengurusan risiko; (c) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (d) Melaporkan insiden keselamatan ICT kepada CERT KKM (e) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; (f) Memantau pematuhan DKICT KKM; (g) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan (h) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan dan pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan;	ICTSO Negeri

	02-03-03 Pasukan Pengendalian Insiden Keselamatan ICT KKM (CERT KKM)	
Peranan dan tanggungjawab CERT KKM	Peranan dan tanggungjawab CERT KKM adalah seperti berikut: (a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; (b) Merekod dan menjalankan siasatan awal insiden yang diterima; (c) Menangani tindak balas *(response)* insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; (d) Menasihati ICTSO KKM mengambil tindakan pemulihan dan pengukuhan; (e) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada KKM; dan (f) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	CERT KKM
	02-03-04 Pengurus ICT	
Peranan dan tanggungjawab Pengurus Komputer	Peranan dan tanggungjawab adalah termasuk seperti berikut: (a) Menentukan kawalan akses semua pengguna terhadap aset ICT kerajaan; (b) Menentukan tahap kawalan akses semua pengguna terhadap aset ICT kerajaan; (c) Melaporkan sebarang perkara atau penemuan / ancaman keselamatan ICT kepada ICTSO; (d) Memastikan kajian semula ke atas keselamatan maklumat dijalankan mengikut peraturan yang ditetapkan; dan (e) Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KKM dilaksanakan.	Penyelaras ICT Fasiliti
	02-03-05 Pentadbir Sistem ICT dan Penyelaras ICT	
Peranan dan tanggungjawab Pentadbir Sistem ICT / Penyelaras ICT	Peranan dan tanggungjawab adalah termasuk seperti berikut: (a) Memastikan kerahsiaan kata laluan aset ICT; (b) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas;	Pentadbir Sistem ICT dan Penyelaras ICT

	(c) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek; (d) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT KKM; (e) Memantau aktiviti capaian harian sistem aplikasi pengguna; (f) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (g) Menyimpan dan menganalisis rekod *audit trail*; (h) Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; (i) Bertanggungjawab memantau setiap peralatan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; dan (j) Bertanggungjawab memastikan setiap perolehan perisian ICT adalah tulen.	
	02-03-06 Pengguna ICT KKM	
	Peranan dan tanggungjawab adalah termasuk seperti berikut: (a) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (b) Melepasi tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi (jika berkaitan); (c) Melaksanakan prinsip-prinsip DKICT KKM dan menjaga kerahsiaan maklumat kerajaan; (d) Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Memastikan perisian ICT yang di instalasi adalah tulen dan sah;	Semua Pengguna KKM

	iv. Menentukan maklumat sedia untuk digunakan; v. Menjaga kerahsiaan kata laluan; vi. Mematuhi piawaian, prosedur, tatacara, langkah atau garis panduan keselamatan yang ditetapkan;dan vii. Memastikan kawalan maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan dipatuhi. (e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO agensi masing-masing dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan (g) Menandatangani Surat Akuan Pematuhan DKICT KKM.	
	02-04 Pihak Luar / Ketiga	
	Pihak KKM hendaklah memastikan keselamatan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar / ketiga dikawal. Perkara yang perlu dipatuhi adalah termasuk seperti berikut: (a) Pihak luar / ketiga hendaklah membaca, memahami dan mematuhi DKICT KKM; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat dan melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum membenarkan capaian atau penggunaan kepada pihak luar / ketiga; (d) Memastikan akses capaian kepada aset ICT KKM perlu berlandaskan kepada perjanjian kontrak; (e) Memastikan semua keperluan keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga; dan Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai: i. Surat Akuan Pematuhan Dasar Keselamatan ICT KKM; ii. Tapisan Keselamatan (KPKK11);	CIO, ICTSO Pentadbir Sistem ICT dan Penyelaras ICT Fasiliti KKM serta Pihak Luar / Ketiga

	iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. (f) Memastikan pihak ketiga menandatangani Surat Tapisan Keselamatan, Surat Akuan Pematuhan DKICT KKM dan Perakuan Akta Rahsia Rasmi 1972.	

PERKARA 03

KAWALAN DAN PENGELASAN ASET

Akauntabiliti Aset		
Objektif :	Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KKM. Memastikan semua aset ICT KKM sentiasa di dalam keadaan baik dan selamat.	
	03-01 Tanggungjawab ke atas Aset ICT	**T/jawab**
	Memastikan semua aset ICT Kerajaan diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset direkodkan dan sentiasa dikemaskini; (b) Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (c) Peraturan bagi penggunaan aset hendaklah dipatuhi seperti Pekeliling Perbendaharaan Tatacara Aset; (d) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Semua Pengguna KKM dan Pegawai Aset
	03-02 Pengelasan dan Pengendalian Maklumat	
Objektif:	Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan tahap sensitiviti masing-masing	
	03-02-01 Pengelasan Maklumat	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada KKM. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: i. Rahsia Besar; ii. Rahsia; iii. Sulit; atau iv. Terhad. (b) Maklumat hendaklah dilabel dan dikendali berasaskan peringkat keselamatan yang dikenal pasti selaras dengan peraturan prosedur yang ditetapkan oleh KKM. Maklumat Rekod Perubatan Pesakit perlu dirahsiakan tertakluk kepada Arahan Pekeliling Ketua Pengarah Kesihatan Bil 17/2010 (Garispanduan Pengendalian dan Pengurusan Rekod Perubatan Pesakit bagi Hospital-Hospital dan Institusi Perubatan)	Semua Pengguna KKM

	03-02-02 Pengendalian Maklumat	
	Aktiviti pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa, menyemak maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Memastikan menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi piawaian, prosedur, tatacara dan garis panduan keselamatan yang dikeluarkan dari semasa ke semasa; (f) Memberi perhatian kepada pengendalian maklumat rahsia rasmi terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah pengurusan pengendalian maklumat rahsia rasmi keselamatan ICT dari diketahui umum.	Semua Pengguna KKM

PERKARA 04

KESELAMATAN SUMBER MANUSIA

Keselamatan Sumber Manusia		
Objektif:	Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan KKM, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga KKM hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
Peranan dan tanggungjawab Ketua Setiausaha KKM	Ketua Setiausaha KKM adalah bertanggungjawab ke atas sumber manusia yang terlibat secara langsung atau tidak langsung dengan maklumat dan kemudahan proses maklumat di bawah kawalannya.	
	04-01 Sebelum Berkhidmat	**T/jawab**
	Memastikan penjawat awam, kontraktor, pihak luar / ketiga dan lain-lain pihak yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT Kerajaan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab penjawat awam, kontraktor, pihak luar / ketiga dan lain-lain pihak yang berkepentingan ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan penyaringan dan pengesahan latar belakang calon untuk penjawat awam, kontraktor, pihak luar / ketiga dan lain-lain pihak yang berkepentingan hendaklah dilakukan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (c) Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua Pengguna KKM
	04-02 Dalam Perkhidmatan	
	Memastikan semua pengguna KKM peka akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT KKM dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT Kerajaan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua pengguna KKM mengurus keselamatan berdasarkan perundangan dan peraturan yang ditetapkan oleh KKM;	Semua Pengguna KKM

	(b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan ICT diberi kepada semua pengguna KKM dan sekiranya perlu diberi kepada kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas semua pengguna KKM sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan KKM; dan (d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	
	04-03 Tamat Perkhidmatan atau Bertukar	
	Peraturan dan prosedur semasa tamat perkhidmatan atau bertukar dari KKM perlu dipatuhi seperti berikut: (a) Memastikan semua aset ICT Kerajaan dikembalikan kepada KKM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan KKM dan/atau terma perkhidmatan.	Semua Pengguna KKM

PERKARA 05

KESELAMATAN FIZIKAL DAN PERSEKITARAN

	05-01 Keselamatan Kawasan	
Objektif :	Melindungi premis dan aset ICT daripada sebarang bentuk pencerobohan, ancaman, kecurian, kerosakan , gangguan serta akses yang tidak dibenarkan.	
	05-01-01 Perimeter Keselamatan Fizikal	**T/jawab**
	Keselamatan Fizikal adalah bertujuan untuk mengesan, mencegah dan menghalang cubaan untuk menceroboh ke kawasan yang menempatkan peralatan, maklumat dan kemudahan proses maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti kawasan keselamatan fizikal dengan jelas, dan lokasi serta keteguhan kawasan ini hendaklah bergantung kepada keperluan untuk melindungi aset dalam kawasan ini dan hasil penilaian risiko; (b) Mempamerkan papan tanda kawasan larangan; (c) Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; (d) Memperkukuhkan dinding dan siling; (e) Jalan keluar masuk; (f) Mengadakan kaunter kawalan; (g) Mewujudkan sistem pas keselamatan; (h) Menyediakan tempat dan bilik khas untuk pelawat; (i) Mewujudkan perkhidmatan kawalan keselamatan; (j) Memasang alat penggera atau kamera (CCTV) jika berkaitan; (k) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (l) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; (m) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad seperti Pusat Data dan sebagainya; dan (n) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Pegawai Keselamatan Agensi Masing-masing, CIO, ICTSO

PERKARA 05

KESELAMATAN FIZIKAL DAN PERSEKITARAN

	05-01-02. Kawalan Keluar Dan Masuk Fizikal	
	Kawalan keluar dan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis/bangunan KKM. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna KKM hendaklah memakai pas keselamatan sepanjang masa berada di permis; (b) Semua pas keselamatan hendaklah diserahkan balik apabila pengguna bertukar agensi, berhenti atau bersara; (c) Pihak luar/pelawat wajib mendaftar dan mendapatkan pas keselamatan di kaunter pelanggan sebelum berurusan dan memulangkan semula selepas selesai urusan; (d) Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pihak luar/ketiga dan lain-lain pihak yang berkepentingan tidak berurusan lagi dengan KKM; (e) Kehilangan pas keselamatan mestilah dilaporkan dengan segera kepada pentadbiran KKM dan pihak polis; dan (f) Jurujual/Pegawai Pemasaran tidak dibenarkan sama sekali berniaga atau mempromosi barangan di premis KKM.	Semua Pengguna KKM
	05-01-03 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. (a) Akses kepada kawasan larangan hanyalah kepada pegawai yang dibenarkan sahaja; dan (b) Pihak luar / ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Semua Pengguna KKM
	05-02 Keselamatan Aset ICT	
Objektif :	Melindungi aset ICT daripada kehilangan, kerosakan, kecurian atau salah guna aset dan gangguan ke atas peralatan mahupun aktiviti KKM.	
	05-02-01 Peralatan ICT	
	Peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh berfungsi apabila diperlukan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah menyemak dan memastikan	Semua Pengguna KKM

	semua peralatan ICT di bawah kawalannya berfungsi dengan baik; (b) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switch, hub, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; (c) Setiap pengguna adalah tanggungjawab di atas kerosakan dan kehilangan peralatan ICT di bawah kawalannya; (d) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran peralatan dan konfigurasi yang telah ditetapkan; (e) Pengguna dilarang sama sekali menambah, menanggal, mengganti dan mengubah sebarang peralatan ICT tanpa kebenaran; (f) Pengguna dilarang menghapus atau memadam perisian sedia ada yang telah dibekalkan dan membuat sebarang instalasi perisian tambahan yang tidak tulen tanpa kebenaran; (g) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan; (h) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (i) Semua peralatan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (j) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); (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 KKM, perlulah mendapat kelulusan dan direkodkan bagi tujuan pemantauan; (m) Peralatan ICT yang hilang hendaklah dilaporkan kepada pihak polis, Ketua Jabatan, ICTSO agensi masing-masing dan Pegawai Aset dengan segera; (n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;	

	(o) Sebarang kerosakan peralatan ICT hendaklah dilaporkan untuk di baik pulih; (p) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (q) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir *(administrator password)* yang telah ditetapkan; (r) Pengguna bertanggungjawab terhadap peralatan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (s) Pengguna hendaklah memastikan semua peralatan komputer, pencetak dan pengimbas dalam keadaan *"OFF/LOCKED"* apabila meninggalkan pejabat; (t) Memastikan *plug* komputer, pencetak dan pengimbas dicabut daripada suis utama *(main switch)* bagi mengelakkan kerosakan peralatan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya. (u) Sebarang bentuk penyelewengan atau salah guna peralatan hendaklah dilaporkan.	
	05-02-02 Media Storan	
	Keselamatan media storan perlu diberi perhatian khusus kerana ia berupaya menyimpan maklumat rasmi dan rahsia rasmi Kerajaan. Langkah-langkah pencegahan hendaklah diambil untuk memastikan kerahsiaan, integriti dan bolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyediakan ruang penyimpanan dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; (b) Menghadkan akses untuk memasuki kawasan penyimpanan media pengguna yang dibenarkan sahaja; (c) Proses pelupusan hendaklah merujuk kepada tatacara pelupusan; dan mendapatkan kelulusan daripada pemilik maklumat terlebih dahulu sebelum maklumat atau kandungan media dihapuskan; dan (d) Merekodkan sistem pengurusan media termasuk inventori, pergerakan, melabel dan penduaan *(backup)*.	Semua Pengguna KKM

	05-02-03 Media Tandatangan Digital	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi 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 agensi masing-masing untuk tindakan seterusnya.	Semua Pengguna KKM
	05-02-04 Media Perisian dan Aplikasi	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang tulen sahaja dibenarkan bagi kegunaan KKM; (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi kecuali dengan kebenaran; (c) Lesen perisian (*registration code, serials, CD-keys)* perlu disimpan secara berasingan daripada CD 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.	Semua Pengguna KKM
	05-02-05 Penyelenggaraan Peralatan ICT	
	Peralatan hendaklah diselenggara dengan betul bagi memastikan sediaan, kerahsiaan dan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua peralatan yang diselenggarakan; (b) Memastikan peralatan hanya di selenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan; (d) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; (e) Bertanggungjawab terhadap setiap peralatan bagi	Penyelaras ICT Fasiliti KKM

	penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (f) Semua penyelenggaraan mestilah mendapat kebenaran; (g) Melaksanakan pelupusan bagi peralatan yang telah dikenal pasti sebagai tidak ekonomik untuk dibaiki *(Beyond Economic Repair (BER))*. Manakala bagi peralatan yang telah diganti hendaklah direkodkan; (h) Penyelenggaraan oleh pihak ketiga hendaklah diiringi oleh kakitangan KKM sehingga kerja penyelenggaraan selesai; dan (i) Penyelenggaraan server atau sistem secara jarak jauh *(remote access)* hanya dibenarkan di dalam rangkaian KKM sahaja.	
	05-02-06 Peminjaman Peralatan Untuk Kegunaan Di Luar Pejabat	
	Peralatan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh KKM bagi membawa keluar peralatan, perisian atau maklumat tertakluk kepada tujuan yang dibenarkan; (b) Melindungi dan mengawal peralatan sepanjang masa; (c) Memastikan aktiviti peminjaman dan pemulangan peralatan ICT direkodkan; dan (d) Menyemak peralatan yang dipulangkan berada dalam keadaan baik dan lengkap.	Ketua Bahagian/ Jabatan/ Unit dan Pegawai Aset
	05-02-07 Pengendalian Peralatan Luar Yang Dibawa Masuk	
	Bagi peralatan yang dibawa masuk ke premis kerajaan, perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan peralatan yang di bawa masuk tidak mengancam keselamatan ICT KKM; (b) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh KKM bagi membawa masuk/keluar peralatan; dan (c) Memeriksa dan memastikan peralatan ICT yang dibawa keluar tidak mengandungi maklumat Kerajaan. Ia perlu disalin dan dihapuskan.	Penyelaras ICT Fasiliti KKM

	05-02-08 Pelupusan dan Kitar Semula Peralatan	
	Peralatan ICT yang hendak dilupuskan perlu melalui prosedur proses pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KKM: (a) Menghapuskan semua kandungan peralatan khususnya maklumat rahsia rasmi; dan (b) Rujuk Surat Pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk "Garis Panduan Pelupusan Peralatan Komputer" untuk maklumat lanjut.	Semua Pengguna KKM
	05-02-09 *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* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. 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 faksimili dan mesin fotostat.	Semua Pengguna KKM
	05-03 Keselamatan Persekitaran	
Objektif :	Melindungi aset ICT Kerajaan dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
	05-03-01 Kawalan Persekitaran	
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai dan pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan KKM. Perkara yang perlu dipatuhi bagi menjamin keselamatan persekitaran, adalah seperti berikut: (a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; (b) Melengkapi semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat	Semua Pengguna KKM

	pencegah kebakaran dan pintu kecemasan; (c) Memasang peralatan perlindungan di tempat yang bersesuaian, mudah dikenali dan dikendalikan; (d) Menyimpan bahan mudah terbakar di luar kawasan kemudahan penyimpanan aset ICT; (e) Meletakkan semua bahan cecair di tempat yang bersesuaian dan berjauhan dari aset ICT; (f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; (g) Menyemak dan menguji semua peralatan perlindungan. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan (h) Akses kepada saluran riser hendaklah sentiasa dikunci.	
	05-03-02 Bekalan Kuasa	
	Perkara yang perlu dipatuhi bagi menjamin keselamatan bekalan kuasa adalah seperti berikut: (a) Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dan menyalurkan bekalan yang sesuai kepada peralatan ICT; (b) Menggunakan peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana kuasa *(generator)* bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan (c) Menyemak dan menguji semua peralatan sokongan bekalan kuasa secara berjadual.	Ketua Bahagian/ Jabatan / Unit
	05-03-03 Keselamatan Kabel	
	Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat. Kabel tersebut hendaklah dilindungi kerana boleh menjadi punca maklumat terdedah. Perkara yang perlu dipatuhi 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 bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan	Semua Pengguna KKM

	(d) Membuat penamaan label yang jelas pada kabel dengan menggunakan kod tertentu dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	
	05-03-04 Prosedur Kecemasan	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan; (b) Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada Pegawai Keselamatan KKM dan Ketua Jabatan; (c) Mengadakan, menguji dan mengemas kini pelan kecemasan dari semasa ke semasa; dan (d) Merancang dan mengadakan latihan kebakaran bangunan *(fire drill)* secara berkala.	Semua Pengguna KKM
	05-04 Keselamatan Dokumen	
	Langkah-langkah pengurusan dokumentasi yang baik dan selamat perlu dilaksanakan bagi memastikan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; (b) Menggunakan tanda atau label keselamatan mengikut klasifikasi seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; (c) Mewujudkan sistem pengurusan dokumen terperingkat bagi menerima, memproses, menyimpan dan menghantar dokumen terperingkat supaya ianya diuruskan berasingan daripada dokumen-dokumen tidak terperingkat; (d) Merekod pergerakan fail dan dokumen bagi memastikan ia mengikut prosedur keselamatan yang telah ditetapkan; (e) Melaporkan kehilangan dan kerosakan ke atas semua jenis dokumen mengikut prosedur Arahan Keselamatan; (f) Melupuskan dokumen mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan Tatacara Jabatan Arkib Negara; dan	Semua Pengguna KKM

	(g) Menggunakan enkripsi *(encryption)* ke atas dokumen terperingkat yang disediakan dan dihantar secara elektronik.	

PERKARA 06

PENGURUSAN OPERASI DAN KOMUNIKASI

	06-01 Pengurusan Prosedur Operasi	
Objektif:	Memastikan pengurusan operasi sistem dan komunikasi dapat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
	06-01-01 Pengendalian Prosedur	**T/jawab**
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur operasi keselamatan ICT hendaklah dikenal pasti, didokumenkan dengan jelas lagi teratur, di kemaskini dan boleh diguna pakai oleh pengguna mengikut keperluan; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; (c) Setiap perubahan kepada sistem dan kemudahan pemprosesan maklumat mestilah dikawal; (d) Tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset KKM; dan (e) Kemudahan ICT untuk pembangunan, pengujian dan operasi mestilah diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah kepada sistem yang sedang beroperasi.	ICTSO dan Penyelaras ICT Fasiliti KKM
	06-01-02 Kawalan Perubahan	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan peralatan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua Pengguna KKM

	06-01-03 Pengasingan Tugas dan Tanggungjawab	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan (c) Peralatan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari peralatan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Penyelaras ICT Fasiliti KKM
	06-02 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.	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dilaksanakan dan diselenggarakan oleh pihak ketiga; (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari masa ke semasa; dan (c) Pengurusan kepada perubahan penyediaan perkhidmatan termasuk menyelenggarakan dan menambahbaikkan polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Pentadbir Sistem ICT
	06-03 Perancangan dan Penerimaan Sistem	
Objektif:	Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
	06-03-01 Perancangan Kapasiti	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; (b) Penggunaan peralatan mestilah dipantau, ditala *(tuned)* dan perancangan perlu dibuat bagi memenuhi keperluan kapasiti	Pentadbir Sistem ICT / Penyelaras ICT Fasiliti KKM

	akan datang untuk memastikan prestasi sistem di tahap optima; (c) Kriteria penerimaan untuk sistem maklumat baru, peningkatan dan versi baru perlu ditetapkan dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem; dan (d) 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.	
	06-03-02 Penerimaan Sistem	
	Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT
	06-04 Perlindungan dari Perisian Berbahaya	
Objektif:	Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *worm,* trojan dan lain-lain.	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS), dan mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang berdaftar, berlesen atau telen sahaja; (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum membuat instalasi; (d) Mengemas kini paten 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 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;	Semua Pengguna KKM

	(i) Membuat aduan mengenai ancaman keselamatan ICT kepada CERT KKM; (j) Kawalan pencegahan, pengesanan dan pemulihan untuk melindungi daripada *malicious code* dan program kesedaran pengguna yang bersesuaian mesti dilaksanakan; dan (k) Dalam keadaan *mobile code* dibenarkan, konfigurasinya hendaklah memastikan bahawa ianya beroperasi berdasarkan kepada dasar keselamatan yang jelas dan mobile code yang tidak dibenarkan perlu dielak dari digunakan.	
	06-05 *Housekeeping*	
Objektif:	Mengekalkan integriti, kebolehsediaan maklumat dan kemudahan pemprosesan maklumat.	
	06-05-01 Salinan Penduaan *(Backup)*	
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan hendaklah dilakukan setiap kali konfigurasi berubah. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Membuat *backup* ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali setahun atau setelah mendapat versi terbaru; (b) Membuat salinan penduaan ke atas semua data dan maklumat mengikut kesesuaian operasi dan kekerapan penduaan bergantung pada tahap kritikal maklumat; (c) Menguji *backup* sedia ada sekurang-kurangnya sekali setahun bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (d) Salinan maklumat dan perisian perlu dibuat dan diuji secara berkala berdasarkan kepada prosedur penduaan; dan (e) Salinan penduaan hendaklah direkodkan dan di simpan di lokasi yang berlainan *(off site)*.	Pentadbir Sistem ICT dan Semua Pengguna KKM
	06-06 Pengurusan Keselamatan Rangkaian	
Objektif:	Memastikan perlindungan keselamatan maklumat dalam rangkaian dan infrastruktur sokongan terurus dan terkawal.	
	06-06-01 Kawalan Infrastruktur Rangkaian	
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi	Pentadbir Rangkaian

	melindungi maklumat yang berhubung kait dengan sistem rangkaian; (b) Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenal pasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar; (c) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (d) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; (e) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (f) *Firewall* hendaklah dipasang sebagai perimeter *defence* kepada aset ICT kerajaan serta dikonfigurasi oleh pentadbir sistem yang dibenarkan sahaja; (g) Semua trafik keluar dan masuk hendaklah melalui *Firewall* di bawah kawalan KKM; (h) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran Pentadbir Rangkaian; (i) Memasang perisian *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat jabatan; (j) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (k) Sebarang penyambungan rangkaian yang bukan di bawah kawalan KKM hendaklah mendapat kebenaran BPM, KKM; (l) Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum; (m) Penggunaan rangkaian Streamyx hendaklah mematuhi surat KKM dengan rujukan KKM/BTMK/190/4/4 (9) bertajuk “Penggunaan Talian Streamyx di Kementerian Kesihatan Malaysia”; dan (n) Penggunaan tanpa wayar LAN di KKM hendaklah mematuhi	

	surat MAMPU dengan rujukan UPTM (S) 159/338/8 Jilid 30 (84) bertajuk "Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar *(Wireless Local Area Network)* di Agensi-agensi Kerajaan".	
	06-07 Pengendalian Media	
Objektif:	Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal seperti pendedahan, pengubahsuaian, peralihan atau pemusnahan aset secara tidak sah.	
	06-07-01 Penghantaran atau Pemindahan	
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu. Media yang mengandungi maklumat Kerajaan perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KKM. Prosedur perlu disediakan untuk pengurusan media mudah alih.	Semua Pengguna KKM
	06-07-02 Prosedur Pengendalian Media	
	Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (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 terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Semua Pengguna KKM
	06-07-03 Penghapusan Media	
	Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat. <u>Nota 2 :</u> Surat Pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk "Garis panduan Pelupusan Peralatan Komputer" boleh dirujuk.	Semua Pengguna KKM
	06-07-04 Keselamatan Sistem Dokumentasi	
	Dokumentasi sistem perlu dilindungi dari capaian yang tidak	Semua Pengguna

	dibenarkan. Perkara yang perlu dipatuhi adalah seperti berikut: (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.	KKM
	06-08 Pengurusan Pertukaran Maklumat	
Objektif :	Memastikan keselamatan pertukaran maklumat dan perisian antara KKM dan agensi luar terjamin.	
	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 atau persetujuan perlu diwujudkan untuk pertukaran maklumat dan perisian di antara KKM dengan agensi luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KKM; dan (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua Pengguna KKM
	06-09 Pengurusan Mel Elektronik (E-mel)	
	Maklumat yang terdapat dalam mel elektronik KKM perlu dilindungi sebaik-baiknya bagi menghindari capaian atau sebaran maklumat yang tidak dibenarkan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh KKM sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; (b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh KKM; (c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;	Semua Pengguna KKM

	(d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; (e) Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi 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) 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; (k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; (l) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan (m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.	
	06-10 Keselamatan Komunikasi Rangkaian	
Objektif:	Memastikan keselamatan pertukaran maklumat dan perisian dalam KKM dan mana-mana entiti luar terjamin.	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; dan (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara KKM dan pihak luar.	Semua Pengguna KKM

	06-10-01 Internet	
	Capaian Internet perlu dikawal dan diurus bagi mengelakkan gangguan sistem rangkaian KKM. Perkara yang perlu dipatuhi adalah seperti berikut: (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 berlesen dan tulen; (e) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh KKM; (f) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimana pun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertakluk kepada arahan dan peraturan yang telah ditetapkan; dan (g) Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Tatacara Peggunaan Dan Keselamatan ICT KKM semasa.	Semua Pengguna KKM
	06-11 Perkhidmatan E-Dagang *(Electronic Commerce Services)*	
Objektif:	Memastikan keselamatan dan sensitiviti aplikasi serta maklumat di dalam perkhidmatan e-dagang dan penggunaannya.	
	06-11-01 E-Dagang	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dengan transaksi dalam talian *(online)* perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan (c) Integriti maklumat yang disediakan dalam sistem untuk kegunaan awam perlu dilindungi untuk mengelakkan	Semua Pengguna KKM

	daripada pengubahsuaian yang tidak dibenarkan.	
	06-11-02 Maklumat Umum	
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (a) Memastikan perisian, data dan maklumat dilindungi dengan kaedah yang bersesuaian; (b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua Pengguna KKM
	06-12 Pemantauan	
Objektif:	Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Log Audit yang merekodkan semua aktiviti perlu diaktifkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala; (c) Kemudahan merekodkan dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; (e) Kesalahan yang dilakukan perlu di log (rekod), di analisa dan di ambil tindakan sewajarnya; dan (f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam KKM atau domain keselamatan perlu diselaraskan dengan satu sumber tepat yang dipersetujui.	Pentadbir Sistem ICT
	06-12-01 Pengauditan dan Forensik ICT	
	ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT KKM; (b) Serangan kod perosak *(malicious code),* halangan pemberian perkhidmatan (*denial of service)*, *spam*, pemalsuan *(forgery phising)*, pencerobohan *(intrusion)*, ancaman *(threats)* dan kehilangan fizikal *(physical loss)*; (c) Pengubahsuaian ciri-ciri peralatan, perisian atau mana-mana	ICTSO

	komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan *bandwidth* rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; dan (h) Aktiviti penukaran alamat IP *(IP address)* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	
	06-12-02 Jejak Audit *(Audit Trail)*	
	Setiap sistem mestilah mempunyai jejak audit. Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan; dan (e) Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem ICT
	06-12-03 Sistem Log	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti	Pentadbir Sistem ICT

	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.	
	06-12-04 Pemantauan Log	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; (c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; (e) Log kesalahan dan penyalahgunaan perlu direkodkan, dianalisis dan diambil tindakan sewajarnya; dan (f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KKM atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui	Pentadbir Sistem ICT

PERKARA 07

KAWALAN CAPAIAN

Kawalan Capaian		
	07-01 Dasar Kawalan Capaian	**T/jawab**
Objektif:	Mengawal capaian ke atas maklumat, kemudahan proses maklumat dan proses urus niaga berdasarkan keperluan urus niaga dan keperluan keselamatan. Peraturan kawalan capaian hendaklah mengambil kira faktor *identification, authentication* dan *authorization.*	
	07-01-01 Keperluan Kawalan Capaian	
	Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan KKM. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawalan capaian ke atas aset ICT hendaklah dilaksanakan secara berkesan mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Kawalan capaian ke atas kemudahan pemprosesan maklumat ; dan (d) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih.	Penyelaras ICT Fasiliti KKM
	07-02 Pengurusan Capaian Pengguna	
Objektif:	Mengawal capaian pengguna ke atas aset ICT KKM dengan memastikan aset ICT dicapai oleh pengguna yang sah dan menghalang capaian yang tidak sah.	
	07-02-01 Tanggungjawab Pengguna	
Objektif:	Setiap pengguna bertanggungjawab ke atas aset ICT yang digunakan.	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan; (b) Memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; dan (c) Mematuhi amalan *clear desk/clear screen policy*.	Semua Pengguna KKM

	07-02-02 Akaun Pengguna	
	Prosedur pendaftaran dan pembatalan kebenaran capaian pengguna perlu diwujudkan dan didokumenkan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Akaun yang diperuntukkan oleh KKM sahaja boleh digunakan. (b) Akaun pengguna mestilah unik dan mencerminkan identiti pengguna. (c) Akaun pengguna yang diwujudkan diberi tahap capaian mengikut peranan dan tanggungjawab pengguna. (d) Tahap capaian akaun pengguna termasuk sebarang perubahan mestilah mendapat kebenaran Ketua Jabatan / Pemilik Sistem secara bertulis dan direkodkan; (e) Pemilikan akaun dan capaian pengguna adalah tertakluk kepada peraturan jabatan dan tindakan pembatalan/pengubahsuaian hendaklah di ambil atas sebab seperti berikut: i. pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh Ketua Jabatan; ii. pengguna bercuti atau bertugas di luar pejabat melebihi satu tempoh yang ditentukan oleh Ketua Jabatan; iii. pengguna bertukar jawatan, tanggungjawab dan/ atau bidang tugas; iv. pengguna bertukar atau berpindah agensi; v. pengguna bersara atau tamat perkhidmatan; dan vi. pengguna yang dikenakan tindakan tatatertib. (f) Aktiviti capaian oleh pengguna hendaklah direkod, di selenggara dengan sistematik dan dipantau.	
	07-02-03 Hak Capaian	
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
	07-02-04 Pengurusan Kata Laluan	
	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah	Semua Pengguna KKM dan Pentadbir

	mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KKM 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; (c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; (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) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; (j) Kata laluan hendaklah ditukar dalam tempoh 90 hari atau selepas tempoh masa yang bersesuaian; dan (k) Mengelakkan penggunaan semula sekurang-kurangnya empat (4) kata laluan yang terdahulu sebagai kata laluan baru.	Sistem ICT
	07-03 Kawalan Capaian Rangkaian	
Objektif:	Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
	07-03-01 Capaian Rangkaian	
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian KKM, rangkaian agensi lain dan rangkaian awam ;	Pentadbir Rangkaian ICT

	(b) Mewujudkan dan menguatkuasakan kaedah untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan pengguna boleh mencapai perkhidmatan yang dibenarkan sahaja; (b) Mewujudkan kaedah pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh; (c) Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; (d) Mengasingkan capaian mengikut kumpulan perkhidmatan maklumat, pengguna dan sistem maklumat dalam rangkaian; (e) Mengawal sambungan ke rangkaian, khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan KKM; dan (f) Mewujud dan melaksana kawalan pengalihan laluan *(routing control)* untuk memastikan pematuhan ke atas peraturan KKM.	
	07-03-02 Capaian Internet	
	Perkara-perkara yang perlu dipatuhi oleh Pentadbir Rangkaian adalah seperti berikut: (a) Penggunaan Internet di KKM hendaklah dipantau secara berterusan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code, virus* dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian KKM; (b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (c) Penggunaan teknologi *(packet shaper)* untuk mengawal aktiviti *(video conferencing, video streaming, chat, downloading)* adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan; Perkara-perkara yang perlu dipatuhi oleh Pengguna adalah seperti berikut:	Pentadbir Rangkaian / Semua Pengguna KKM

	(a) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; (b) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Setiausaha KKM / pegawai yang diberi kuasa; (c) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; (d) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet; (e) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; (f) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh KKM; (g) Hanya pegawai yang mendapat kebenaran sahaja boleh mengendalikan akaun media sosial rasmi fasiliti. Kandungan perbincangan hendaklah mendapat kelulusan Ketua Jabatan terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; (h) Penyambungan capaian ke Internet tanpa kebenaran tidak dibenarkan sama sekali; dan (i) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; ii. Memuat naik, memuat turun dan menyimpan maklumat rasmi di luar KKM seperti di syarikat pembekal mahupun laman storan atas talian; dan iii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah dan/atau fitnah.	

PERKARA 07

KAWALAN CAPAIAN

	07-04 Kawalan Capaian Sistem Pengoperasian	
Objektif:	Memastikan bahawa capaian ke atas sistem operasi dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja.	
	07-04-01 Capaian Sistem Pengoperasian	
	Kaedah yang digunakan hendaklah mampu menyokong perkara berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan KKM; (b) Mewujudkan jejak audit *(audit trail)* ke atas semua capaian sistem operasi terutama pengguna bertaraf khas *(super user)*; (c) Menjana amaran *(alert)* sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; (d) Menyedia kaedah sesuai untuk pengesahan capaian *(authentication)*; dan (e) Menghadkan tempoh penggunaan mengikut kesesuaian. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem operasi menggunakan prosedur pengurusan kawalan capaian server yang selamat; (b) Prosedur pengurusan kawalan capaian server yang selamat perlulah: i. Menggunakan kaedah pengenalan pengguna yang unik dan teknik pengesahan pengguna yang berkesan dan selamat; ii. Melaksana sistem pengurusan kata laluan yang interaktif dan menjamin kualiti serta keselamatan kata laluan; iii. Mengawal penggunaan utiliti yang berkeupayaan melepasi sistem dan aplikasi terhad; iv. Menamatkan sesi yang tidak aktif selepas tempoh masa yang ditetapkan; dan v. Hadkan tempoh masa penggunaan bagi meningkatkan keselamatan aplikasi yang berisiko tinggi.	Pentadbir Sistem ICT

	07-04-02 Kad Pintar	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; (b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan (d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pihak yang berkenaan.	Semua Pengguna KKM
	07-05 Kawalan Capaian Aplikasi dan Maklumat	
Objektif:	Menghalang capaian tidak sah ke atas sistem aplikasi dan maklumat.	
	Kawalan capaian adalah seperti berikut: (a) Membenarkan pengguna mencapai aplikasi dan maklumat mengikut tahap capaian yang ditentukan; (b) Menyediakan kaedah perlindungan bagi menghalang capaian tidak sah ke atas aplikasi dan maklumat daripada utiliti yang sedia ada dalam sistem operasi dan perisian malicious yang berupaya melangkaui kawalan sistem; dan (c) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; Perkara yang perlu dipatuhi adalah seperti berikut: (a) Capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna perlu dihadkan berdasarkan prinsip “Perlu Tahu Sahaja (Need To Know Basis)”, selaras dengan fungsi kerja dan peraturan KKM; (b) Semua pembangunan aplikasi perlu disediakan dengan dokumen Peranan/Fungsi Matrik yang telah diluluskan. Dokumen ini perlu bagi menggariskan dan menunjukkan kawalan akses pengguna; (c) Semakan Dokumen Peranan/Fungsi Matrik bagi sesebuah aplikasi perlu dilakukan secara berkala iaitu sekurang-kurangnya sekali setahun; (d) Setiap aplikasi perlu direka dengan fungsi menguatkuasakan tamat masa sesi yang terbiar (*idle* timeout), iaitu apabila tiada	Pentadbir Sistem ICT

	aktiviti pengguna untuk tempoh masa yang tertentu, sesi akan ditamatkan. Pengguna perlu log masuk semula selepas penamatan *idle timeout* tersebut. Saranan bagi tempoh tamat masa adalah 15 minit; (e) Kaedah penamatan atau pembatalan akses perlu diluluskan sekurang-kurangnya oleh dua (2) peringkat iaitu Pengarah / Penyelia / Pentadbir Sistem; dan (f) Sistem yang sensitif perlu persekitaran pengkomputeran yang khusus dan terasing.	
	07-06 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif:	Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mewujudkan peraturan dan garis panduan keselamatan yang bersesuaian untuk melindungi dari risiko penggunaan peralatan mudah alih dan kemudahan komunikasi; dan (b) Mewujudkan peraturan dan garis panduan untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat.	Pentadbir Sistem ICT
	07-06-01 Peralatan Mudah Alih	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua Pengguna KKM
	07-06-02 Kerja Jarak Jauh	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, data, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua Pengguna KKM

PERKARA 08

PEROLEHAN, PEMBANGUNAN, PENAMBAHBAIKAN DAN PENYELENGGARAAN SISTEM MAKLUMAT

	08-01 Keselamatan Dalam Membangunkan, Menambahbaik dan Menyelenggara Sistem Aplikasi	
Objektif :	Memastikan sistem aplikasi yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang telah dikenalpasti.	
	Ketua Setiausaha KKM bertanggungjawab: (a) Memastikan kaedah keselamatan yang bersesuaian dikenal pasti, dirancang dan dilaksanakan pada setiap peringkat perolehan, pembangunan dan penyelenggaraan sistem aplikasi; (b) Melindungi kerahsiaan, integriti dan kesahihan maklumat menggunakan kaedah tertentu; dan (c) Menjaga dan menjamin keselamatan sistem aplikasi.	
	08-01-01 Keperluan Keselamatan Sistem Aplikasi	**T/jawab**
Objektif:	Memastikan keperluan keselamatan sistem aplikasi dikenal pasti, dipersetujui dan didokumenkan pada setiap peringkat perolehan, pembangunan, penambahbaikan dan penyelenggaraan. Pernyataan keperluan bagi sistem aplikasi hendaklah menjelaskan mengenai kawalan jaminan 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; (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; (e) Memastikan kawalan capaian yang telah ditetapkan oleh	Pemilik Sistem dan Pentadbir Sistem ICT

	KKM dipatuhi; dan (f) Memastikan pembangunan sistem menggunakan teknik *secure coding*.	
	08-01-02 Ketepatan Maklumat	
Objektif:	Memastikan kawalan keselamatan yang sesuai dilaksanakan bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Data hendaklah disemak dan disahkan sebelum dimasukkan ke dalam aplikasi bagi menjamin ketepatan dan kesesuaian; (b) Semakan pengesahan hendaklah digabung di dalam aplikasi untuk mengenal pasti sebarang kesilapan maklumat sama disengajakan atau tidak; (c) Kawalan yang sesuai hendaklah dikenal pasti dan di laksana bagi pengesahan dan melindungi integriti mesej dalam aplikasi; dan (d) Proses semak hendaklah dijalankan ke atas hasil data daripada setiap proses aplikasi untuk menjamin ketepatan dan kesesuaian.	Semua Pengguna KKM
	08-01-03 Pengesahan Data Input dan Output	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (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.	Pemilik Sistem dan Pentadbir Sistem
	08-02 Kawalan Kriptografi	
Objektif:	Memastikan kaedah kriptografi diguna untuk melindungi kerahsiaan, kesahihan dan integriti maklumat.	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peraturan untuk melindungi maklumat tertentu menggunakan kaedah kriptografi yang sesuai hendaklah dibangunkan dan dilaksanakan; dan (b) Memastikan kaedah yang selamat dan berkesan untuk pengurusan kata laluan yang menyokong teknik kriptografi diguna pakai oleh KKM.	Pentadbir Sistem ICT

	08-02-01 Enkripsi	
	Pengguna hendaklah membuat enkripsi *(encryption)* ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa. Mengenalpasti maklumat sensitif atau maklumat rahsia rasmi yang perlu di enkripsi (encryption). Membangunkan fungsi enkripsi bagi maklumat yang dikenalpasti.	Semua Pengguna KKM Pemilik Sistem Pemilik Sistem
	08-02-02 Tandatangan Digital	
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua Pengguna KKM
	08-02-03 Pengurusan Infrastruktur Kunci Awam (PKI)	
	Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua Pengguna KKM
	08-03 Keselamatan Fail Sistem	
Objektif:	Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; (c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan (e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan	Pemilik Sistem dan Pentadbir Sistem
	08-04 Keselamatan Dalam Proses Pembangunan, Penambahbaikan Dan Penyelenggaraan	
Objektif:	Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
	08-04-01 Prosedur Kawalan Perubahan	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peraturan formal untuk mengawal pelaksanaan perubahan; (b) Semakan teknikal selepas perubahan sistem operasi dibuat	Pemilik Sistem dan Pentadbir Sistem ICT

	bagi menjamin tiada impak negatif ke atas keselamatan operasi KKM. (c) Pembangunan dan penambahbaikan ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (d) Pembangunan atau penambahbaikan sistem aplikasi perlu dipantau; (e) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (f) Akses kepada kod sumber *(source code)* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan (g) Menghalang sebarang peluang untuk membocorkan maklumat.	
	08-04-02 Pembangunan Sistem Aplikasi Secara *Outsource*	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pembangunan sistem aplikasi oleh pihak luar di kawal selia dan dipantau oleh KKM dari semasa ke semasa ; (b) Kod sumber *(source code)* bagi semua aplikasi adalah menjadi hak milik KKM; (c) Pembangunan sistem aplikasi disarankan dilaksanakan di dalam premis KKM; dan (d) Memastikan pembangunan sistem menggunakan teknik *secure coding*.	Pentadbir Sistem ICT
	08-05. Kawalan Teknikal Keterdedahan *(Vulnerability)*	
Objektif:	Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
	Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko	Pentadbir Sistem ICT

	berkaitan.	
	08-06 Kawalan Perisian Operasi	
Objektif:	Memastikan kaedah yang sesuai dilaksanakan untuk mengawal capaian ke atas fail sistem dan kod sumber program bagi menjamin keselamatan sistem fail.	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peraturan untuk mengawal pemasangan perisian ke dalam persekitaran operasi diwujudkan; (b) Peraturan diwujudkan untuk pemilihan, perlindungan dan kawalan data ujian; dan (c) Capaian ke atas kod sumber program dikawal dan terhad kepada pengguna yang dibenarkan sahaja.	Pentadbir Sistem ICT

PERKARA 09

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

Pengurusan Pengendalian Insiden Keselamatan ICT		
Objektif :	Memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.	
	09-01 Kaedah Pelaporan	**T/jawab**
	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 DKICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada Ketua/ICTSO di agensi dan CERT KKM 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 kaedah 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. Carta alir pelaporan insiden keselamatan ICT di KKM seperti **Lampiran 1** selaras dengan Prosedur Pelaporan Insiden BPM.KKM.ISO/ISMS/P2/PK03. Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam; dan (c) Prosedur Pelaporan Insiden BPM.KKM.ISO/ISMS/P2/PK03.	Semua Pengguna KKM

PERKARA 09

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

	09-02 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif:	Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
	09-02-01 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 mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KKM. 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) Mewujud dan mendokumenkan prosedur pengurusn insiden; (b) Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; (c) Menyimpan jejak audit, penduaan secara berkala dan melindungi integriti semua bahan bukti; (d) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (e) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; (f) Menyediakan pelan tindakan pemulihan segera; dan (g) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO

PERKARA 10

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

Dasar Kesinambungan Perkhidmatan		
Objektif :	Menjamin operasi perkhidmatan agar tidak tergendala dan memastikan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
	10-01 Pengurusan Kesinambungan Perkhidmatan	**T/jawab**
	Pengurusan Kesinambungan Perkhidmatan *(Business Continuity Management, BCM)* hendaklah dibangunkan untuk memastikan pendekatan yang menyeluruh dilaksanakan bagi mengatasi gangguan ke atas aktiviti penyediaan perkhidmatan KKM dan melindungi aktiviti daripada kesan bencana serta pemulihan perkhidmatan dalam tempoh yang ditetapkan. Pelan ini mestilah diluluskan oleh JPICT KKM. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Keperluan keselamatan maklumat dibangunkan untuk mengurus dan selenggara proses formal untuk mengawal pelaksanaan perubahan; (c) Peraturan untuk menangani gangguan ke atas penyediaan perkhidmatan dengan mengenal pasti keadaan tersebut, kebarangkalian berlaku dan kesan sekiranya berlaku; (d) Merancang dan melaksana peraturan kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (e) Hanya satu rangka pelan kesinambungan perkhidmatan yang menyeluruh dibangunkan, di dokumentasikan, dipersetujui oleh pengurusan dan diselenggarakan bagi setiap KKM; (f) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (g) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (h) Membuat penduaan *(backup)*; dan (i) Menguji dan mengemas kini pelan kesinambungan perkhidmatan sekurang-kurangnya setahun sekali bagi memastikan keberkesanannya.	Koordinator PKP

	Pelan BCM yang dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel KKM dan pembekal *(vendor)* berserta nombor yang boleh dihubungi (faksimile, telefon bimbit, telefon pejabat 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 dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. KKM hendaklah memastikan salinan pelan BCM sentiasa dikemaskini dan dilindungi seperti di lokasi utama.	

PERKARA 11

PEMATUHAN

	11-01 Pematuhan dan Keperluan Perundangan	
Objektif :	Meningkatkan tahap keselamatan ICT bagi memastikan DKICT KKM sentiasa dipatuhi.	
	11-01-01 Pematuhan Dasar	**T/jawab**
	Setiap Pengguna di KKM hendaklah membaca, memahami dan mematuhi DKICT KKM, undang-undang atau peraturan-peraturan yang berkuatkuasa. Semua aset ICT di KKM termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Setiausaha KKM/pegawai yang diberi kuasa berhak untuk memantau sebarang penyalahgunaan sumber KKM.	Semua Pengguna KKM
	11-01-02 Pematuhan Keperluan Sistem 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 Pengguna KKM
	11-01-03 Keperluan Perundangan	
	Dasar ini bertujuan memastikan rekabentuk, operasi, penggunaan dan pengurusan sistem maklumat adalah selaras serta berkeupayaan menghalang perlanggaran mana-mana keperluan perundangan, peraturan dan perjanjian yang berkuatkuasa. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perlembagaan, undang-undang, peraturan, perjanjian yang dimeterai dan lain-lain perkara yang relevan kepada keselamatan sistem maklumat dan organisasi hendaklah dikenal pasti, di dokumentasikan dan dikemaskini; (b) Peraturan yang sesuai dilaksanakan untuk pematuhan ke atas perlembagaan, undang-undang dan keperluan perjanjian mengenai penggunaan material yang tertakluk kepada hak milik harta intelek; (c) Rekod penting hendaklah dilindungi daripada hilang, rosak dan dipalsukan selaras dengan keperluan undang-undang, peraturan dan keperluan perjanjian KKM; (d) Perlindungan ke atas data dan maklumat privasi hendaklah mematuhi perundangan, peraturan dan terma perjanjian jika	Semua Pengguna KKM

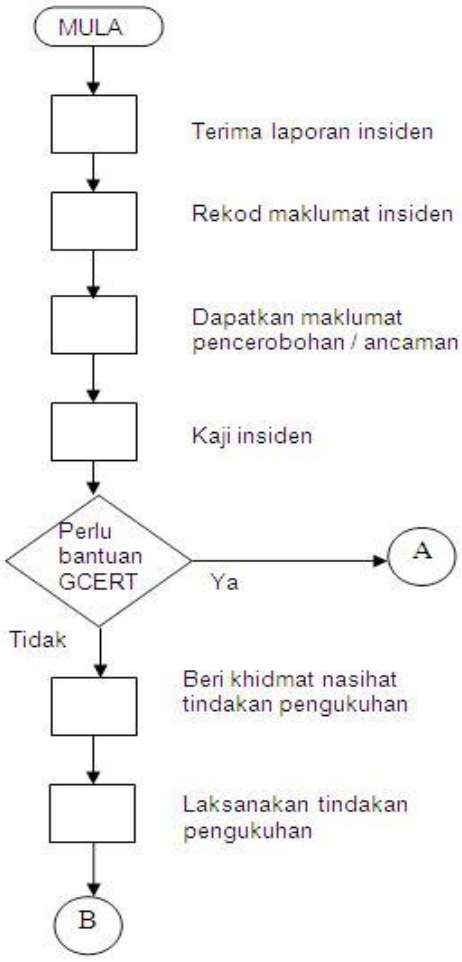
	perlu; dan (e) Penyalahgunaan pemprosesan maklumat adalah tidak dibenarkan. (f) Penggunaan kriptografi dikawal selaras dengan perjanjian, perundangan dan peraturan yang berkuatkuasa.	
	11-01-04 Pematuhan kepada Dasar, Piawaian dan Teknikal Keselamatan	
	Dasar ini bertujuan memastikan keselamatan maklumat disemak secara berkala supaya patuh dan selaras dengan dasar dan piawaian keselamatan KKM. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pegawai penyelia hendaklah memastikan bahawa semua peraturan keselamatan di bawah kawal selia masing-masing dipatuhi selaras dengan perundangan, peraturan dan lain-lain keperluan keselamatan; dan (b) Sistem maklumat hendaklah disemak dan diuji secara berkala untuk pastikan mematuhi pelaksanaan piawaian keselamatan yang ditetapkan. Rujuk **Lampiran 5** bagi senarai perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi.	Semua Pengguna KKM
	11-01-05 Pelanggaran Dasar	
	Pelanggaran DKICT KKM boleh dikenakan tindakan tatatertib.	Ketua Setiausaha KKM

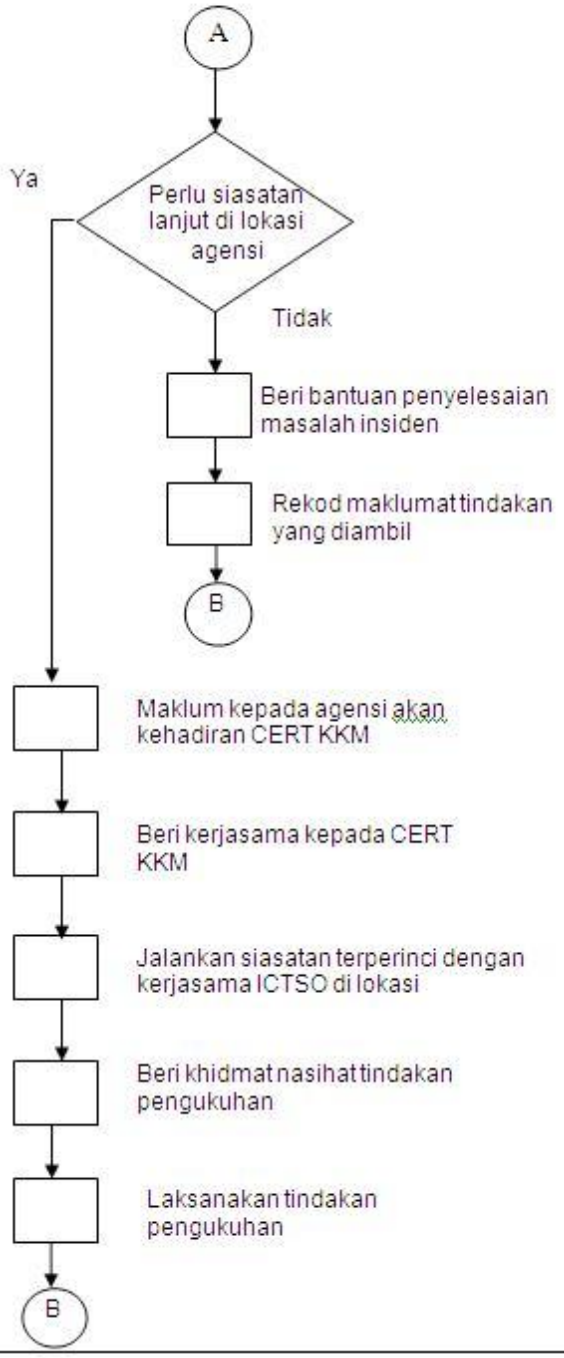
GLOSARI

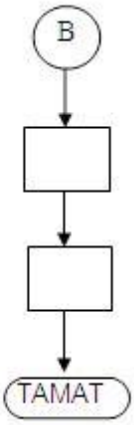
KKM	-	Kementerian Kesihatan Malaysia
BPM	-	Bahagian Pengurusan Maklumat
GCERT	-	Pasukan Pengendalian Insiden Keselamatan ICT MAMPU
CERT KKM	-	Pasukan Pengendalian Insiden Keselamatan ICT KKM
MYCERT	-	Pasukan Pengendalian Insiden Keselamatan ICT Malaysia
CIO	-	Setiausaha Bahagian BPM, KKM
ICTSO	-	Pegawai Keselamatan ICT, KKM - Timbalan Setiausaha Bahagian Cawangan Pemantauan, Keselamatan & Sokongan Teknikal ICT, BPM, KKM
ICTSO Agensi	-	Pegawai Keselamatan ICT yang dilantik di fasiliti KKM
ICT	-	*Information and Communication Technology*
Insiden Keselamatan ICT	-	Bencana (adverse event) yang berlaku ke atas aset ICT atau kemungkinan ancaman berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar DKICT sama ada disengajakan atau tidak disengajakan
ISMS	-	*Information Security Management System*
ISP	-	*Internet Service Provider*
Outsource	-	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui
Pengawai Aset	-	Pegawai yang bertanggungjawab ke atas pengurusan inventori aset ICT di fasiliti KKM
Pentadbir Sistem ICT	-	Pengurus Projek / Pentadbir Rangkaian / Pentadbir Sistem Aplikasi / Pentadbir Pangkalan Data / Pengurus Pusat Data
Penyelaras ICT Fasiliti KKM	-	Penyelaras ICT Bahagian / Jabatan Kesihatan Negeri (JKN) / Hospital / Institut/ Makmal / Kolej / Farmasi / Pejabat Kesihatan Daerah (PKD) / Pejabat Kesihatan Kawasan (PKK) / Pejabat Kesihatan Bahagian (PKB) / Pejabat Pergigian Daerah (PPD) / Institut Pengurusan Kesihatan (IPK) / Klinik Kesihatan (KK) / Klinik Pergigian (KP) / Klinik Kesihatan Ibu Dan Anak (KKIA) /Klinik Desa (KD), Klinik 1 Malaysia (K1M) dan semua fasiliti KKM Pegawai yang dilantik menguruskan hal-hal ICT

Fasiliti KKM	-	Bahagian / Jabatan Kesihatan Negeri (JKN) / Hospital / Institut/ Makmal / Kolej / Farmasi / Pejabat Kesihatan Daerah (PKD) / Pejabat Kesihatan Kawasan (PKK) / Pejabat Kesihatan Bahagian (PKB) / Pejabat Pergigian Daerah (PPD) / Institut Pengurusan Kesihatan (IPK) / Klinik Kesihatan (KK) / Klinik Pergigian (KP) / Klinik Kesihatan Ibu Dan Anak (KKIA) /Klinik Desa (KD), Klinik 1 Malaysia (K1M) dan semua fasiliti KKM
Pihak Luar/Ketiga	-	Kontraktor, pembekal dan lain-lain pihak yang berkepentingan
Public-Key Infrastructure (PKI)	-	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet
Semua Pengguna KKM	-	Pegawai, kakitangan dan kontraktor yang terlibat dengan penggunaan ICT di KKM
Sistem Aplikasi	-	Sistem yang dibangunkan oleh organisasi secara *inhouse* atau *outsource* atau sistem yang dibeli daripada pembekal
WAN	-	Rangkaian Kawasan Luas
LAN	-	Rangkaian Kawasan Setempat.

LAMPIRAN 1 : CARTA ALIR PELAPORAN INSIDEN KESELAMATAN
SUMBER : DOKUMEN P2 ISMS - Prosedur Pelaporan Insiden BPM.KKM.ISO/ISMS/P2/PK03

Tanggungjawab	Tindakan	Dokumen Sokongan
FasilitiKKM / GCERT / PRISMA		Emel
CERT KKM		Fail Insiden
Fasiliti KKM		Fail log
CERT KKM		
CERT KKM		
CERT KKM		
FASILITI KKM		

Tanggungjawab	Tindakan	Dokumen Sokongan
		
CERT KKM	Beri bantuan penyelesaian masalah insiden	
CERT KKM	Rekod maklumat tindakan yang diambil	Emel
CERT KKM	Maklum kepada agensi akan kehadiran CERT KKM	Emel
FASILITI KKM	Beri kerjasama kepada CERT KKM	
CERT KKM	Jalankan siasatan terperinci dengan kerjasama ICTSO di lokasi	
CERT KKM	Beri khidmat nasihat tindakan pengukuhan	
FASILITI KKM / CERT KKM	Laksanakan tindakan pengukuhan	

Tanggungjawab	Tindakan	Dokumen Sokongan
FASILITI KKM		Borang IRH1.0 / Borang IRH1.1
CERT KKM		Borang IRH1.0 / Borang IRH1.1

LAMPIRAN 2 : SURAT AKUAN PEMATUHAN DKICT KKM

DASAR KESELAMATAN ICT KEMENTERIAN KESIHATAN MALAYSIA

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT KEMENTERIAN KESIHATAN MALAYSIA

Nama Penuh (Huruf Besar) : ……

No. Kad Pengenalan : ……

Jawatan : ……

Bahagian : ……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan Keselamatan ICT Kementerian Kesihatan; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : ……..

Tarikh : ……..

Pengesahan Pegawai Keselamatan ICT

……
(Nama Pegawai Keselamatan ICT)
b.p. Ketua Setiausaha
Kementerian Kesihatan Malaysia

Tarikh : ……

LAMPIRAN 3: BORANG TAPISAN KESELAMATAN

SULIT Borang KPKK 11

Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
Jabatan Perdana Menteri

BORANG SOALAN KESELAMATAN
UNIT TAPISAN KESELAMATAN

KETERANGAN DIRI

(Untuk dipenuhkan dalam tiga (3) salinan)

1. Jawatan sekarang/ pekerjaan yang diminta: ……..……...

   di dalam Kementerian / Jabatan:……

2. Nama Penuh (Huruf Besar): …….

3. Nama dalam tulisan Cina (Jika Berkenaan):……...

4. Lain-lain nama : (Perempuan yang sudah kahwin, tulis nama asal)

   Nama dalam tulisan Cina jika berkenaan:……

5. (a) No. Kad Pengenalan Baru / Lama:……

6. Jantina:…….

7. Tarikh Lahir:……

8. Tempat Lahir:……..

9. Kerakyatan Sekarang:…… No. Sijil:……

10. Alamat penuh tempat tinggal sekarang:……

    ……

SULIT Borang KPKK 11

11. Alamat-alamat tempat tinggal dalam masa 10 tahun yang lepas.

Alamat	Dari	Hingga

12. Nama dan alamat bapa: ……

……

13. Nama dan alamat suami/ isteri:……..

……

Tarikh:…….. ……
(Tandatangan)

LAMPIRAN 4: PERAKUAN AKTA RAHSIA RASMI 1972

PERAKUAN UNTUK DITANDATANGANI OLEH KONTRAKTOR BERKENAAN DENGAN AKTA RAHSIA RASMI 1972

Adalah saya dengan ini mengaku bahawa perhatian saya telah dirujuk kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkah laku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya peroleh sebagai perunding dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya sebagai Perunding dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akuan selanjutnya bagi maksud ini apabila meninggalkan perkhidmatan sebagai Perunding Kerajaan.

Tandatangan : .....
Nama :
No.Kad Pengenalan :
Jawatan :
Syarikat :
Tarikh :

Disaksikan oleh : .....
(Tandatangan)
Nama :
No. Kad Pengenalan :
Jawatan : Timbalan Setiausaha Bahagian
Jabatan : Cawangan Pemantauan, Keselamatan & Sokongan Teknikal ICT,Bahagian Pengurusan Maklumat

Tarikh :

Cop Jabatan :

LAMPIRAN 5: SENARAI PERUNDANGAN ATAU PERATURAN-PERATURAN YANG PERLU DIPATUHI

Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di KKM:

(a) Arahan Keselamatan;

(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) Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam";

(f) Akta Tanda Tangan Digital 1997;

(g) Akta Rahsia Rasmi 1972;

(h) Akta Jenayah Komputer 1997;

(i) Akta Hak cipta (Pindaan) Tahun 1997;

(j) Akta Komunikasi dan Multimedia 1998;

(k) Perintah-Perintah Am;

(l) Arahan Perbendaharaan;

(m) Arahan Teknologi Maklumat 2007;

(n) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002;

(o) Pekeliling Am Kementerian Kesihatan Malaysia Bilangan 2 Tahun 2009 bertajuk "Tatacara Penggunaan dan Keselamatan Rangkaian ICT Kementerian Kesihatan Malaysia";

(p) Surat KKM dengan rujukan KKM/BTMK/190/4/4 (9) bertajuk "Penggunaan Talian Streamyx di Kementerian Kesihatan Malaysia";

(q) Surat MAMPU dengan rujukan UPTM (S) 159/338/8 Jilid 30 (84) bertajuk "Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar *(Wireless Local Area Network)* di Agensi-agensi Kerajaan" yang bertarikh 20 Oktober 2006;

(r) Surat Arahan Ketua Pengarah MAMPU yang bertajuk "Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan" yang bertarikh 1 Jun 2007;

(s) Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;

(t) Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasajawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);

(u) Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) yang bertajuk "Tatacara Penyediaan, Penilaian dan Penerimaan Tender";

(v) Surat Pekeliling Perbendaharaan Bil. 3/1995 yang bertajuk "Peraturan Perolehan Perkhidmatan Perundingan";

(w) Garis Panduan Keselamatan MAMPU 2004; dan

(x) *Standard Operating Procedure* (SOP) ICT MAMPU.