KEMENTERIAN SUMBER MANUSIA
JABATAN PEMBANGUNAN KEMAHIRAN

JPK

CIAST

DASAR KESELAMATAN ICT

PUSAT LATIHAN PENGAJAR &
KEMAHIRAN LANJUTAN

Dasar Keselamatan ICT CIAST
Diterbitkan pada Januari 2011 (Edisi 1.0)

ISI KANDUNGAN

PENGENALAN

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

OBJEKTIF

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

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

Manakala, objektif utama Keselamatan ICT CIAST ialah seperti berikut:

(a) Memastikan kelancaran operasi CIAST dan meminimumkan kerosakan atau kemusnahan;

(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

(c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT.

Terdapat empat (4) komponen asas keselamatan ICT iaitu:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

(c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

(d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT CIAST merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(a) Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

(b) Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

(c) Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

(d) Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan

(e) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; ancaman yang wujud akibat daripada kelemahan tersebut; risiko yang mungkin timbul; dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Aset ICT CIAST terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT CIAST menetapkan keperluan-keperluan asas berikut:

(a) Data dan maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan

(b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT CIAST ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkaraperkara berikut:

(a) Perkakasan
Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan CIAST. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian
Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada CIAST;

(c) Perkhidmatan
Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

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

(d) Data dan Maklumat
Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif CIAST. Contohnya, sistem dokumentasi, prosedur operasi, rekodrekod CIAST, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

(e) Manusia
Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian CIAST bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan; dan

(f) Premis Komputer Dan Komunikasi
Semua kemudahan serta premis yang digunakan untuk menempatkan perkara **(a)** - **(e)** di atas. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

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

(a) Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut.

(b) Hak akses minimum

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

(c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah CIAST menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka. Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;
iii. Menentukan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi 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.

(d) Pengasingan

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

(e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

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

(f) Pematuhan

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

(g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan pelan pemulihan bencana/ kesinambungan perkhidmatan; dan

(h) Saling Bergantungan

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

BIDANG 01 **PEMBANGUNAN DAN PENYELENGGARAAN DASAR**	
0101 Dasar Keselamatan ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan CIAST dan perundangan yang berkaitan.	
010101 Pelaksanaan Dasar	
Pelaksanaan dasar ini akan dijalankan oleh Pengarah CIAST selaku Pengerusi Pengurusan Keselamatan dan Kesihatan Pekerjaan (KKP) CIAST. Jawatankuasa Keselamatan ICT (JKICT) di bawah KKP ini terdiri daripada Ketua Pegawai Maklumat (CIO), Pengurus ICT, Pegawai Keselamatan ICT (ICTSO), Pentadbir Sistem ICT dan semua Ketua Bahagian/Program.	Pengarah CIAST
010102 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna CIAST (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO
010103 Penyelenggaraan Dasar	
Dasar Keselamatan ICT CIAST adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT CIAST: (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT), CIAST; (c) Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JKICT; dan (d) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	ICTSO
010104 Pengecualian Dasar	
Dasar Keselamatan ICT CIAST adalah terpakai kepada semua pengguna ICT CIAST dan tiada pengecualian diberikan.	Semua Pengguna

BIDANG 02 **ORGANISASI KESELAMATAN**	
0201 Infrastruktur Organisasi Dalaman	
Objektif: Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT CIAST.	
020101 Pengarah CIAST	
Pengarah CIAST adalah berperanan dan bertanggungjawab dalam perkara-perkara seperti berikut: (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT CIAST; (b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT CIAST; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT CIAST; dan	Pengarah CIAST
020102 Ketua Pegawai Maklumat (CIO)	
Ketua Pegawai Maklumat (CIO) bagi CIAST ialah Timbalan Pengarah (Pengurusan Latihan). Peranan dan tanggungjawab CIO adalah seperti berikut: (a) Membantu Pengarah dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Menentukan keperluan keselamatan ICT; (c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT CIAST serta pengurusan risiko dan pengauditan; dan (d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT CIAST. (e) Mempengerusikan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT), CIAST.	CIO

020103 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) bagi CIAST ialah Ketua Penyelaras Program Unit Infrastruktur (KPP IF1), Program Pembelajaran Elektronik dan Multimedia (PEM). Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Mengurus keseluruhan program-program keselamatan ICT CIAST; (b) Menentukan kawalan akses pengguna terhadap aset ICT; (c) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT CIAST. (d) Menjalankan pengurusan risiko; (e) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan CIAST berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (f) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (g) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan (h) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	ICTSO
020104 Pengurus ICT	
Pengurus ICT bagi CIAST ialah Ketua Program Pembelajaran Elektronik dan Multimedia (KP PEM). Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan CIAST; (b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT CIAST; (c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT CIAST kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT CIAST;	Pengurus ICT

(e) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO;	
020105 Pentadbir Sistem ICT	
Pentadbir Sistem ICT bagi CIAST ialah Ketua Penolong Pengarah Unit Infrastruktur (KPP IF2), Program Pembelajaran Elektronik dan Multimedia (PEM). Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang 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 CIAST; (c) Memantau aktiviti capaian harian sistem aplikasi pengguna; (d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (e) Menganalisis dan menyimpan rekod jejak audit; (f) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan (g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	Pentadbir Sistem ICT
020106 Pengguna	
Pengguna mempunyai peranan dan tanggungjawab seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT CIAST; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Lulus tapisan keselamatan; (d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT CIAST dan menjaga kerahsiaan maklumat CIAST;	Semua Pengguna

(e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan ICT;	
020107 Jawatankuasa Keselamatan ICT CIAST	
Jawatankuasa Keselamatan ICT (JKICT) adalah jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT CIAST. Keanggotaan JKICT CIAST adalah seperti berikut: **Pengerusi :** CIO CIAST **Setiausaha:** ICTSO Ahli: (1) Pengurus ICT; (2) Pentadbir Sistem; (3) Ketua Bahagian / Program; dan (4) lain-lain ahli yang dilantik dari semasa ke semasa. Urusetia bagi JKICT CIAST adalah Unit Infrastruktur, PEM. **Bidang kuasa:** (a) Memperakukan/meluluskan dokumen DKICT CIAST; (b) Memantau tahap pematuhan keselamatan ICT; (c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam CIAST yang mematuhi keperluan DKICT CIAST; (d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; (e) Memastikan DKICT CIAST selaras dengan dasar-dasar ICT kerajaan semasa; (f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; (g) Membincang tindakan yang melibatkan pelanggaran DKICT CIAST; dan (h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	JKICT CIAST

0202 Pihak Ketiga	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).	
020101 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT CIAST; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; (d) Akses kepada aset ICT CIAST perlu berlandaskan kepada perjanjian kontrak; (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT CIAST; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek.	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

BIDANG 03 PENGURUSAN ASET	
0301 Akauntabiliti Aset	
Objektif: Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT CIAST.	
030101 Inventori Aset ICT	
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini; (b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di CIAST; (d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan (e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pengurus ICT, Pentadbir Sistem, Pegawai Aset dan Semua Pengguna.
0302 Pengelasan dan Pengendalian Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
030201 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad	Semua Pengguna
030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah	Semua Pengguna

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.	

BIDANG 04 KESELAMATAN SUMBER MANUSIA	
0401 Keselamatan Sumber Manusia Dalam Tugas Harian	
Objektif: Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan CIAST, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga CIAST hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
040101 Sebelum Perkhidmatan	
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan CIAST serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua
040102 Dalam Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan pegawai dan kakitangan CIAST serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh CIAST; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT CIAST secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan CIAST serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh CIAST; dan (d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Program Pembelajaran Eletronik dan Multimedia (PEM), CIAST.	Semua

040103 Bertukar atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada CIAST mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturanyang ditetapkan oleh CIAST dan/atau terma perkhidmatan.	Semua

BIDANG 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN	
0501 Keselamatan Kawasan	
Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
050101 Kawalan Kawasan	
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (c) Memasang alat penggera atau kamera; (d) Menghadkan jalan keluar masuk; (e) Mengadakan kaunter kawalan; (f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; (g) Mewujudkan perkhidmatan kawalan keselamatan; (h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan. (j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; (k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Pengarah, CIO, Pengurus ICT, ICTSO

050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Setiap pengguna CIAST hendaklah menunjukkan kad pekerja mereka apabila diminta oleh pegawai yang diberi kuasa; (b) Semua pas bekerja hendaklah diserahkan balik kepada CIAST apabila pengguna berhenti atau bersara; (c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama CIAST. Pas ini hendaklah dikembalikan semula selepas tamat lawatan. (d) Kehilangan pas mestilah dilaporkan dengan segera. (e) Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT CIAST.	Semua
050103 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di CIAST adalah bilik Pengarah, bilik Timbalan Pengarah, bilik *server,* kabinet *switch,* pusat kawalan CCTV, bilik PABX, stor aset ICT dan makmal-makmal komputer. (a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan (b) Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Semua
0502 Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT CIAST dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
050201 Kawalan Kawasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;	Semua Pengguna

(c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

(d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;

(e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

(f) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

(g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

(h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;

(i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS);

(j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci.

(k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;

(l) Peralatan ICT yang hendak dibawa keluar dari premis CIAST, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan;

(m) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

(n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

(o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;

(p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada ICTSO untuk dibaik pulih;

(q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

(r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (s) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT; (t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (u) Pengguna hendaklah memastikan semua perkakasan komputer,pencetak dan pengimbas dalam keadaan "*OFF*" apabila meninggalkan pejabat; (v) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan (w) Memastikan plag dicabut daripada suis utama (*main switch*) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
050202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; (c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Akses dan pergerakan media storan hendaklah direkodkan;	Semua Pengguna
050203 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan CIAST;	Semua pengguna

(b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; (c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan di tempat yang selamat berasingan daripada CD-ROM *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan (d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah direkod.	
050204 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan perkakasan hanya boleh diselenggara oleh pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT. (g) Pengguna hendaklah mematuhi Arahan Pengurusan yang berkaitan dengan penyelenggaraan komputer masing-masing.	Pegawai Aset ICT dan Semua Pengguna
050205 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis CIAST adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua Pengguna

050206 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh CIAST dan ditempatkan di CIAST Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan CIAST. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; (b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; (c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (d) Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (f) Pegawai Aset ICT bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori Sistem Pengurusan Aset (SPA); (g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan (h) Pengguna ICT adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran computer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di CIAST; iii. Memindah keluar dari CIAST mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab CIAST; dan	Pegawai Aset ICT / Urusetia Pelupusan Aset ICT

v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	

0503 Keselamatan Persekitaran

Objektif:

Melindungi aset ICT CIAST dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

050301 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 Pengurus ICT. Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: (a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; (b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; (c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; (d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; (e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; (f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; (g) Semua peralatan perlindungan hendaklah disemak dan diuji. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan (h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	Semua pengguna

050302 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT.	Pengurus ICT dan ICTSO

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; (b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) 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.	
050303 Kabel	
Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pengurus ICT dan ICTSO
050304 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur / manual / dasar / panduan keselamatan dan kesihatan pekerjaan CIAST; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Kesihatan Pekerjaan CIAST.	Semua Pengguna dan Pegawai Keselamatan dan Kesihatan Pekerjaan CIAST
0504 Keselamatan Dokumen	
Objektif: Melindungi maklumat CIAST dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	

050401 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan Akta Arkib Negara; dan (e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua