PENGENALAN

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

OBJEKTIF

Dasar Keselamatan ICT KADA diwujudkan untuk memastikan tahap keselamatan ICT KADA terurus dan menjamin kesinambungan urusan KADA dengan meminimumkan kesan insiden keselamatan ICT.

SKOP

Dasar ini meliputi semua sumber atau aset ICT yang digunakan seperti :

i) Maklumat (contoh : fail, dokumen, data elektronik);
ii) Perisian (contoh : aplikasi dan sistem perisian); dan
iii) Fizikal (contoh : komputer, peralatan komunikasi dan media magnet).

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

PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT KADA 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 sahaja atas dasar “perlu mengetahui”. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen **Arahan Keselamatan perenggan 53, muka surat 15**;

b) Hak akses minimum

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

c) Akauntabiliti

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

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. 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

Dasar keselamatan ICT KADA hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk pelanggaran ke atasnya yang boleh membawa ancaman kepada keselamatan ICT;

g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehjadian 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 saling bergantung antara satu sama lain. Dengan itu, tindakan mempelbagaikan pendekatan dalam menyusun dan mencorakkan sebanyak mungkin mekanisme keselamatan adalah perlu bagi menjamin keselamatan yang maksimum.

PERKARA 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR

01.1	**Dasar Keselamatan ICT KADA**	
01.1.1	**Perlaksanaan Dasar**	**T/jawab**
	Perlaksanaan dasar ini akan dijalankan oleh Pengurus Besar KADA dan dibantu oleh Jawatankuasa Keselamatan ICT yang terdiri daripada pegawai-pegawai berikut : i) Ketua Pegawai Maklumat (Pengurus Besar KADA); ii) Ketua Bahagian Teknologi Maklumat (Pengarah Bahagian Perancangan dan Penilaian); iii) Pegawai Keselamatan ICT (*ICTSO*) (Pegawai Teknologi Maklumat); iv) Ketua Program Teknologi Maklumat (Pen. Peg. Teknologi Maklumat); v) Pegawai Keselamatan KADA; dan vi) Lain-lain Pengarah Bahagian yang dilantik.	Pengurus Besar
01.1.2	**Penyebaran Dasar**	
	Dasar ini bertujuan memastikan hala tuju pengurusan organisasi untuk melindungi aset ICT selaras dengan keperluan perundangan. Dasar ini perlu disebarkan kepada semua pengguna KADA (termasuk kakitangan, pembekal dan pakar runding yang berurusan dengan KADA)	ICTSO
01.1.3	**Penyelenggaraan Dasar**	
	Dasar keselamatan ICT KADA adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT KADA; a. Kenalpasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan	ICTSO

	Mesyuarat Jawatankuasa Pemandu ICT (JPICT); c. Perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna; dan d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun.	
01.1.4	**Pengecualian Dasar**	
	Dasar Keselamatan ICT KADA adalah terpakai kepada semua pengguna ICT KADA dan tiada pengecualian diberikan.	Semua

PERKARA 02 KESELAMATAN ORGANISASI

02.1	**Infrastruktur Keselamatan Organisasi**	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.		
02.1.1	**Ketua Pegawai Maklumat (CIO)**	**T/jawab**
	Pengurus Besar KADA adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut : a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT KADA; b. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT KADA; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT KADA.	CIO
02.1.2	**Ketua Bahagian Teknologi Maklumat (KBTM)**	
	Pengarah Bahagian Perancangan dan Penilaian KADA adalah merupakan Ketua Bahagian Teknologi Maklumat (KBTM). Peranan dan tanggungjawab beliau adalah seperti berikut :	KBTM

	a. Membantu CIO/Pengurus Besar dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Menentukan keperluan keselamatan ICT; dan c. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.	
02.1.3	**Pegawai Keselamatan ICT (ICTSO)**	
	Pegawai Teknologi Maklumat adalah merupakan Pegawai Keselamatan ICT (ICTSO). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut : a. Mengurus keseluruhan program-program keselamatan ICT KADA; b. Menguatkuasakan Dasar Keselamatan ICT KADA; c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT KADA kepada semua pengguna; d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT KADA; e. Menjalankan pengurusan risiko; f. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. Memberi amaran terhadap kemungkinan berlakunya ancaman bahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h. Melaporkan insiden keselamatan ICT kepada Pasukan Tindakbalas Insiden Keselamatan ICT (CGERT) MAMPU dan memaklumkannya kepada CIO; i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenalpasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;	ICTSO

	j. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT KADA; dan k. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
02.1.4	**Pengurus Teknikal**	
	Juruteknik Komputer adalah merupakan Pengurus Teknikal KADA. Peranan dan tanggungjawab Pengurus Teknikal adalah seperti berikut : a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KADA; b. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan KADA; c. Menentukan kawalan akses semua pengguna terhadap asset ICT KADA; d. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan e. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KADA.	Pengurus Teknikal
02.1.5	**Pentadbir Sistem ICT**	
	Penolong Pegawai Teknologi Maklumat (2) adalah merupakan Pentadbir Sistem ICT KADA. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut : a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek; c. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT KADA;	Pentadbir Sistem ICT

	d. Memantau aktiviti capaian harian pengguna; e. Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; f. Menyimpan dan menganalisis rekod jejak audit; dan g. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	
02.1.6	**Pentadbir Rangkaian**	
	Penolong Pegawai Teknologi Maklumat (1) adalah merupakan Pentadbir Rangkaian. Peranan dan tanggungjawab pentadbir rangkaian adalah seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT KADA; c. Memantau aktiviti capaian rangkaian harian pengguna; d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. Menyimpan dan menganalisis rekod jejak audit; dan f. Menyediakan laporan akses rangkaian secara berkala.	Pentadbir Rangkaian
02.1.7	**Pengguna**	
	Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KADA;	Pengguna

	b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Lulus tapisan keselamatan; d. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat KADA; e. Melaksanakan langkah-langkah perlindungan seperti berikut: 1) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; 2) Memeriksa maklumat dan mementukan ia tepat dan lengkap dari semasa ke semasa; 3) Menentukan maklumat sedia untuk digunakan; 4) Menjaga kerahsiaan kata laluan; 5) Mematuhi standard, prosedur, langkah dan garis panduan yang ditetapkan; memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan 6) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; g. Menghadiri program-program kesedaran mengenai keselamatan ICT;dan h. Menandatangani surat akuan pematuhan Dasar Keselamatan ICT KADA.	
02.1.8 Pihak Ketiga		
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga.		
02.1.8.1 Keperluan Keselamatan Kontrak dengan Pihak Ketiga.		
	Akses kepada aset ICT KADA perlu berlandaskan kepada perjanjian kontrak.	CIO, KBTM, ICTSO,

	Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan. a. Dasar Keselamatan ICT KADA; b. Tapisan Keselamatan; c. Perakuan Akta Rahsia Rasmi 1972; d. Hak Harta Intelek; Nota 1: Surat Pekeliling Perbendaharaan Bilangan 2 Tahun 1995 bertajuk "Tatacara Penyediaan, Penilaian dan Penerimaan Tender" dan Surat Pekeliling Perbendaharaan Bilangan 3 Tahun 1995 bertajuk "Peraturan Perolehan Perkhidmatan Perundingan" yang berkaitan juga boleh dirujuk.	Pengurus Teknikal, Pentadbir Sistem ICT, Pentadbir Rangkaian dan Pihak Ketiga.

PERKARA 03 KAWALAN DAN PENGELASAN ASET

03.1	**Akauntabiliti Aset**	
Objektif:	Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KADA.	
03.1.1	**Inventori Aset**	
	Semua aset ICT KADA hendaklah direkodkan. Ini termasuklah mengenal pasti aset , mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Setiap pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah kawalannya.	Pentadbir Sistem ICT, Pentadbir Rangkaian Semua
03.2	**Pengelasan dan Pengendalian Maklumat**	
Objektif:	Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
03.2.1	**Pengelasan Maklumat**	
	Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut :	Semua

	1. Rahsia Besar; 2. Rahsia; 3. Sulit;atau 4. Terhad	
03.2.2	**Pengendalian Maklumat**	
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut : a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran, dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua

PERKARA 04 KESELAMATAN SUMBER MANUSIA

04.1	**Keselamatan ICT Dalam Tugas Harian**	
Objektif : Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT KADA.		
04.1.1	**Tanggungjawab Keselamatan**	
	Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak.	Semua

	Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.	
04.1.2	**Terma dan Syarat Perkhidmatan**	
	Semua warga KADA yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	Semua
04.1.3	**Perakuan Akta Rahsia Rasmi**	
	Warga KADA yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972.	Semua
04.2	**Menangani Insiden Keselamatan ICT**	
Objektif : Meminimumkan kesan insiden keselamatan ICT.		
04.2.1	**Pelaporan Insiden**	
	Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera : a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang , dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Nota : Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan Insiden Keselamatan ICT” mengenainya bolehlah	Semua

	dirujuk.	
04.3	**Pendidikan**	
Objektif : Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.		
04.3.1	**Program Kesedaran Keselamatan ICT**	
	Setiap pengguna di KADA perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT KADA.	ICTSO
04.4	**Tindakan Tatatertib**	
Objektif : Meningkatkan kesedaran dan pematuhan ke atas Dasar Keselamatan ICT KADA.		
04.4.1	**Pelanggaran Dasar**	
	Pelanggaran Dasar Keselamatan ICT KADA akan dikenakan tindakan tatatertib.	Semua

PERKARA 05 KESELAMATAN FIZIKAL

05.1	**Keselamatan Kawasan**	
Obketif : Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.		
05.1.1	**Perimeter Keselamatan Fizikal**	
	Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut : a. Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi keteguhan keselamatan fizikal hendaklah bergantung kepada keprluan untuk melindungi aset dan hasil penilaian risiko; b. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; c. Memperkukuhkan dinding dan syiling;	CIO dan Pegawai Keselamatan.

	d. Memasang alat penggera atau kamera; e. Menghadkan jalan keluar masuk; f. Mengadakan kaunter kawalan; g. Menyediakan tempat atau bilik khas untuk pelawat-Pelawat; dan h. Mewujudkan perkhidmatan kawalan keselamatan.	
05.1.2	**Kawalan Masuk Fizikal**	
	a. Setiap pengguna KADA hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Setiap pelawat boleh mendapatkan Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; c. Semua pas keselamatan hendaklah diserahkan balik Kepada jabatan apabila pengguna berhenti, bertukar atau bersara; d. Setiap pelawat hendaklah mendaftar di pintu masuk utama di balai pengawal terlebih dahulu; e. Kehilangan pas mestilah dilaporkan dengan segera; f. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT KADA;	Semua dan Pelawat
05.1.3	**Kawasan Larangan**	
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di KADA adalah bilik Pengarah , bilik Timbalan Ketua Pengarah, bilik Pengarah Bahagian, bilik Ketua Jabatan, bilik ICT dan bilik Server di Unit Teknologi Maklumat. Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja: a. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila	Semua

	perlu; b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai;dan c. Semua penggunaan peralatan yang melibatkan penghantaran, kemaskini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	
05.2	**Keselamatan Peralatan**	
Objektif:	Melindungi peralatan dan maklumat.	
05.2.1	**Perkakasan**	
	Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu: a. Setiap pengguna hendaklah menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan baik dan sempurna; b. Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; c. Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;dan d. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO.	Semua
05.2.2	**Dokumen**	
	Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi: a. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b. Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan kepada dokumen;	Semua

	c. Menggunakan penyulitan (encryption) ke atas dokumen rahsia rasmi yang disediakan dan di hantar secara elektronik ; dan d. Memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak.	
05.2.3	**Media Storan**	
	Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat: a. Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat. b. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja. c. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusam pemilik maklumat terlebih dahulu; dan d. Pergerakan media storan hendaklah direkodkan.	Semua
05.2.4	**Kabel**	
	Kabel komputer hendaklah dilindung kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah di tetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya; d. Port; dan e. Hanya kakitangan dari Seksyen Sokongan dan Operasi di Bahagian Teknologi Maklumat	BTM dan ICTSO

	dibenarkan membuat sebarang pindaan atau penyenggaraan.	
05.2.5	**Penyelenggaraan**	
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti: a. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan. b. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja. c. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan d. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengarah Bahagian berkenaan.	Semua
05.2.6	**Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat**	
	Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan : a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan dan mengikut prosedur yang ditetapkan oleh BTM.	Semua
05.2.7	**Peralatan Di Luar Premis**	
	Bagi perkakasan yang dibawa keluar dari premis KADA, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawasan KADA: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang	Semua

	bersesuaian.	
05.2.8	**Pelupusan**	
	Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KADA: a. Semua kandungan peralatan ICT khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding degauzing* atau pembakaran. b. Sekiranya maklumat perlu di simpan, maka pengguna bolehlah membuat panduan; dan c. Maklumat lanjut pelupusan bolehlah merujuk kepada Surat Pekeliling Perbendaharaan Bilangan 7 Tahun 1995 bertajuk "Garis Panduan Pelupusan Peralatan Komputer".	Semua
05.2.9	**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 di atas meja pekerja atau di paparan skrin apabila pekerja tidak berada di tempatnya : a. Gunakan kemudahan *password* screen saver atau log keluar apabila meninggalkan komputer; b. Bahan-bahan sensitif hendaklah disimpan dalam laci atau kabinet fail yang berkunci.	Semua
05.3	**Keselamatan Persekitaran**	
Objektif : Melindungi aset ICT KADA dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.		
05.3.1	**Kawalan Persekitaran**	
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi	Semua

	menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil : a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang ditempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah di larang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; dan g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurannya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	
05.3.2	**Bekalan Kuasa**	
	a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti UPS (*uninterruptible Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Juruteknik Elektrik dan Pengurus Teknikal

05.3.3	**Prosedur Kecemasan**	
	a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MAMPU 2004 ; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang di lantik mengikut aras;	Semua

PERKARA 06 PENGURUSAN OPERASI DAN KOMUNIKASI

06.1	**Pengurusan Prosedur Operasi**	
Objektif: Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan dengan betul dan selamat.		
06.1.1	**Pengendalian Prosedur**	
	a. Semua prosedur keselamatan ICT yang diwujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	ICTSO
06.1.2	**Kawalan Perubahan**	
	a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan;	Semua

	c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan;dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
06.1.3	**Prosedur Pengurusan Insiden**	
	Bagi memastikan tindakan menangani insiden keselamatan ICT di ambil dengan cepat, teratur dan berkesan; prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: a. Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c. Menyimpan jejak audit dan memelihara bahan bukti; dan d. Menyediakan tindakan pemulihan segera.	ICTSO dan Pengurus Teknikal
06.2	**Perancangan Dan Penerimaan Sistem**	
Objektif:	Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
06.2.1	**Perancangan Kapasiti**	
	a. Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO dan Pentadbir Sistem ICT
06.2.2	**Penerimaan Sistem**	
	Semua sistem baru (termasuklah sistem yang dikemas kini	ICTSO dan

	atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT
06.3	**Perisian Berbahaya**	
Objektif:	Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian yang berbahaya seperti virus dan trojan.	
06.3.1	**Perlindungan Dari Perisian Berbahaya**	
	a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan *Intrusion Detection System* (IDS) dan mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997; c. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; d. Mengemas kini *pattern* anti virus sebulan sekali; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Semua
06.4	**Housekeeping**	
Objektif:	Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.	
06.4.1	**Penduaan**	
	Bagi memastikan sistem dapat dibangunkan semula setelah	Semua

	berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan disimpan di *off site*. a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; dan c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan.	
06.4.2	**Sistem Log**	
	a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Mewujudkan satu system lod secara berpusat dan perlu dibuat pendua; c. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera;dan d. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	BTM dan Pengurus Teknikal
06.5	**Pengurusan Rangkaian**	
Objektif:	Melindungi maklumat dalam rangkaian dan insfrastruktur sokongan.	
06.5.1	**Kawalan Insfrastruktur Rangkaian**	
	Insfrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan : a. Tanggungjawab atau kerja-kerja operasi rangkaian dan operasi komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;	ICTSO dan Pengurus Teknikal

	b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja iaitu kakitangan dari seksyen sokongan dan operasi; d. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e. *Firewell* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi kerajaan serta dikonfigurasi oleh pentadbir sistem; f. Semua trafik keluar masuk hendaklah melalui *firewell* dibawah kawalan KADA; g. Semua perisian *sniffer* atau *network analyzer* atau perisian seumpama dengannya adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. Memasang perisian Intrusion Detection System (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat KADA. i. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan KADA hendaklah mendapat kebenaran ICTSO; k. Semua pengguna hanya dibenarkan menggunakan rangkaian KADA sahaja. Penggunaan modem atau melakukan penyambungan ke rangkaian lain atau yang seumpamanya, adalah dilarang sama sekali dan hendaklah mendapat kebenaran ICTSO; dan	

	l. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	
06.5.2	**Wireless**	
	Langkah-langkah minimum perlu dilaksanakan bagi memperkukuhkan kawalan keselamatan sistem rangkaian tanpa wayar (wireless). Berikut adalah langkah-langkah pengukuhan sistem rangkaian tanpa wayar : a. Langkah-langkah mesti mengikut Arahan Keselamatan dan para 4.4.3.2 *Malaysian Public Sector Management of ICT Security Handbook (MyMIS)* yang dikeluarkan oleh MAMPU pada 2001; b. Melaksanakan enkripsi ke atas wireless access point (AP); c. Meningkatkan keselamatan penggunaan wireless access point (AP) menerusi kaedah berikut : i) Menggunakan enkripsi dan network key yang kukuh dengan kombinasi pelbagai character seperti alphabet, aksara khas dan nombor; ii) Kerap menukar kata laluan atau network key; dan iii) Kawalan penggunaan MAC Address. d. Pengukuhan struktur rangkaian setempat boleh dilaksanakan seperti berikut : i) Mereka bentuk sistem rangkaian setempat supaya akses point menerusi wireless access point (AP) perlu melalui tapisan keselamatan yang sewajarnya; dan ii) Mereka bentuk kawalan capaian menggunakan pengenalan pengguna (*user authentication*) melalui penggunaan *Radius Server*. e. Pengukuhan keselamatan fizikal pula boleh dilaksanakan seperti berikut : i) Memasang alat reflector yang akan mengawal pancaran signal radio wireless access point (AP) dalam jarak yang	Semua

	dikehendaki; ii) Menggunakan cat dinding yang khas yang dapat menghalang pancaran signal supaya dapat melampaui jarak yang dikehendaki seperti *Defend Air Radio Shield Paint*; dan iii) Menggunakan *window shield* yang dapat menghalang signal daripada melepasi melalui tingkap.	
06.6	**Pengurusan Media**	
Objektif: Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak di kawal.		
06.6.1	**Penghantaran dan Pemindahan**	
	Penghantaran dan pemindahan media keluar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Semua
06.6.2	**Prosedur Pengendalian Media**	
	a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	Semua
06.6.3	**Keselamatan Sistem Dokumentasi**	
	a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian	ICTSO dan Pentadbir Sistem ICT

	sistem dokumentasi sedia ada.	
06.7	**Keselamatan Komunikasi**	
Objektif:	Melindungi aset ICT melalui sistem komunikasi yang selamat	
06.7.1	**Internet**	
	a. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan; b. Bahan yang diperoleh dari internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber internet hendaklah dinyatakan; c. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet; d. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh KADA; f. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertaluk kepada dasar dan peraturan yang telah ditetapkan; dan g. Maklumat lanjut mengenai keselamatan internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk " Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan".	Semua
06.7.2	**Mel Elektronik**	
	a. Akaun atau alamat mel elektronik (e-mail) yang diperuntukkan oleh KADA sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang;	Semua

	b. Setiap e-mel disediakan hendaklah mematuhi format yang telah ditetapkan oleh KADA; c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi 2 (dua) megabait semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; f. Pengguna hendaklah mengelak dari membuka e-mel dari penghantar yang tidak diketahui atau diragui; g. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; h. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;dan k. Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “ Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan”	

PERKARA 07 KAWALAN CAPAIAN

07.1	**Dasar Kawalan Capaian**
Objektif:	Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset KADA.

07.1.1	**Keperluan Dasar**	
	Capaian kepada proses dan maklumat hendaklah di kawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan , dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	BTM, ICTSO
07.2	**Pengurusan Capaian Pengguna**	
Objektif:	Mengawal capaian pengguna ke atas aset ICT KADA.	
07.2.1	**Akaun Pengguna**	
	Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi menenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh Jabatan sahaja boleh digunakan; b. Akaun pengguna mestilah unik; c. Akaun pengguna yang diwujud pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i) Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu; ii) Bertukar bidang tugas kerja; iii) Ke agensi lain; iv) Bertukar;	Semua

	v) Bersara; dan vi) Ditamatkan perkhidmatan	
07.2.2	**Jejak Audit**	
	Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi : a. Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan c. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan Pentadbir sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubah suaian yang tidak dibenarkan.	Pentadbir Sistem ICT
07.3	**Kawalan Capaian Sistem dan Aplikasi**	
Objektif:	Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.	
07.3.1	**Sistem Maklumat dan Aplikasi**	
	Capaian sistem dan aplikasi di KADA adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah di patuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;	Pentadbir Sistem ICT, ICTSO

	c. Memaparkan notis amaran pada skrin computer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d. Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; e. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan f. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	
07.4	**Peralatan Komputer Mudah Alih**	
Objektif:	Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.	
07.4.1	**Penggunaan Peralatan Komputer Mudah Alih**	
	a. Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; dan b. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Pentadbir Sistem ICT

Perkara 08 Perolehan, Pembangunan dan Penyelenggaraan Sistem Maklumat.

08.1	**Perolehan, Pembangunan dan Penyelenggaraan Sistem Maklumat.**
Objektif : Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian. CIO KADA bertanggungjawab : a. Memastikan kaedah keselamatan yang bersesuaian dikenalpasti, dirancang dan dilaksanakan pada setiap peringkat perolehan, pembangunan dan penyelenggaraan sistem maklumat; b. Melindungi kerahsiaan, integriti dan kesahihan maklumat menggunakan kaedah	

	tertentu; c. Memastikan sistem fail dan aktiviti berkaitan beroperasi dengan baik dan selamat; dan d. Menjaga dan menjamin keselamatan sistem maklumat.	
08.1.1	**Keperluan Keselamatan Sistem Maklumat**	**T/jawab**
	Memastikan keperluan keselamatan sistem maklumat dikenal pasti, dipersetujui dan didokumenkan pada setiap peringkat perolehan, pembangunan dan penyelenggaraan. Pernyataan keperluan bagi sistem maklumat baru atau penambahbaikan ke atas sistem sedia ada hendaklah menjelaskan mengenai kawalan jaminan keselamatan.	Semua
08.1.2	**Proses Aplikasi dengan Tepat**	
	Memastikan kawalan keselamatan yang sesuai dijalin ke dalam aplikasi 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 pencemaran maklumat sama ada kerana kesilapan atau disengajakan; c. Kawalan yang sesuai hendaklah dikenalpasti dan dilaksanakan 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
08.1.3	**Kawalan Kriptografi**	
	Memastikan kaedah kriptografi digunakan untuk melindungi kerahsiaan, kesahihan dan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut :	Pentadbir Sistem ICT

	a. Peraturan untuk melindungi maklumat menggunakan kaedah kriptografi yang sesuai hendaklah dibangunkan dan dilaksanakan; dan b. Memastikan kaedah yang selamat dan berkesan untuk pengurusan kunci yang menyokong teknik kriptografi diguna pakai di KADA.	
08.1.4	**Kawalan Perisian Operasi**	
	Memastikan kaedah yang sesuai dilaksanakan untuk mengawal capaian ke atas fail sistem dan kod sumber program bagi menjamin keselamatan 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
08.1.5	**Keselamatan Dalam Proses Pembangunan dan Sokongan**	
	Memastikan keselamatan perisian sistem aplikasi dan maklumat dikawal supaya selamat dalam semua keadaan. Perkara yang perlu dipatuhi adalah seperti berikut : a. Peraturan formal untuk mengawal perlaksanaan perubahan; b. Semakan teknikal selepas perubahan sistem operasi dibuat bagi menjamin tiada impak negetif ke atas keselamatan operasi KADA; c. Perubahan ke atas perisian dikawal dan terhad ke atas yang perlu sahaja; d. Semua peluang untuk kebocoran maklumat dihalang; dan e. Pembangunan perisian oleh pihak luar dikawal selia dan dipantau oleh KADA dari semasa ke semasa.	Pemilik Sistem, ICTSO, Pentadbir Sistem ICT

08.1.6	**Penyulitan**	
	Pengguna hendaklah membuat penyulitan (*encryption*) ke atas maklumat sensitive atau maklumat rahsia rasmi pada setiap masa.	Semua
08.1.7	**Tandatangan Digital**	
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rajsia rasmi secara elektronik.	Semua
08.1.8	**Pengurusan Kunci**	
	Pengurusan kunci hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
08.2	**Fail Sistem**	
Objektif : Memastikan supaya fail system dikawal dan dikendalikan dengan baik dan selamat.		
08.2.1	**Kawalan Fail Sistem**	
	a. Proses pengemaskini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statik, pemulihan dan keselamatan.	Pentadbir Sistem ICT

Perkara 09 Pengurusan Insiden Keselamatan ICT

09.1	**Pengurusan Insiden Keselamatan ICT**
Objektif : Memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan serta meminimumkan kesan insiden keselamatan ICT.	

09.1.1	Prosedur Pengurusan Insiden	T/jawab
	Prosedur pengurusan insiden perlu diwujudkan dan didokumenkan. Perkara yang perlu dipatuhi adalah seperti berikut : a. Mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c. Menyimpan audit trail dan memelihara bahan bukti; dan d. Menyediakan pelan tindakan pemulihan segera.	ICTSO
09.1.2	**Pelaporan Insiden**	
	Insiden keselamatan ICT hendaklah dilaporkan kepada ICTSO dengan kadar segera. Insiden keselamatan ICT adalah termasuk yang berikut : 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 disyaki digunakan tanpa kebenaran dan kecurian maklumat/data; c. Katalaluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Kejadian sistem luar kuasa seperti kehilangan fail, sistem kerap kali gagal berfungsi dan kesilapan/ralat dalam komunikasi data; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Nota 3: Pekeliling Am Bilangan 1 Tahun 2001 bertajuk “Mekanisme Pelaporan insiden Keselamatan ICT” boleh dirujuk.	Semua pengguna KADA

Perkara 10 Pengurusan Kesinambungan Perkhidmatan

10.1	**Dasar Kesinambungan Perkhidmatan**	
Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan memastikan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
10.1.1	**Pelan Pengurusan Kesinambungan Perkhidmatan.**	**T/jawab**
	Pelan Kesinambungan Perkhidmatan hendaklah dibangunkan untuk memastikan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian : a. Keperluan keselamatan maklumat dibangunkan untuk mengurus dan selenggara proses formal untuk mengawal perlaksanaan perubahan; b. Peraturan untuk menangani gangguan ke atas penyediaan perkhidmatan serta mengenal pasti keadaan tersebut, kebarangkalian berlaku dan kesan sekiranya berlaku; c. Merancang dan melaksana peraturan kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; d. Hanya satu rangka pelan kesinambungan perkhidmatan yang menyeluruh dibangunkan, di dokumentasikan, dipersetujui oleh pengurusan dan diselenggarakan bagi setiap KADA; dan e. Menguji dan mengemaskini pelan kesinambungan perkhidmatan untuk memastikan berkesan.	ICTSO, Pentadbir Sistem ICT

Perkara 11 Pematuhan

11.1	**Pematuhan dan Keperluan Perundangan**	
Objektif : Meningkatkan tahap keselamatan ICT bagi mengelak dari perlanggaran kepada Dasar keselamatan ICT KKM.		
11.1.1	**Pematuhan Dasar**	**T/jawab**
	Setiap Pengguna di KADA hendaklah membaca, memahami	Semua

	dan mematuhi Dasar Keselamatan ICT, undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa.	
11.1.2	**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 dikenalpasti, di dokumentasikan dan dikemaskini; b. Peraturan yang sesuai dilaksanakan untuk pematuhan ke atas perlembagaan, undang-undang dan keperluan kontrak mengenai penggunaan bahan 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 KADA; d. Perlindungan ke atas data dan hak milik peribadi hendaklah mematuhi perundangan, peraturan dan terma perjanjian jika perlu; e. Pengguna dilarang menggunakan kemudahan proses maklumat untuk tujuan yang tidak dibenarkan; dan f. Penggunaan kriptografi dikawal selaras dengan perjanjian, perundangan dan peraturan yang berkuatkuasa. Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di jabatan : a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk “Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan”;	Semua

	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 Jenayah Komputer 1997; h. Akta Hak cipta (Pindaan) tahun 1997; i. Akta Komunikasi dan Multimedia 1998; j. Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS); k. Pekeliling Am Kementerian Kesihatan Malaysia Bilangan 7 tahun 2005 bertajuk "Tatacara Penggunaan dan Keselamatan Rangkaian ICT Kementerian Kesihatan Malaysia; l. Surat KKM dengan rujukan KKM/BMTK/190/4/4 (9) bertajuk "Penggunaan Talian Streamyx di Kementerian Kesihatan Malaysia", dan m. 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".	
11.1.3	**Pematuhan kepada Dasar, Standard dan Teknikal Keselamatan.**	
	Dasar ini bertujuan memastikan keselamatan maklumat disemak secara berkala supaya patuh dan selaras dengan dasar dan standard keselamatan KADA. Perkara yang perlu dipatuhi adalah seperti berikut :	Semua

	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 perlaksanaan standard keselamatan yang ditetapkan.	