Perkara 01 Pembangunan dan Penyelenggaraan Dasar

Dasar Keselamatan ICT JAKOA		
	1. Pelaksanaan Dasar	**T/jawab**
Tanggungjawab melaksanakan dasar	Ketua Pengarah JAKOA 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.	Ketua Pengarah JAKOA
	2. Penyebaran Dasar	
Sebaran	Dasar ini bertujuan memastikan hala tuju pengurusan organisasi untuk melindungi aset ICT selaras dengan keperluan perundangan. Dasar ini perlu disasarkan kepada semua pengguna JAKOA (termasuk kakitangan, pembekal dan pakar runding yang berurusan dengan JAKOA).	ICTSO
	3. Penyelenggaraan Dasar	
Penyelarasan mengikut perubahan dan keperluan semasa	Dasar Keselamatan ICT JAKOA adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi aplikasi prosedur perundangan dan kepentingan sosial. Prosedur penyelenggaraan Dasar Keselamatan ICT JAKOA 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 ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatakuasa Pemandu ICT (JPICT) JAKOA ; dan (c) Memaklumkan perubahan dasar yang telah dipersetujui oleh JPICT kepada semua pengguna JAKOA.	ICTSO
	4. Pemakaian Dasar	
Pemakaian dan tiada pengecualian	Dasar Keselamatan ICT JAKOA adalah terpakai kepada semua pengguna ICT JAKOA dan tiada pengecualian diberikan.	Semua pengguna JAKOA

Perkara 02 Organisasi Keselamatan

Organisasi Keselamatan		
Objektif :	Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif JAKOA.	
	1. Ketua Pengarah JAKOA	**T/jawab**
Peranan dan tanggungjawab Ketua Pengarah JAKOA	Peranan dan tanggungjawab Ketua Pengarah JAKOA adalah seperti berikut : (a) Memastikan pelaksanaan pasukan penyelaras keselamatan ICT JAKOA; (b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT JAKOA; (c) Memastikan semua keperluan JAKOA (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 JAKOA.	Ketua Pengarah JAKOA
	2. Struktur Dalam Organisasi	
	Struktur formal dalam JAKOA 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 dari semua peringkat JAKOA 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	Semua Pengguna JAKOA

	pihak yang relevan dipelihara; dan (g) Memastikan kajian semula ke atas keselamatan maklumat dijalankan mengikut peraturan yang ditetapkan.	
	3. Peranan Ahli Pasukan Penyelaras Keselamatan ICT	
Objektif :	Menerangkan peranan dan tanggungjawab ahli pasukan penyelaras keselamatan ICT JAKOA.	
	3.1. Ketua Pegawai Maklumat (CIO)	
Peranan dan tanggungjawab CIO	Peranan dan tanggungjawab adalah termasuk seperti berikut: (a) Mewujud dan mengetuai pasukan penyelaras keselamatan ICT JAKOA; (b) Menasihati Ketua Pengarah JAKOA 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 memahami peruntukan di bawah Dasar Keselamatan ICT JAKOA.	CIO
	3.2. Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO	Peranan dan tanggungjawab adalah termasuk seperti berikut: (a) Mengurus keseluruhan program-program keselamatan ICT JAKOA; (b) Menguatkuasa dan memantau pematuhan Dasar Keselamatan ICT JAKOA; (c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT JAKOA kepada semua pengguna; (d) Mewujudkan garis panduan dan prosedur selaras dengan keperluan Dasar Keselamatan ICT JAKOA; (e) Menjalankan pengurusan risiko;	ICTSO

	(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 laporan mengenainya; (h) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkannya kepada CIO; (i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan (j) Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT JAKOA.	
	3.3 Pengurus Komputer	
Peranan dan tanggungjawab Pengurus Komputer	Peranan dan tanggungjawab adalah termasuk seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JAKOA; (b) Menentukan kawalan akses semua pengguna terhadap aset ICT kerajaan; (c) Menentukan tahap kawalan akses semua pengguna terhadap aset ICT kerajaan; (d) Melaporkan sebarang perkara atau penemuan/ancaman keselamatan ICT kepada ICTSO; dan (e) Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT JAKOA dilaksanakan.	Penyelaras ICT
	3.4. Pentadbir Sistem ICT	
Peranan dan tanggungjawab Pentadbir Sistem	Peranan dan tanggungjawab adalah termasuk seperti berikut:	Pentadbir Sistem ICT

ICT	(a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JAKOA; (b) Memastikan kerahsiaan kata laluan aset ICT; (c) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; (d) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar atau pihak ketiga yang berhenti atau tamat projek; (e) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamtan ICT JAKOA; (f) Memantau aktiviti capaian harian pengguna; (g) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (h) Menyimpan dan menganalisis rekod *audit trail*; dan (i) Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	
	3.5. Pengguna ICT JAKOA	
Peranan dan tanggungjawab Pengguna ICT JAKOA	Peranan dan tanggungjawab adalah termasuk seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT JAKOA; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Melepasi tapisan keselamatan (jika berkaitan); (d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat kerajaan; (e) Melaksanakan langkah-langkah perlindungan seperti berikut:	Semua Pengguna JAKOA

	(i) menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (ii) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (iii) Menentukan maklumat sedia untuk digunakan; (iv) Menjaga kerahsiaan kata laluan; (v) Mematuhi standard, 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. (f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; dan (g) Menghadiri program-program kesedaran mengenai keselamatan ICT.	
	4. Pihak luar/ketiga	
	Pihak JAKOA hendaklah memastikan keselamatan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar/ketiga dikawal. Perkara yang perlu dipatuhi adalah termasuk seperti berikut: (a) Mengenal pasti risiko keselamatan maklumat dan kemudahan proses maklumat dan laksana kawalan yang sesuai sebelum beri kebenaran capaian; (b) Mengenal pasti keperluan keselamatan sebelum membenarkan capaian atau penggunaan kepada pengguna luar. Capaian kepada aset ICT JAKOA perlu berlandaskan kepada perjanjian kontrak; dan (c) Memastikan semua keperluan keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga.	Pentadbir Sistem ICT dan Penyelaras ICT

	(d) Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai: (i) Dasar Keselamatan ICT JAKOA; (ii) Tapisan Keselamatan; (iii) Perakuan Akta Rahsia Rasmi 1972; dan (iv) Hak Harta Intelek <u>Nota 1:</u> 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.	

Perkara 03 Kawalan dan Pengelasan Aset

Akauntabiliti Aset		
Objektif :	Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT JAKOA.	
	1. Tanggungjawab ke atas Inventori Aset	**T/jawab**
	Memastikan semua aset ICT Kerajaan diberi perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset dikenal pasti dan maklumat aset direkodkan dalam borang daftar harta modal dan inventori (KEW.PA 2 dan KEW.PA 3) dan sentiasa dikemas kini. (b) Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan (c) Peraturan bagi penggunaan aset hendaklah dikenal pasti, didokumenkan dan dilaksanakan.	Semua Pengguna JAKOA Pengurus Aset

	2. Pengelasan Maklumat	
	Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan tahap sensitivity masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada JAKOA. 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; dan (iv) Terhad (b) Maklumat hendaklah dilabel dan dikenali berasaskan peringkat keselamatan yang dikenal pasti selaras dengan peraturan prosedur yang ditetapkan oleh JAKOA.	Semua Pengguna JAKOA
	3. Pengendalian Maklumat	
	Aktiviti pengendalian maklumat seperti pewujudan, pengumpulan pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendahlah 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 standard, prosedur dan garis panduan keselamatan yang dikeluarkan dari semasa ke semasa; (f) Memberi perhatian kepada pengendalian maklumat rahsia rasmi terperingkat terutama semasa pewujudan	Semua Pengguna JAKOA

	pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah pengurusan pengendalian maklumat rahsia rasmi keselamatan ICT dari diketahui umum.	

Perkara 04 Keselamatan Sumber Manusia

Keselamatan Sumber Manusia		
	Ketua Pengarah JAKOA adalah bertanggungjawab ke atas sumber manusia yang terlibat secara langsung atau tidak langsung dengan maklumat dan kemudahan proses maklumat di bawah kawalannya.	
	1. Sebelum Berkhidmat	**T/jawab**
	Memastikan penjawat awam, kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan memahami tanggungjawab masing-masing ke atas keselamatan ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT Kerajaan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peranan dan tanggungjawab penjawat awam, kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan mestilah dinyatakan dengan lengkap dan jelas; (b) Penyaringan dan pengesahan latar belakang calon untuk penjawat awam, kontraktor, pihak 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 da syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua Pengguna JAKOA

	2. Dalam Perkhidmatan	
	Memastikan semua pengguna JAKOA sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong dasar keselamatan ICT JAKOA dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT Kerajaan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua pengguna JAKOA mengurus keselamaan berdasarkan perundangan dan peraturan yang ditetapkan oleh JAKOA; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan ICT diberi kepada semua pengguna JAKOA dan sekiranya perlu diberi kepada kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan dari semasa ke semasa; dan (c) Memastikan adanya proses tindakan disiplin ke atas semua pengguna JAKOA sekiranya berlaku perlanggaran dengan perudangan dan peraturan ditetapkan JAKOA.	Semua Pengguna JAKOA
	3. Tamat Perkhidmatan atau Bertukar	
	Memastikan semua pengguna JAKOA diurus dengan teratur apabila tamat perkhidmatan atau bertukar dar JAKOA. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT Kerajaan dikembalikan kepada JAKOA mengikut peraturan yang ditetapkan JAKOA 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 JAKOA.	Semua Pengguna JAKOA

Perkara 05 Keselamatan Fizikal dan Persekitaran

Keselamatan Kawasan		
Objektif :	Mencegah akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan dan gangguan kepada premis dan maklumat.	

	1. 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) Mengehadkan jalan keluar masuk; (f) Mengadakan kaunter kawalan; (g) Mewujudkan system pas keselamatan; (h) Menyediakan tempat dan bilik khas untuk pelawat; (i) Mewujudkan perkhidmatan kawalan keselamatan; dan (j) Memasang alat penggera atau kamera (CCTV) jika berkaitan.	CIO dan ICTSO
	2. Kawalan Masuk Fizikal	
	Kawalan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis/bangunan JAKOA. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna JAKOA hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Setiap pihak luar/pelawat hendaklah mendaftar dan diwajibkan mendapat Pas Keselamatan di kaunter perkhidmatan pelanggan yang ditempatkan di pintu	Semua Pengguna JAKOA

	masuk terlebih dahulu sebelum ke tempat berurusan dan hendaklah memulangkan semual selepas selesai urusan (jika berkaitan); (c) Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila penjawat awam, kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan tamat perkhidmatan atau bersara (jika berkaitan); (d) Kehilangan pas keselamatan mestilah dilaporkan dengan segera kepada pentadbiran JAKOA; dan (e) Jurujual/Pegawai Pemasaran tidaj dibenarkan sama sekali berniaga/mempromosi barangan di premis JAKOA.	
	3. Keselamatan Aset ICT	
Objektif :	Melindungi peralatan dan maklumat daripada kehilangan, kerosakan kecurian atau salah guna aset dan gangguan ke atas aktiviti JAKOA.	
	3.1. Perkakasan	
	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 peralatan ICT di bawah kawalannya berfungsi dengan baik; (b) Semua perkakasan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan dilengkapi dengan ciri-ciri keselamatan; (c) Setiap pengguna adalah tanggungjawab di atas kerosakan dan kehilangan perkakakasan ICT di bawah kawalannya; dan (d) Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada Penyelaras ICT.	Semua Pengguna JAKOA
	3.2. Dokumen	
	Langkah-langkah pengurusan dokumentasi yang baik dan selamat perlu dilaksanakan bagi memastikan integriti maklumat.	Semua Pengguna JAKOA

	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; (b) Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, Terhad dan Terbuka kepada dokumen; (c) Mewujudkan sistem pengurusan dokumen terperingkat bagi menerima, memproses, menyimpan dan menghantar dokumen terperingkat supaya ianya diuruskan berasingan daripada dokumen-dokumen tidak terperingkat; dan (d) Menggunakan enkripsi *(encryption)* ke atas dokumen terperingkat yang disediakan dan dihantar secara elektronik.	
	3.3. Media Storan (seperti Pita Magentik,Cakera Keras, CD, *Optical Disk, Removal Disk (ThumbPen Drive)* dan lain-lain)	
	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, integrity dan kebolehsediaan maklumat yang di simpan 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) Mengehadkan akses untuk memasuki kawasan penyimpanan media kepada mereka atau 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 system pengurusan media termasuk inventori, pergerakan, melabel dan penduaan *(backup).*	Semua Pengguna JAKOA

	4. Prasarana Sokongan	
Objektif :	Melindungi aset ICT Kerajaan dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
	4.1 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 Kerajaan (KPKK).	Semua Pengguna JAKOA
	Perkara yang perlu dipatuhi bagi menjamin keselamatan persekitaran, adalah seperti berikut : (a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan computer 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 pencegah kebakaran dan pintu kecemasan; (c) Memasang peralatan perlindungan ditempat 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 da berjauhan dari aset ICT; (f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan computer; dan (g) Menyemak dan menguji semua peralatan perlindungan sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	
	4.2. Bekalan Kuasa	
	Perkara yang perlu dipatuhi bagi menjamin keselamatan	Ketua

	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 UPS (Uninterruptable Power Supply) 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.	Bahagian/Jabatan/ Unit/ Seksyen
	4.3. Prosedur Kecemasan	
	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh Pegawai Keselamatan JAKOA; (b) Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada Pegawai Keselamatan JAKOA; (c) Mengadakan, menguji dan mengemas kini pelan kecemasan dari semasa ke semasa; dan (d) Merancang dan mengadakan latihan kebakaran angunan *(fire drill)* secara berkala.	Semua Pengguna JAKOA
	4.4. 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 mengikuti 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 JAKOA

	(d) Membuat penamaan kabel menggunakan kod tertentu.	
	4.5. Penyelenggaraan Peralatan ICT	
	Perkakasan hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggarakan; (b) Memastikan perkakasan hanya di selenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; dan (d) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Penyelaras ICT
	4.6. Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat	
	Perkakasan yang dipinjam untuk kegunaan luar pejabat adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh JAKOA 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.	
	4.7. 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 JAKOA; (b) Mendapatkan kelulusan mengikut peraturan yang telag ditetapkan oleh JAKOA bagi membawa masuk/keluar peralatan; dan (c) Memerikda dan memastikan peralatan ICT yang dibawa keluar tidak mengandungi maklumat Kerajaan. Ia perlu disalin dan dihapuskan.	Penyelaras ICT
	4.8. 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 JAKOA: (a) Menghapuskan semua kandungan peralatan khususnya maklumat rahsia rasmi terlebih dahulu sama ada melalui rahsia rasmi terlebih dahulu sama ada melalui *shredding, grinding, degauzing* atau pembakaran sebelum pelupusan; dan (b) Rujuk Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan" untuk maklumat lanjut.	Semua Pengguna JAKOA
	4.9. *Clear Desk* dan *Clear Screen*	
	Semua maklumat dalam apa jua bentuk media hendaklah di simpan dengan teratur dan selamat bagi mengelakkan kerosakkan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitive 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 meninggalakan computer; (b) Menyimpan bahan-bahan sensitive di dalam laci atau cabinet fail yang berkunci; dan	Semua Pengguna JAKOA

	(c) Memastikan semua dokumen diambil segera dar pencetak, pengimbas, mesin faksimili dan mesin fotostat.	

Perkara 06 Pengurusan Operasi dan Komunikasi

Pengurusan Prosedur Operasi		
	Ketua Pengarah JAKOA adalah bertanggungjawab memastikan pengurusan operasi sistem dan komunikasi dapat berfungsi dengan betul dan selamat.	
	1. Tanggungjawab dan Prosedur Operasi	**T/jawab**
	Memastikan kemudahan pemprosesan maklumat beroperasi seperti yang ditetapkan dan selamat. Perkara yang perlu dipatuhi adalah seperti: (a) Semua prosedur operasi keselamatan ICT hendaklah dikenal pasti, didokumenkan dengan jelas lagi teratur, di kemas kini dan boleh diguna pakai oleh pengguna mengikut keperluan; (b) Setiap perubahan kepada sistem dan kemudahan pemprosesan maklumat mestilah dikawal; (c) Tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset JAKOA; dan (d) Kemudahan ICT untuk pembangunan, pengujian dan operasi mestilah diasingkan agi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah kepada system yang sedang beroperasi.	ICTSO dan Penyelaras ICT
	2. 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	Pentadbir Sistem ICT

	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 menambahbaikan polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	
	3. Perancangan dan Penerimaan Sistem	
Objektif :	Mengurangkan risiko kegagalan atau gangguan sistem. 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 akan datang untuk memastikan prestasi sistem di tahap optimum; (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.	Pentadbir Sistem ICT
	4. Perlindungan dari *Malicious Code* (Kod Jahat)	
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 :	Semua Pengguna JAKOA

	(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 di lindungi di bawah hak cipta terpelihara; (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; (d) Mengemaskini paten anti virus dari semasa ke semasa; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktivit yang tidak dingini 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 in bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; (i) Mengedar amaran mengenai ancaman seperti serangan virus terhadap keselamatan aset ICT JAKOA; (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.	
	5. Housekeeping	
Objektif :	Mengekalkan integriti. Kebolehsediaan maklumat dan kemudahan pemprosesan maklumat.	

	5.1. Penduaan (Backup)	
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, Salinan penduaan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan disimpan di lokasi yang berlainan *(off site).* Perkara yang perlu dipatuhi adalah seperti berikut: (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 kesesuaian 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; dan (d) Salinan maklumat dan perisian perlu dibuat dan diuji secara berkala berdasarkan kepada prosedur penduaan.	Pentadbir Sistem ICT
	5.2. Sistem Log	
	Perkara yang perlu dipatuhi adalah seperti berikut : (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	Pentadbir Sistem ICT
	6. Pengurusan Keselamatan Rangkaian	
Objektif :	Memastikan perlindungan keselamatan maklumat dalam rangkaian dan infrastruktur sokongan terurus dan terkawal.	
	6.1. Kawalan Infrastruktur Rangkaian	
	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian.	Pentadbir Sistem ICT

	Perkara yang perlu dipatuhi adalah seperti berikut : (a) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi 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 berkenaan disediakan secara dalaan atau melalui perkhidmatan 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 dilokasi 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) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; (g) *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta di konfigurasi oleh pentadbir sistem yang dibenarkan sahaja; (h) Semua trafik keluar dan masuk hendaklah melalui *Firewall* di bawah kawalan JAKOA; (i) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; (j) Memasang perisian *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan akiviti-aktiviti lain yang boleh mengancam sistem dan maklumat jabatan;	

	(k) Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktivti yang dilarang seperti yang termaktub di dalam PKPA 1/2003; (l) Sebarang penyambungan rangkaian yang bukan di bawah kawalan JAKOA hendaklah mendapat kebenaran BTMK, JAKOA ; (m) Penggunaan modem adalah dilarang sama sekali bagi pengguna rangkaian MOH*Net; (n) Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum; (o) Penggunaan rangkaian Streamyx hendaklah mematuhi surat JAKOA dengan rujukan JAKOA/BTMK/190/4/4 (9) bertajuk "Penggunaan Talian Streamyx di KKLW"; dan (p) Penggunaan tanpa wayar LAN di JAKOA 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".	
	7. 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.	
	7.1. 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 JAKOA. Prosedur perlu disediakan untuk pengurusan media mudah alih.	Pentadbir Sistem ICT
	7.2. Penghapusan	
	Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	Pentadbir Sistem ICT

	Nota 2: Pekeliling Perbendaharaan Bilangan 5 Tahun 2007 bertajuk "Tatacara Pengurusan Aset Alih Kerajaan" boleh dirujuk.	
	7.3. Prosedur Pengendalian Maklumat	
	Prosedur ini bertujuan untuk mengendali dan menyimpan maklumat perlu diwujudkan untuk melindungi maklumat daripada di dedah tanpa kebenaran atau di salah guna. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua media hendaklah dilabelkan mengikut tahap sensitiviti sesuatu maklumat; (b) Mengehadkan dan menentukan capaian kepada pengguna yang dibenarkan sahaja; (c) Mengehadkan pengedaran data untuk tujuan rasmi dan dibenarkan sahaja; (d) Penyelenggaraan media hendaklah dikawal dan direkodkan bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan (e) Semua media hendaklah disimpan di tempat yang selamat.	Pentadbir Sistem ICT
	7.4. Keselamatan Sistem Dokumentasi	
	Dokumentasi sistem perlu dilindungi dari capaian yang tidak 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.	Semua Pengguna JAKOA
	8. Keselamatan Komunikasi Rangkaian	
Objektif:	Memastikan keselamatan pertukaran maklumat dan perisian dalam JAKOA dan mana-mana entity luar terjamin.	Semua Pengguna JAKOA

	Perkara yang perlu dipatuhi adalah seperti berikut: (a) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran makluamt melalui penggunaan pelbagai jenis kemudahan komunikasi; dan (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara JAKOA dan pihak luar.	
	8.1. Internet	
	Capaian Internet perlu dikawal dan diurus bagi mengelakkan gangguan sistem rangkaian JAKOA. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Laman yang dilayri hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan; (b) Bahan yang diperolehi dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendakalh 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 JAKOA; (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 Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk “Garis Panduan Mengenai Tatacara Penggunaan	Semua Pengguna JAKOA

	Internet dan Mel Elektronik di Agensi-agensi Kerajaan".	
	8.2. Mel Elektronik	
	Maklumat yang terdapat dalam mel elektronik JAKOA 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 JAKOA 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 JAKOA; (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 kepilkan, sekiranya perlu, tidak melebihi dua (2) megabit 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 identity 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	Semua Pengguna JAKOA

	arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; dan (j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat. **8.3. Perkhidmatan e-Dagang**	
Objektif :	Memastikan keselamatan perkhidmatan e-dagang dan penggunaannya. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Maklumat yang terlibat dalam e-dagang perlu dilindungidaripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam 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 daripada pengubahsuaian yang tidak dibenarkan.	Semua Pengguna JAKOA
	9. 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 dihasilkan 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	Pentadbir Sistem ICT

	direkodkan; (e) Kesalahan yang dilakukan perlu di log (rekod), di analisa san di ambil tindakan sewajarnya; dan (f) Masa yang berkaitan dengan sistem pemprosesan maklumat dalam JAKOA atau domain keselamatan perlu diselaraskan dengan satu sumber tepat yang dipersetujui.	

Perkara 07 Kawalan Capaian

Kawalan Capaian		
	Ketua Pengarah JAKOA adalah bertanggungjawab ke atas kawalan capaian aset ICT. Kawalan capaian ini mesti dilaksanakan dengan berkesan berasaskan keperluan pengguna dan keselamatan.	
	1. Keperluan Kawalan Capaian	**T/jawab**
Objektif :	Mengawal capaian ke atas makluamt, kemudah proses maklumat, dan proses urus niaga berdasarkan keperluan urus niaga dan keperluan keselamatan. Peraturan kawalan capaian hendaklah mengambil kira faktor *identification, authentication* dan *authorization*.	Semua Pengguna JAKOA
	1.1 Dasar Kawalan Capaian	
	Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan pengurusan JAKOA dan keselamatan. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Kawalan capaian ke atas maklumat dan proses urus niaga mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Kawalan capaian ke atas *information process facilities* seperti capaian pengguna; dan (d) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih.	Semua Pengguna JAKOA

	2. Pengurusan Capaian Pengguna	
Objektif :	Memastikan bahawa sistem makluamt dicapai oleh pengguna yang sah dan menghalang capaian yang tidak sah. Prosedur pendaftaran dan pembatalan kebenaran capaian pengguna perlu diwujudkan dan didokumenkan. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat; (b) Akaun pengguna yang di wujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran Ketua Jabatan secara bertulis dan direkodkan; (c) Pemilikan akaun 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; (iii) melebihi satu tempoh yang ditentukan oleh Ketua Jabatan; (iv) pengguna bertukar jawatan, tanggunagjawab dan/ atau bidang tugas; (v) pengguna bertukar atau berpindah agensi; dan (vi) pengguna bersara atau tamat perkhidmatan. (d) Aktiviti capaian oleh pengguna di rekod, di selenggara dengan sistematik dan dikaji dari semasa ke semasa. Maklumat yang direkod termasuk identity pengguna, sumber yang digunakan, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi diguna dan aktiviti capaian secara sah atau sebaliknya.	Pentadbir Sistem atau Penyelaras ICT
	3. Tanggungjawab Pengguna	

Objektif :	Memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan proses maklumat. 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 JAKOA
	4. Kawalan Capaian Rangkaian	
Objektif :	Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang menepati kesesuaian penggunaannya di antara rangkaian JAKOA dan rangkaian lain-lain organisasi; dan (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan, yang menepati kesesuaian penggunaannya. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Memastikan pengguna boleh mencapai perkhidmatan yang dibenarkan sahaja; (b) Mewujudkan mekanisme pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh; (c) Menggunakan kaedah pengenalan automatic berdasarkan lokasi dan peralatan untuk pengesahan sambungan ked ala rangkaian; (d) Mengawal capaian fizikal dan logical ke atas kemudahan port diagnostic dan konfigurasi jarak jauh; (e) Mengasingkan capaian mengikut kumpulan perkhidmatan maklumat, pengguna dan sistem maklumat dalam rangkaian;	Pentadbir Sistem ICT

	(f) Mengawal sambungan ke rangkaian, khususnya bagi kemudahan yang dikongsi dan menjangkau sempadana JAKOA; dan (g) Mewujud dan melaksana kawalan pengalihan laluan *(routing control)* untuk memastikan pematuhan ke atas peraturan JAKOA.	
	5. Kawalan Capaian Sistem Operasi	
Objektif :	Memastikan bahawa capaian ke atas sistem operasi dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja. Kaedah yang digunakan hendaklah mampu menyokong perkara berikut : (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan JAKOA; (b) Mewujudkan *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) Mengehadkan tempoh penggunaan mengikut kesesuaian. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem operasi menggunakan prosedur log-on yang selamat; (b) Prosedur log-on yang selamat perlulah : (i) Menggunakan kaedah pengenalan penggunaan yang unik dan teknik pengesahan yang berkesan dan selamat; (ii) Melaksana sistem pengurusan kata laluan yang interaktif dan menjamin kualiti serta keselamatan kata laluan; (iii) Mengawal penggunaan utility yang berkeupayaan melepasi sistem dan aplikasi terhad;	Pentadbir Sistem ICT

	(vi) Menamatkan sesi yang tidak aktif selepas tempoh masa yang ditetapkan; dan (v) Hadkan tempoh masa penggunaan bagi meningkatkan keselamatan aplikasi yang berisiko tinggi.	
	6. Kawalan Capaian Aplikasi dan Maklumat	
Objektif :	Menghalang capaian tidak sah ke atas sistem aplikasi dan maklumat. Kawalan capaian hendaklah : (a) Membenarkan pengguna mencapai aplikasi dan maklumat mengikut tahap capaian yang ditentukan; (b) Menyediakan mekanisme perlindungan bagi menghalang capaian tidak sah ke atas aplikasi dan maklumat daripada utility yang sedia ada dalam sistem operasi dan perisian malicious yang berupaya melangkaui kawalan sistem; dan (c) Tidak berkrompomi dengan sebarang sistem yang berkongsi sumber. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Capaian ke atas maklumat dan fungsi sistem aplikasi oleh pengguna pelu dihadkan, selaras dengan peraturan JAKOA; dan (b) Sistem yang sensitive perlu persekitaran pengkomputeran yang khusus dan terasing.	Pentadbir Sistem ICT
	7. 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

Perkara 08 Perolehan, Pembangunan dan Penyelenggaraan Sistem Maklumat

Perolehan, Pembangunan dan Penyelenggaraan Sistem Maklumat		
Objektif :	Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
	Ketua Pengarah JAKOA bertanggungjawab : (a) Memastikan kaedah keselamatan yang bersesuaian dikenal pasti, 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.	
	1. Keperluan Keselamatan Sistem Maklumat	**T/jawab**
Objektif :	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 Pengguna JAKOA
	2. Proses Aplikasi dengan Tepat	
Objektif :	Memastikan kawalan keselamatan yang sesuai dijalin je 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;	Semua Pengguna JAKOA

	(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 dikenal pasti dan dilaksana 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.	
	3. 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 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 oleh JAKOA.	Pentadbir Sistem ICT
	4. 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
	5. Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif :	Memastikan keselamatan perisian sistem aplikasi dan	Pentadbir Sistem ICT

	maklumat dikawal supaya selamat dalam semua keadaan. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Peraturan formal untuk mengawal pelaksanaan perubahan; (b) Semakan teknikal selepas perubahan sistem operasi dibuat bagi menjamin tiada impak negative keatas keselamatan operasi JAKOA; (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 JAKOA dari semasa ke semasa.	

Perkara 09 Pengurusan Insiden Keselamatan ICT

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

	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 digunkan tanpa kebenaran dan kecurian maklumat/data; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; (d) Kejadian sistem luar biasa seperti kehilangan fail, sistem kerap kali gagal fungsi dan kesilapan/ralat dalam komunikasi data; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dingin. <u>Nota 3 :</u> Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisma Pelaporan Insiden Keselamatan ICT" boleh dirujuk.	Semua Pengguna JAKOA

Perkara 10 Pengurusan Kesinambungan Perkhidmatan

Dasar Kesinambungan Perkhidmatan		
Objektif :	Menjamin operasi perkhidmatan agar tidak tergendala dan memastikan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
	1. Pelan Pengurusan Kesinambungan Perkhidmatan	**T/jawab**
	Pelan Kesinambungan Perkhidmatan hendaklah dibangunkan untuk memastikan pendekatan yang menyeluruh dilaksanakan bagi mengatasi gangguan ke atas aktiviti penyediaan perkhidmatan JAKOA dan melindungi perkhidmatan dalam tempoh yang ditetapkan. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Keperluan keselamatan maklumat dibangunkan untuk mengurus dan selenggara proses formal untuk mengawal pelaksanaan perubahan;	ICTSO, Pentadbir Sistem ICT

	(b) Peraturan untuk menangani gangguan ke atas penyediaan perkhidmatan dengan 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 JAKOA; dan (e) menguji dan mengemas kini pelan kesinambungan perkhidmatan untuk memastikan berkesan.	

Perkara 11 Pematuhan

Pematuhan dan Keperluan Perundangan		
Objektif :	Meningkatkan tahap keselamatan ICT bagi mengelak dari perlanggaran kepada Dasar Keselamatan ICT JAKOA	
	1. Pematuhan Dasar	**T/jawab**
	Setiap Pengguna di JAKOA hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT, undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa.	Semua Pengguna JAKOA
	2. Keperluan Perundangan	
	Dasar ini bertujuan memastikan reka bentuk, operasi, penggunaan dan pengurusan sistem maklumat adalah selaras serta berkeupayaan menghalang perlanggaran mana-mana keperluan perundangan, peraturan dan perjanjian yang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut : (a) Semua perlembangaan, undang-undang, peraturan, perjanjian yang dimeterai dan lain-lain perkar yang releven kepada keselamatan siste maklumat dan organisasi hendaklah dikenal pasti, di dokumentasikan dan dikemas kini;	Semua Pengguna JAKOA

	(b) Peraturan yang sesuai dilaksanakan untuk pematuhan ke atas perlembagaan, undang-undang dan keperluan kontrak mengenai penggunaan bahan yang tertakluk kepada hak milik intelek; (c) Rekod penting hendaklah dilindungi daripada hilang, rosak dan dipalsukan selaras dengan keperluan undang-undang, peraturan dan keperluan perjanjian JAKOA; (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"; (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 1977; (g) Akta Jenayah Komputer 1997;	

	(h) Akta Hak Cipta (Pindaan) Tahun 1977; (i) Akta Komunikasi dan Multimedia 1998; (j) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS); (k) Pekeliling Am Kementerian Kemajuan Luar Bandar Dan Wilayah Malaysia Bilangan 7 Tahun 2005 bertajuk "Tatacara Penggunaan dan Keselamatan Rangkaian ICT Kementerian Kesihatan"; (l) Surat KKLW dengan rujukan KKM/BTMK/190/4/4(9) bertajuk "Penggunaan Talian 1Gov*Net di Kementerian Kemajuan Luar Bandar Dan Wilayah; 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".	
	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 JAKOA. 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 pelaksaan standard keselamatan yang ditetapkan.	Semua Pengguna JAKOA