



DASAR KESELAMATAN ICT

PEJABAT KETUA PEGAWAI KESELAMATAN KERAJAAN MALAYSIA (CGSO)

Versi 2.1

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	1 dari 84

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
25 FEB 2009	2.0	JPICT CGSO BIL 1/2009	18 MAC 2009
30 SEPT 2012	2.1	Mesyuarat DKICT	11 OKTOBER 2012

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	2 dari 84

JADUAL PINDAAN DASAR KESELAMATAN ICT CGSO

TARIKH	VERSI	PINDAAN
30 SEPT 2012	2.1	i. Tajuk baru: Penilaian Risiko Keselamatan ICT , muka surat 17 ii. Perkara K02/01/03 Pegawai Keselamatan ICT (ICTSO), mukasurat: 23 perenggan baru iaitu perenggan (k) menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan. iii. Perkara K02/01/04 Pengurus ICT, muka surat 22, tambahan maklumat Pengurus ICT iv. Perkara K02/01/05 Pentadbir Sistem ICT, muka surat 24, tambahan maklumat Pentadbir Sistem ICT. v. Perkara K02/01/06 Pengguna perenggan (c), muka surat 25, menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rahsia rasmi.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	3 dari 84

KANDUNGAN

Pengenalan	9
Objektif	9
Pernyataan Dasar	10
Skop	12
Prinsip-Prinsip	14
Penilaian Risiko Keselamatan ICT	17
 Kawalan 01 Dasar Keselamatan ICT	 18
Objektif	18
K01/01 Perlaksanaan Dasar	18
K01/02 Penyebaran Dasar	18
K01/03 Penyelenggaraan Dasar	18
K01/04 Pengecualian Dasar	19
 Kawalan 02 Organisasi Keselamatan	 20
Objektif	20
K02/01 Infrastruktur Organisasi Dalaman	20
K02/01/01 Ketua Pengarah	20
K02/01/02 Ketua Pegawai Maklumat (CIO)	20
K02/01/03 Pegawai Keselamatan ICT (ICTSO)	21
K02/01/04 Pengurus ICT	22
K02/01/05 Pentadbir Sistem ICT	22
K02/01/06 Pengguna	23
K02/01/07 Jawatankuasa Keselamatan ICT CGSO (JKICT)	23
K02/01/08 CGSO CERT	24
K02/02 Pihak Ketiga	26
K02/02/01 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	26
 Kawalan 03 Pengurusan Aset	 27
Objektif	27
K03/01 Inventori Aset	27
K03/02 Pengelasan dan Pengendalian Maklumat	27
K03/02/01 Pengelasan Maklumat	27
K03/02/02 Pengendalian Maklumat	28

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	4 dari 84

KAWALAN 04 KESELAMATAN SUMBER MANUSIA	29
K04/01 Keselamatan ICT Dalam Tugas Harian	29
Objektif	29
K04/01/01 Sebelum Perkhidmatan	29
K04/01/02 Dalam Perkhidmatan	29
K04/01/03 Bertukar Atau Tamat Perkhidmatan	30
 KAWALAN 05 KESELAMATAN FIZIKAL	 31
K05/01 Keselamatan Kawasan	31
Objektif	31
K05/01/01 Keselamatan Fizikal	31
K05/01/02 Kawalan Masuk Fizikal	32
K05/01/03 Kawasan Larangan	32
K05/02 Keselamatan Peralatan	33
Objektif	33
K05/02/01 Peralatan ICT	33
K05/02/02 Media Storan	35
K05/02/03 Media Tandatangan Digital	36
K05/02/04 Media Perisian dan Aplikasi	36
K05/02/05 Penyelenggaraan	36
K05/02/06 Peralatan Di Luar Premis	37
K05/02/07 Pelupusan Perkakasan	37
K05/03 Keselamatan Persekitaran	39
Objektif	39
K05/03/01 Kawalan Persekitaran	39
K05/03/02 Bekalan Kuasa	40
K05/03/03 Kabel	40
K05/03/04 Prosedur Keselamatan	41
K05/04 Keselamatan Dokumen dan Sistem Dokumentasi	41
Objektif	41
K05/04/01 Dokumen	41
 KAWALAN 06 PENGURUSAN OPERASI DAN KOMUNIKASI	 43
K06/01 Pengurusan Prosedur Operasi	43
Objektif	43
K06/01/01 Pengendalian Dokumen Prosedur Operasi	43
K06/01/02 Kawalan Perubahan	43

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	5 dari 84

	K06/01/03 Pengasingan Tugas dan Tanggungjawab	44
K06/02	Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	44
	Objektif	44
	K06/02/01 Perkhidmatan Penyampaian	44
K06/03	Perancangan dan Penerimaan Sistem	45
	Objektif	45
	K06/03/01 Perancangan Kapasiti	45
	K06/03/02 Penerimaan Sistem	45
K06/04	Perisian Berbahaya	45
	Objektif	45
	K06/04/01 Perlindungan dari Perisian Berbahaya	46
	K06/04/02 Perlindungan dari <i>Mobile Code</i>	46
K06/05	<i>Housekeeping</i>	46
	Objektif	47
	K06/05/01 Backup	47
K06/06	Pengurusan Rangkaian	47
	Objektif	47
	K06/06/01 Kawalan Infrastruktur Rangkaian	47
K06/07	Pengurusan Media	48
	Objektif	48
	K06/07/01 Penghantaran dan Pemindahan	49
	K06/07/02 Prosedur Pengendalian Media	49
	K06/07/03 Keselamatan Sistem Dokumentasi	49
K06/08	Pengurusan Pertukaran Maklumat	49
	Objektif	49
	K06/08/01 Pertukaran Maklumat	50
	K06/08/02 Pengurusan Mel Elektronik (E-mel)	50
K06/09	Pemantauan	51
	Objektif	51
	K06/09/01 Pengauditan dan Forensik ICT	52
	K06/09/02 Jejak Audit	52
	K06/09/03 Sistem Log	53
	K06/09/04 Pemantauan Log	53
KAWALAN 07 KAWALAN CAPAIAN		55
K0701	Kawalan Capaian	55
	Objektif	55

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	6 dari 84

K07/02	Pengurusan Capaian Pengguna	55
	Objektif	55
	K07/02/01 Akaun Pengguna	55
	K07/02/02 Hak Capaian	56
	K07/02/03 Pengurusan Kata Laluan	56
	K07/02/04 <i>Clear Desk</i> dan <i>Clear Screen</i>	57
K07/03	Kawalan Capaian Rangkaian	58
	Objektif	58
	K07/03/01 Capaian Rangkaian	58
	K07/03/02 Capaian Internet	58
K07/04	Kawalan Capaian Sistem Pengoperasian	60
	Objektif	60
	K07/04/01 Capaian Sistem Pengoperasian	60
	K07/04/01 Kad Pintar	61
K07/05	Kawalan Capaian Aplikasi dan Maklumat	61
	Objektif	61
K07/06	Peralatan Mudah Alih dan Kerja Jarak Jauh	62
	Objektif	62
	K07/06/01 Peralatan Mudah Alih	62
	K07/06/02 Kerja Jarak Jauh	62
KAWALAN 08	PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	63
K08/01	Keselamatan Dalam Membangunkan Sistem dan Aplikasi	63
	Objektif	63
	K08/01/01 Keperluan Keselamatan Sistem Maklumat	63
	K08/01/02 Pengesahan Data Input dan Output	63
K08/02	Kawalan Kriptografi	64
	Objektif	64
	K08/02/01 Enkripsi	64
	K08/02/02 Tandatangan Digital	64
	K08/03/03 Pengurusan Infrastruktur Kunci Awam (<i>PKI</i>)	64
K08/03	Keselamatan Sistem Fail	64
	Objektif	64
K08/04	Pembangunan dan Sokongan Sistem	65
	Objektif	65

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	7 dari 84

	K08/04/01 Prosedur Kawalan Perubahan	65
	K08/04/02 Pembangunan Secara Outsource	65
K08/05	Kawalan Teknikal Keterdedahan (Vulnerability)	66
	Objektif	66
	K08/05/01 Kawalan dari Ancaman Teknikal	66
KAWALAN 09	PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN	67
K09/01	Mekanisme Pelaporan Insiden Keselamatan ICT	67
	Objektif	67
	K09/01/01 Mekanisme Pelaporan	67
K09/02	Pengurusan Maklumat Insiden Keselamatan ICT	68
	Objektif	68
KAWALAN 10	PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	70
K10/01	Dasar Kesenambungan Perkhidmatan	70
	Objektif	70
	K10/01/01Pelan Kesenambungan Perkhidmatan	70
KAWALAN 11	PEMATUHAN	72
K11/01	Pematuhan dan Keperluan Perundangan	72
	Objektif	72
	K11/01/01 Pematuhan Dasar	72
K11/02	Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	72
K11/03	Pematuhan Keperluan Audit	72
K11/04	Keperluan Perundangan	73
K11/05	Pelanggaran Dasar	73
7	GLOSARI	74
8	LAMPIRAN	
	Lampiran 1	78
	Lampiran 2	79
	Lampiran 3	83

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	8 dari 84

PENGENALAN

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

OBJEKTIF

Dasar Keselamatan ICT CGSO diwujudkan untuk menjamin kesinambungan urusan CGSO dengan meminimumkan kesan insiden keselamatan ICT. Objektif utama Dasar Keselamatan ICT CGSO ialah seperti berikut:

- (a) Memastikan kelancaran operasi dan perkhidmatan CGSO dan meminimumkan kerosakan atau kemusnahan;
- (b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;
- (c) Mencegah salah guna atau kecurian aset ICT Kerajaan;
- (d) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;
- (e) Meningkatkan tahap kesedaran keselamatan ICT kepada kakitangan, pengguna dan pembekal;
- (f) Memperkukuhkan pengurusan risiko;
- (g) Melindungi aset ICT daripada penyalahgunaan oleh personel, pengguna dan pembekal

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	9 dari 84

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Keselamatan perlindungan ada lah suatu proses berterusan yang tidak boleh dikompromi. Ia melibatkan aktiviti berterusan yang mesti dilakukan dari semasa ke semasa kerana ancaman dan kelemahan terhadap keselamatan 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 daripada sumber yang sah.

Dasar Keselamatan ICT CGSO merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan ketersediaan 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;

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	10 dari 84

- b) Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas- kini. Ia hanya boleh diubah dengan cara yang dibenarkan seperti yang terkandung di dalam Arahan Keselamatan;
- 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;
- 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 seperti:

- a) Ancaman yang wujud akibat daripada kelemahan tersebut;
- b) Risiko yang mungkin timbul; dan
- c) Langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	11 dari 84

SKOP

Aset ICT CGSO terdiri daripada personel, data atau maklumat, perkakasan, perisian, telekomunikasi dan kemudahan ICT. Dasar Keselamatan ICT CGSO 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 sistem 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 dan tidak menjejaskan perkhidmatannya.

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

a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan agensi. Contohnya komputer, *Server*, 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;

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	12 dari 84

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.
- iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawa dingin, sistem pencegah kebakaran dan lain-lain.

d) Data atau Maklumat

Maklumat terkumpul dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif CGSO. Contoh: Sistem dokumentasi, prosedur operasi, rekod-rekod agensi, 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 bagi mencapai misi dan objektif CGSO. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

f) Premis Komputer dan Komunikasi

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

Setiap perkara di atas perlu diberi perhatian sewajarnya. Sebarang kebocoran maklumat rasmi/ rahsia rasmi atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah keselamatan.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	13 dari 84

PRINSIP-PRINSIP

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

a) Akses atas dasar Prinsip Perlu Mengetahui

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar Prinsip Perlu Mengetahui sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan perenggan 53 Arahan Keselamatan;

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 mewujudkan, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu maklumat. Hak akses perlu dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab setiap personel CGSO yang terlibat;

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 mampu menyokong kemudahan mengesan atau mengesahkan 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;

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	14 dari 84

- 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 mewujudkan, memadam, mengemaskini, 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, *server*, *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

f) Pematuhan

Dasar Keselamatan ICT CGSO 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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	15 dari 84

dilakukan melalui aktiviti penduaan dan mewujudkan pelan kesinambungan perkhidmatan; dan

h) Saling Bergantungan

Setiap prinsip di atas adalah saling 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.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	16 dari 84

PENILAIAN RISIKO KESELAMATAN ICT

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

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat CGSO termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain. CGSO bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling Am Bilangan 6 Tahun 2005: Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

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

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

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	17 dari 84

KAWALAN 01
DASAR KESELAMATAN ICT

Objektif:

DKICT CGSO diwujudkan untuk melindungi aset ICT bagi memastikan kelancaran operasi jabatan secara berterusan, meminimumkan kerosakan atau kemusnahan aset-aset ICT melalui usaha pencegahan atau mengurangkan kesan kejadian yang tidak diingini berdasarkan kepada ciri-ciri keselamatan iaitu kerahsiaan, integriti, tidak boleh disangkal, kebolehsediaan dan kesahihan.

K01/01 Pelaksanaan Dasar

	Pelaksanaan dasar ini akan dijalankan oleh Ketua Pengarah CGSO dibantu oleh Jawatankuasa Keselamatan ICT CGSO yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), dan ahli-ahli yang dilantik oleh Ketua Pengarah.	Ketua Pengarah CGSO
--	---	------------------------------------

K01/02 Penyebaran Dasar

	Dasar ini perlu disebarkan kepada semua pengguna CGSO (termasuk kakitangan, pembekal, pakar runding dan lain-lain)	ICTSO
--	--	--------------

K01/03 Penyelenggaraan Dasar

	DKICT CGSO adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, polisi Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan DKICT CGSO: (a) Menenal pasti dan tentukan perubahan yang diperlukan; (b) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO dan sekiranya perlu ICTSO akan mengangkat untuk	ICTSO
--	--	--------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	18 dari 84

	pertimbangan Jawatankuasa Keselamatan ICT (JKICT) CGSO; (c) Memaklumkan perubahan yang telah dipersetujui oleh JKICT kepada semua pihak iaitu kakitangan, pengguna dan pembekal; dan (d) Menyemak semula dokumen sekurang-kurangnya sekali setahun atau mengikut keperluan bagi memastikan dokumen sentiasa relevan.	
K01/04 Pengecualian Dasar		
	DKICT CGSO adalah terpakai kepada semua pengguna ICT dan tiada pengecualian diberikan.	Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	19 dari 84

KAWALAN 02 ORGANISASI KESELAMATAN

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT CGSO.

K02/01 Infrastruktur Organisasi Dalam

K02/01/01 Ketua Pengarah CGSO

	Peranan dan tanggungjawab Ketua Pengarah CGSO adalah seperti berikut: (a) Memastikan pengguna memahami peruntukan-peruntukan di bawah DKICT CGSO; (b) Memastikan pengguna mematuhi DKICT CGSO; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT CGSO; dan (d) Mempengerusikan Jawatankuasa Keselamatan ICT (JPIC), CGSO	Ketua Pengarah CGSO
--	---	-----------------------------------

K02/01/02 Ketua Pegawai Maklumat (CIO)

	Jawatan Ketua Pegawai Maklumat (CIO) CGSO adalah disandang oleh Timbalan Ketua Pengarah (Dasar) . Peranan dan tanggungjawab CIO adalah seperti berikut: (a) Membantu Ketua Pengarah CGSO dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT;	CIO
--	--	-------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	20 dari 84

	(b) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT CGSO; (c) Bertanggungjawab menyelaraskan dan mengurus pelan tindakan dan program keselamatan seperti penyediaan DKICT CGSO, pelan latihan dan kesedaran pengguna, pengurusan risiko dan pengauditan; dan (d) Menentukan keperluan keselamatan ICT;	
--	---	--

K02/01/03 Pegawai Keselamatan ICT (ICTSO)

	Jawatan ICTSO bagi CGSO adalah disandang oleh Pengarah Bahagian Keselamatan ICT dan Rahsia Rasmi. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a) Mengurus keseluruhan program-program keselamatan ICT CGSO; b) Menkuatkuasakan pelaksanaan DKICT CGSO; c) Memberi penerangan dan pendedahan berkenaan DKICT CGSO kepada semua pengguna; d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT CGSO; e) Menjalankan pengurusan risiko; f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan CGSO berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT Kerajaan (GCERT), MAMPU dan memaklukkannya kepada CIO; i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT	ICTSO
--	--	--------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	21 dari 84

	dan memperakukan langkah-langkah baik pulih dengan segera; dan j) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan k) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
--	--	--

K02/01/04 Pengurus ICT

	Ketua Unit Teknologi Maklumat CGSO merupakan Pengurus ICT CGSO. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a) Mengkaji semula melaksanakan kawalan keselamatan ICT selaras dengan keperluan CGSO; b) Menentukan kawalan akses pengguna terhadap aset ICT CGSO; c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT CGSO.	Pengurus ICT
--	---	---------------------

K02/01/05 Pentadbir Sistem ICT

	Pegawai Teknologi Maklumat di Cawangan Operasi dan Rangkaian merupakan Pentadbir Sistem ICT di CGSO . 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	Pentadbir Sistem ICT
--	---	-----------------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	22 dari 84

	capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT CGSO; 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 memberhentikanannya 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.	
--	---	--

K02/01/06 Pengguna

	Pengguna mempunyai peranan dan tanggungjawab seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT CGSO; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rahsia rasmi; d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT CGSO dan menjaga kerahsiaan maklumat CGSO; e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan g) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT CGSO sebagaimana Lampiran 1.	Pengguna
--	--	-----------------

K02/01/07 Jawatankuasa Keselamatan ICT CGSO

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	23 dari 84

	Jawatankuasa Keselamatan ICT (JKICT) merupakan jawatankuasa yang bertanggungjawab dalam keselamatan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi keselamatan ICT CGSO. Keanggotaan JKICT CGSO adalah seperti berikut: Pengerusi : Ketua Pengarah CGSO Ahli : (1) CIO CGSO (2) Timbalan Ketua Pengarah (Operasi) (3) Semua Pengarah Bahagian (4) ICTSO CGSO Urus Setia bagi JKICT CGSO ialah Unit Keselamatan ICT Bidang kuasa: a) Memperakukan/meluluskan dokumen DKICT CGSO; b) Memantau tahap pematuhan keselamatan ICT; c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi aplikasi khusus dalam CGSO yang mematuhi keperluan DKICT CGSO; d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; e) Memastikan DKICT CGSO selaras dengan dasar-dasar ICT kerajaan semasa; f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa; g) Membincang tindakan yang melibatkan pelanggaran DKICT CGSO; dan h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	JKICT CGSO
K02/01/09 Pasukan Tindak Balas Insiden Keselamatan ICT CGSO (CGSO CERT)		
	Keanggotaan CGSO CERT adalah seperti berikut: Pengerusi: ICTSO CGSO	CGSO CERT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	24 dari 84

	Ahli : 1. Pegawai Teknologi Maklumat di Unit Teknologi Maklumat 2. Pegawai Teknologi Maklumat di Unit Keselamatan ICT 3. Timbalan Pengarah Unit Keselamatan ICT 4. Penolong Pegawai Teknologi Maklumat Kanan di Unit Teknologi Maklumat 5. Penolong Pegawai Keselamatan Kerajaan di Unit Keselamatan ICT Urusetia: Unit Teknologi Maklumat Peranan dan tanggungjawab CGSO CERT adalah seperti berikut: (a) Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; (b) Merekod dan menjalankan siasatan awal insiden yang diterima; (c) Menangani tindak balas (<i>response</i>) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; (d) Menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai <i>input</i> atau untuk tindakan seterusnya; dan (e) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT untuk mengelakkan sebarang insiden.	
--	--	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	25 dari 84

K02/02 Pihak Ketiga

Objektif:

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).

K02/02/01 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 CGSO; (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 CGSO perlu berlandaskan kepada perjanjian kontrak; (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak luar/asing. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT CGSO; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; iv. Hak Harta Intelek; dan v. Arahan Teknologi Maklumat.	CIO, CTSO, Pengurus ICT , Pentadbir Sistem ICT dan Pihak Ketiga
--	---	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	26 dari 84

KAWALAN 03 PENGURUSAN ASET

03/01 Akauntabiliti Aset

Objektif :

Untuk memberikan perlindungan keselamatan yang bersesuaian ke atas semua aset ICT CGSO.

K03/01/01 Inventori Aset

	Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: (a) Memastikan semua aset dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemaskini; (b) memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (c) memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di CGSO; (d) memastikan peraturan bagi pengendalian aset dikenal pasti, didokumen dan dilaksanakan; dan (e) Memastikan setiap pengguna adalah bertanggungjawab ke atas semua aset ICT dibawah seliaannya.	Pentadbir Sistem dan semua
--	--	--

K03/02 Pengelasan dan Pengendalian Maklumat

K03/02/01 Pengelasan Maklumat

	Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh Pegawai yang diberi kuasa mengikut Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam Arahan Keselamatan seperti berikut:	Semua
--	--	---------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	27 dari 84

	(a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad.	
K03/02/02 Pengendalian Maklumat		
	Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampaikan, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut : (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; (c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	Semua

KAWALAN 04
KESELAMATAN SUMBER MANUSIA

K04/01 Keselamatan ICT Dalam Tugas Harian

Objektif:

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan CGSO, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga CGSO hendaklah mematuhi terma dan syarat perkhidmatan dan peraturan semasa yang berkuat kuasa.

K04/01/01 Sebelum Perkhidmatan

	Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab personel, atau pihak ketiga seperti pembekal, pakar runding dan lain-lain yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk personel, atau pihak ketiga yang terlibat selaras dengan keperluan perkhidmatan; dan (c) Memastikan semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan agar dipatuhi.	Semua
--	---	--------------

K04/01/02 Dalam Perkhidmatan

	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan personel, atau pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh CGSO;	Semua
--	---	--------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	29 dari 84

	(b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT CGSO 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 personel, atau pihak ketiga yang berkepentingan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan oleh CGSO; 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, pihak pengguna boleh merujuk kepada Bahagian Latihan dan Kompetensi atau Unit Teknologi Maklumat CGSO.	
K04/01/03 Bertukar Atau Tamat Perkhidmatan		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada CGSO 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 peraturan yang ditetapkan CGSO dan/atau terma perkhidmatan.	Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	30 dari 84

KAWALAN 05
KESELAMATAN FIZIKAL

K05/01 Keselamatan Kawasan

Objektif :

Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat.

K05/01/01 Keselamatan Fizikal

	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. (b) Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (c) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; (d) Memasang alat penggera atau kamera; (e) Mengehadkan jalan keluar masuk; (f) Mengadakan kaunter kawalan; (g) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; (h) Mewujudkan perkhidmatan kawalan keselamatan; (i) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (j) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; (k) Mereka bentuk dan melaksanakan perlindungan fizikal dari	CIO, ICTSO
--	--	-------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	31 dari 84

	kebakaran, banjir, letupan, kacau-bilau dan bencana; (l) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (m) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	
K05/01/02 Kawalan Masuk Fizikal		
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Setiap pengguna CGSO hendaklah memakai pas keselamatan sepanjang waktu bertugas; (b) Setiap pelawat hendaklah mendaftar seterusnya mendapatkan Pas Keselamatan Pelawat di pintu masuk Kompleks Jabatan Perdana Menteri dan hendaklah dikembalikan semula selepas tamat urusan; (c) Semua pas keselamatan hendaklah diserahkan semula kepada CGSO apabila pengguna bertukar ke jabatan lain, berhenti atau bersara. (d) Kehilangan pas mesti dilaporkan dengan segera.	Semua
K05/01/03 Kawasan Larangan		
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di CGSO ialah bilik Ketua Pengarah, bilik-bilik Timbalan Ketua Pengarah dan bilik server . Akses kepada bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberikan kuasa sahaja: (a) Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik, supaya boleh digunakan bila perlu. (b) Pihak ketiga dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi	Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	32 dari 84

	perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan (c) Semua penggunaan peralatan yang melibatkan penghantaran, kemaskini dan penghapusan maklumat rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Pengarah CGSO.	
--	---	--

K05/02 Keselamatan Peralatan
Objektif:

Melindungi peralatan ICT CGSO daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

K05/02/01 Peralatan ICT

	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; (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 disamping melakukan imbasan ke atas media storan yang digunakan; (g) Penggunaan kata laluan untuk akses ke sistem komputer	Semua
--	---	--------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	33 dari 84

	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. (k) Peralatan rangkaian seperti switches, hub, router dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; (l) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (air ventilation) yang sesuai; (m) Peralatan ICT yang hendak dibawa keluar dari premis CGSO, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan; (n) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera; (o) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (p) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT; (q) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih; (r) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (s) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (t) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (administrator password) yang telah ditetapkan oleh Pentadbir Sistem ICT;	
--	--	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	34 dari 84

	(u) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (v) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan <i>ready to use</i> apabila meninggalkan pejabat; (w) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; dan (x) Memastikan plag dicabut daripada suis utama (main switch) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
K05/02/02 Media Storan		
	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, <i>optical disk</i>, <i>flash disk</i>, CDROM, <i>Thumb Drive</i> dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan ketersediaan 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 daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang	Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	35 dari 84

	mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; (e) Akses dan pergerakan media storan hendaklah direkodkan;	
K05/02/03 Media Tandatangan Digital		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Semua
K05/02/04 Media Perisian dan Aplikasi		
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan CGSO; (b) Sistem aplikasi dalaman tidak dibenarkan diagih/didemonstrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; (c) Lesen perisian (<i>registration code, serials, CD-keys</i>) perlu disimpan berasingan daripada <i>CD-rom, disk</i> atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan (d) <i>Source code</i> sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua
K05/02/05 Penyelenggaraan		
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan ketersediaan, kerahsiaan dan integriti.	Pegawai Aset dan Unit Teknologi

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	36 dari 84

	Langkah-langkah keselamatan yang perlu diambil termasuklah seperti berikut: (a) Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (b) Mematuhi spesifikasi yang ditetapkan oleh pengeluar bagi semua perkakasan yang diselenggara; (c) Memastikan perkakasan hanya diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pihak pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Memastikan pihak ketiga mematuhi segala arahan dan peraturan yang ditetapkan oleh CGSO.	Maklumat
K05/02/06 Peralatan di Luar Premis		
	Perkakasan yang dibawa keluar dari premis CGSO 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
K05/02/07 Pelupusan Perkakasan		
	Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh CGSO dan ditempatkan di CGSO. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan CGSO.	Semua, Pegawai Aset, Unit Teknologi Maklumat

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	37 dari 84

	Langkah-langkah seperti berikut hendaklah dipatuhi: (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 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 bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ; (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 komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di CGSO; iii. Memindah keluar dari CGSO mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja	
--	--	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	38 dari 84

	pelupusan di bawah tanggungjawab CGSO; dan v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau thumb drive sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
--	--	--

K05/03 Keselamatan Persekitaran
Objektif:

Melindungi aset ICT CGSO daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaiian atau kemalangan.

K05/03/01 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 Bahagian Kelengkapan Fizikal dan Inovasi, CGSO. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: (a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan susun 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	Semua
--	--	--------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	39 dari 84

	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 sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan (h) Akses kepada saluran riser hendaklah sentiasa dikunci.	
--	--	--

K05/03/02 Bekalan Kuasa

	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa: (a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik; (b) peralatan sokongan seperti <i>Uninterruptable Power Supply</i> (UPS) dan penjana (<i>generator</i>) 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.	Pengurus ICT dan ICTSO
--	---	------------------------

K05/03/03 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	Unit ICT dan ICTSO
--	---	--------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	40 dari 84

	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.	
--	---	--

K05/03/04 Prosedur Kecemasan

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Bertugas yang dilantik.	Semua, Pegawai Bertugas
--	--	--

K05/04 Keselamatan Dokumen dan Sistem Dokumentasi

Objektif:

Melindungi maklumat CGSO daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuai.

K05/04/01 Dokumen

	Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan sistem dokumentasi: (a) Memastikan kaedah penyimpanan dokumen selaras dengan Arahan Keselamatan; (b) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada; (c) Setiap dokumen hendaklah ditanda dan dilabelkan mengikut klasifikasi keselamatan seperti Terhad, Sulit, Rahsia atau Rahsia Besar; (d) Pergerakan fail dan dokumen hendaklah direkodkan dan	Semua
--	---	---------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	41 dari 84

	perluah mengikut prosedur Arahan Keselamatan; (e) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (f) Pelupusan dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (g) Menggunakan penyulitan (<i>encryption</i>) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	
--	---	--

KAWALAN 06
PENGURUSAN OPERASI DAN KOMUNIKASI

K06/01 Pengurusan Prosedur Operasi

Objektif:

Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

K06/01/01 Pengendalian Dokumen Prosedur Operasi

	(a) Semua prosedur keselamatan ICT yang diwujudkan, dikenalpasti dan masih digunakan hendaklah didokumenkan, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan.	Semua
--	--	-------

K06/01/02 Kawalan Perubahan

	(a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah	Semua
--	--	-------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	43 dari 84

	ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
--	--	--

K06/01/03 Pengasingan Tugas dan Tanggungjawab

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahan yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujudkan, memadam, kemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan daripada perkakasan yang digunakan sebagai production. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pengurus ICT, ICTSO
--	---	----------------------------

K06/02 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga
Objektif:

Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.

K06/02/01 Perkhidmatan Penyampaian

	Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga;	Semua
--	--	--------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	44 dari 84

	(b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan (c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	
--	---	--

K06/03 Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

K06/03/01 Perancangan Kapasiti

	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; Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	ICTSO, Pengurus ICT
--	--	---------------------------

K06/03/02 Penerimaan Sistem

	Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	ICTSO, Pentadbir Sistem ICT
--	---	-----------------------------------

K06/04 Perisian Berbahaya

Objektif:

Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.

K06/04/01 Perlindungan dari Perisian Berbahaya

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	45 dari 84

	Perkara-perkara yang perlu dilaksanakan bagi memastikan perlindungan aset ICT dari perisian berbahaya: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, <i>Intrusion Detection System</i> (IDS) dan <i>Intrusion Prevention System</i> (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuatkuasa; (c) Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; (d) Mengemaskini antivirus dengan <i>pattern</i> antivirus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (g) Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Semua
--	---	-------

K06/04/02 Perlindungan dari *Mobile Code*

	Penggunaan mobile code yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
--	---	-------

K06/05 Housekeeping

Objektif:

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	46 dari 84

Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

K06/05/01 Backup

	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, <i>backup</i> seperti yang disenaraikan hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-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 <i>backup</i> ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan <i>backup</i> bergantung pada tahap kritikal maklumat; dan (c) Menyimpan sekurang-kurangnya tiga (3) generasi backup; dan (d) Merekod dan menyimpan salinan backup di lokasi yang berlainan dan selamat.	Semua
--	--	-------

K06/06 Pengurusan Rangkaian
Objektif:

Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

K06/06/01 Kawalan Infrastruktur Rangkaian

	Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Langkah-langkah bagi menangani ancaman ke atas rangkaian adalah seperti berikut: (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko	Unit ICT
--	---	----------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	47 dari 84

	seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan mestilah melalui proses <i>Factory Acceptance Check (FAC)</i> semasa pemasangan dan konfigurasi; (e) <i>Firewall</i> hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi, diselenggara dan diselua oleh pentadbir sistem; (f) Semua trafik keluar dan masuk hendaklah melalui <i>firewall</i> di bawah kawalan CGSO; (g) Semua perisian <i>sniffer</i> atau <i>network analyser</i> adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; (h) Memasang perisian <i>Intrusion Prevention System (IPS)</i> bagi mengesan sebarang cubaan mencerooboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat CGSO; (i) Memasang <i>Web Content Filtering</i> pada <i>Internet Gateway</i> untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan CGSO adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian CGSO sahaja dan penggunaan modem adalah dilarang sama sekali; dan (l) Kemudahan bagi wireless LAN perlu dipastikan kawalan keselamatan.	
--	---	--

K06/07 Pengurusan Media

Objektif:

Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

K06/07/01 Penghantaran dan Pemindahan

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	48 dari 84

	Penghantaran atau pemindahan media yang mengandungi maklumat terperingkat ke luar pejabat hendaklah mendapat kebenaran daripada CIO terlebih dahulu.	Semua
K06/07/02 Prosedur Pengendalian Media		
	Di antara prosedur-prosedur pengendalian media termasuk: (a) Melabelkan semua media elektronik mengikut ketetapan pemeringkatan berdasarkan Arahan Keselamatan; (b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; dan (f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Semua
K06/07/03 Keselamatan Sistem Dokumentasi		
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Semua
K06/08 Pengurusan Pertukaran Maklumat		
Objektif: Memastikan keselamatan pertukaran maklumat dan perisian antara CGSO dan agensi luar terjamin.		

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	49 dari 84

K06/08/01 Pertukaran Maklumat

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (b) Pertukaran maklumat dan perisian di antara CGSO dengan mana-mana pihak perlu mematuhi Arahan Keselamatan dan Akta Rahsia Rasmi 1972; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari CGSO; dan (d) Polisi dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi maklumat yang berhubung kait dengan sistem maklumat CGSO.	Semua
--	---	-------

K06/08/02 Pengurusan Mel Elektronik (E-mel)

	Penggunaan e-mel di CGSO hendaklah dipantau secara berterusan oleh Pentadbir Sistem untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" dan mana-mana undang-undang bertulis yang berkuatkuasa: Di antara langkah-langkah pengendalian mel elektronik termasuk: a) Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh CGSO 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 CGSO; c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;	Semua
--	---	-------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	50 dari 84

	d) Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; e) Pengguna dinasihatkan menggunakan fail kepilai, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; f) Pengguna hendaklah mengelak daripada membuka e-mel daripada penghantar yang tidak diketahui atau diragui; g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; h) Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; i) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; j) Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; k) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; l) Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan mailbox masing-masing.	
--	---	--

K06/09 Pemantauan
Objektif:

Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

K06/09/01 Pengauditan dan Forensik ICT

	ICTSO mestilah bertanggungjawab merekod dan menganalisis	ICTSO
--	--	-------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	51 dari 84

	perkara-perkara berikut: a) Sebarang percubaan pencerobohan kepada sistem ICT CGSO; b) Serangan kod perosak (malicious code), halangan pemberian perkhidmatan (denial of service), spam, pemalsuan (forgery, phishing), pencerobohan (intrusion), ancaman (threats) dan kehilangan fizikal (physical loss); c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f) Aktiviti instalasi dan penggunaan perisian yang membebaskan jalur lebar (bandwidth) rangkaian; g) Aktiviti penyalahgunaan akaun e-mel; dan h) Aktiviti penukaran alamat IP (IP address) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	
K06/09/02 Jejak Audit		
	Setiap sistem mestilah mempunyai jejak audit (audit trail). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a) Rekod setiap aktiviti transaksi; b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan	Pentadbir Sistem ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	52 dari 84

	d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
--	---	--

K06/09/03 Sistem Log

	Pentadbir Sistem hendaklah melaksanakan perkara-perkara 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 lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem hendaklah melaporkan kepada CIO, ICTSO dan Pengurus ICT.	Pentadbir Sistem ICT
--	---	----------------------

K06/09/04 Pemantauan Log

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu	Pentadbir Sistem ICT, Unit ICT
--	--	--------------------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	53 dari 84

	dipantau secara berkala; c) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan f) Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam CGSO atau domain keselamatan perlu diselaraskan dengan sumber waktu yang dipersetujui.	
--	--	--

KAWALAN 07

KAWALAN CAPAIAN

Objektif :

Memahami dan mematuhi keperluan keselamatan dalam mencapai maklumat.

K07/01 Kawalan Capaian

	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: - Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; - Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; - Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan - Kawalan ke atas kemudahan pemprosesan maklumat.	Unit ICT, ICTSO
--	---	--------------------

K07/02 Pengurusan Capaian Pengguna

Objektif:

Mengawal capaian pengguna ke atas aset ICT CGSO.

K07/02/01 Akaun Pengguna

	Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi:	Pentadbir Sistem ICT, Pengguna
--	--	--------------------------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	55 dari 84

	(a) Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; (d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan CGSO. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut; - Pengguna yang bercuti panjang melebihi dua (2) minggu; - Bertukar bidang tugas kerja; - Bertukar ke agensi lain; - Bersara; atau - Ditamatkan perkhidmatan	
--	---	--

K07/02/02 Hak Capaian

	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
--	---	----------------------

K07/02/03 Pengurusan Kata Laluan

	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh CGSO seperti berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah	Pengguna dan Pentadbir Sistem ICT
--	--	-----------------------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	56 dari 84

	dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; (d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; (e) Kata laluan <i>windows</i> dan <i>screen saver</i> hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama; (f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; (g) Kuatkuasakan pertukaran kata laluan semasa <i>login</i> kali pertama atau selepas <i>login</i> kali pertama atau selepas kata laluan diset semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; dan (i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan. (j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan (k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
K07/02/04 Clear Desk dan Clear Screen		
	Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Clear Desk dan Clear Screen bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.	Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	57 dari 84

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan password screen saver atau logout apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimile dan mesin fotostat.	
--	---	--

K07/03 Kawalan Capaian Rangkaian

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

K07/03/01 Capaian Rangkaian

	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian CGSO, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Sistem ICT dan ICTSO
--	--	---------------------------------------

K07/03/02 Capaian Internet

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di CGSO hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan <i>malicious code</i> dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian CGSO. (b) Penggunaan Internet hanyalah untuk kegunaan rasmi	Semua
--	--	--------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	58 dari 84

	sahaja. CIO berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya. (c) Kaedah <i>Content Filtering</i> mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan. (d) Penggunaan teknologi (<i>packet shaper</i>) untuk mengawal aktiviti (video conferencing, <i>video streaming</i>, <i>chat</i>, <i>downloading</i>) adalah perlu bagi menguruskan penggunaan <i>bandwidth</i> yang maksimum dan lebih berkesan. (e) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; (f) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh KetuaPengarah/ pegawai yang diberi kuasa; (g) Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; (h) Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Pengarah Bahagian sebelum dimuat naik ke Internet; (i) Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; (j) Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh CGSO; (k) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti newsgroup dan buletin board. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; (l) Penggunaan modem untuk tujuan sambungan ke Internet	
--	--	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	59 dari 84

	tidak dibenarkan sama sekali; dan (m) Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	
--	--	--

K07/04 Kawalan Capaian Sistem Pengoperasian

Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.

K07/04/01 Capaian Sistem Pengoperasian

	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian kepada sistem komputer. Kemudahan ini juga perlu bagi: (a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan (b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (a) Mengesahkan pengguna yang dibenarkan selaras dengan peraturan jabatan; (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian; dan (c) Menjana amaran (<i>alert</i>) sekiranya berlaku pelanggaran ke	Pentadbir Sistem dan ICTSO
--	---	-----------------------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	60 dari 84

	atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi termasuk berikut: a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur log on yang terjamin; b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; c) Mengehadkan dan mengawal penggunaan program; dan d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
--	---	--

K07/04/02 Kad Pintar

	(a) Penggunaan kad pintar kerajaan elektronik (Kad EG) hendaklah digunakan bagi capaian sistem kerajaan elektronik yang dikhususkan. Proses permohonan kad pintar hendaklah dibuat melalui Bahagian Khidmat Pengurusan; (b) Kad pintar hendaklah disimpan ditempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (c) Pengkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan (d) Sebarang kehilangan, kerosakan dan kata laluan disekat terhadap kad pintar perlu dimaklumkan kepada pihak Bahagian Khidmat Pengurusan.	
--	--	--

K07/05 KawalanCapaian Aplikasi dan Maklumat
Objektif:

Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.

	Bertujuan melindungi sistem maklumat dan aplikasi sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang	Pentadbir
--	---	-----------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	61 dari 84

	boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log) bagi mengesan aktiviti-aktiviti yang tidak diingini; (c) Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; (d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan (e) Capaian sistem maklumat dan aplikasi melalui jarak jauh amat digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Sistem dan ICTSO
--	---	------------------

K07/06 Peralatan Mudah Alih dan Kerja Jarak Jauh
Objektif:

Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh

K07/06/01 Peralatan Mudah Alih

	Kawalan peralatan mudah alih hendaklah mengikut peraturan-peraturan yang telah digariskan di dalam Langkah-Langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba dan Peranti Mudah Alih Sektor Awam i 5 Jun 2012.	Semua
--	---	-------

K07/06/02 Kerja Jarak Jauh

	Perkara yang perlu dipatuhi adalah seperti berikut: Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua
--	---	-------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	62 dari 84

KAWALAN 08
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

K08/01 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif :

Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

K08/01/01 Keperluan Keselamatan Sistem Maklumat

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; (c) Aplikasi perlu mengandungi semakan pengesahan (validation) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (d) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	ICTSO, Pentadbir Sistem ICT, Pengurus ICT
--	---	--

K08/01/02 Pengesahan Data Input dan Output

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pentadbir
--	---	-----------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	63 dari 84

	(a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan (b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Sistem ICT
--	--	------------

K08/02 Kawalan Kriptografi
Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

K08/02/01 Enkripsi

	Pengguna hendaklah membuat enkripsi (<i>encryption</i>) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Pengguna
--	--	----------

K08/02/02 Tandatangan Digital

	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pengguna
--	---	----------

K08/03/03 Pengurusan Infrastruktur Kunci Awam (PKI)

	Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pengguna
--	--	----------

K08/03 Keselamatan Fail Sistem
Objektif:

Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji;	Pentadbir Sistem ICT
--	---	-------------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	64 dari 84

	(c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan (e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	
--	---	--

K08/04 Pembangunan dan Sokongan Sistem

Objektif:

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

K08/04/01 Prosedur Kawalan Perubahan

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi; (c) Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; (d) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (e) Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan (f) Menghalang sebarang peluang untuk membocorkan maklumat.	Pengurus ICT, Pentadbir Sistem ICT
--	--	---

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	65 dari 84

K08/04/02 Pembangunan Secara <i>Outsource</i>		
	Pembangunan perisian aplikasi secara <i>outsource</i> perlu dipantau oleh Unit Teknologi Maklumat CGSO Kod sumber (<i>Source code</i>) adalah menjadi hak milik CGSO sebelum penyerahan kod sumber ini perlu melalui proses pemindahan teknologi (<i>Transfer of Technology</i>).	Pengurus ICT, Pentadbir Sistem ICT
K08/05 Kawalan Teknikal Keterdedahan (Vulnerability)		
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.		
K08/05/01 Kawalan dari Ancaman Teknikal		
	Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	66 dari 84

KAWALAN 09
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

K09/01 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan dan memastikan sistem ICT CGSO dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej CGSO dan sistem penyampaian perkhidmatan.

K09/01 Mekanisme Pelaporan

	Insiden keselamatan ICT bermaksud musibah (adverse event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dengan kadar segera: (a) Maklumat didapati hilang, didedahkan kepada pihak ketiga atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisma kawalan akses, hilang, dicuri atau didedahkan, disyaki hilang atau dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan mencerooboh, penyelewengan dan insiden-insiden yang tidak diingini.	Semua
--	--	-------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	67 dari 84

	Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di CGSO sepertimana Lampiran 2. Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 i PengurusanPengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
--	---	--

K09/02 Pengurusan Maklumat Insiden Keselamatan ICT
Objektif:

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

	Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada CGSO. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;	ICTSO
--	--	-------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	68 dari 84

	(c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	
--	--	--

KAWALAN 10

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

K10/01 Dasar Kesenambungan Perkhidmatan

Objektif :

Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.

K10/01/01 Pelan Kesenambungan Perkhidmatan

	Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JKICT CGSO dan perkara-perkara berikut perlu diberi perhatian: (a) Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (c) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (d) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (e) Membuat <i>backup</i>; dan (f) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. (g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	Pengurus ICT
--	---	-------------------------

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	70 dari 84

	Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel CGSO dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. CGSO hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	
--	---	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	71 dari 84

KAWALAN 11

PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak daripada pelanggaran kepada Dasar Keselamatan ICT CGSO.

K11/01/01 Pematuhan Dasar

	Setiap pengguna di CGSO hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT CGSO dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua aset ICT di CGSO termasuk maklumat yang disimpan di dalamnya ada lah hak milik Kerajaan dan Ketua Pengarah Keselamatan Kerajaan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain daripada tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT CGSO selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber CGSO.	Semua
--	---	-------

K11/02 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

	ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
--	--	-------

K11/03 Pematuhan Keperluan Audit

	Pematuhan kepada keperluan audit perlu bagi meminimumkan	
--	--	--

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	72 dari 84

	ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua
K11/04 Keperluan Perundangan		
	Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di CGSO adalah seperti di Lampiran 3.	Semua
K11/05 Pelanggaran Dasar		
	Pelanggaran Dasar Keselamatan ICT CGSO boleh dikenakan tindakan tatatertib di bawah Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib 1993) atau didakwa di bawah Akta Rahsia Rasmi 1972 dan akta-akta berkaitan yang berkuatkuasa.	Semua

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	73 dari 84

GLOSARI	
<i>Antivirus</i>	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, <i>optical disk</i> , <i>flash disk</i> , CDROM untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasa, perisian, perkhidmatan, data atau maklumat dan manusia.
<i>Backup</i>	Proses penduaan sesuatu dokumen atau maklumat.
<i>Bandwidth</i>	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CGSO CERT	Organisasi yang ditubuhkan untuk membantu CGSO mengurus pengendalian insiden keselamatan ICT
CIO	<i>Chief Information Officer</i> Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan s maklumat bagi menyokong arah tuju sesebuah organisasi.
Content Filtering	Satu teknik yang menyekat atau membenarkan berdasarkan analisis kepada kandungan dan bukannya berdasarkan sumber atau kriteria. Ia digunakan secara meluas untuk capaian internet dan email.
<i>Denial of service</i>	Halangan pemberian perkhidmatan.
<i>Downloading</i>	Aktiviti muat-turun sesuatu perisian.
<i>Encryption</i>	Enkripsi atau penyulitan ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
<i>Firewall</i>	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
<i>Forgery</i>	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (<i>information theft / espionage</i>), penipuan(<i>hoaxes</i>).
GCERT	<i>Government Computer Emergency Response Team</i> atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	74 dari 84

<i>Hard disk</i>	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
<i>Hub</i>	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (<i>broadcast</i>) data yang diterima daripada sesuatu <i>port</i> kepada semua <i>port</i> yang lain.
ICT	<i>Information and Communication Technology</i> .(Teknologi Maklumat dan Komunikasi).
ICTSO	<i>ICT Security Officer</i> Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (<i>server</i>) atau komputer lain.
<i>Internet Gateway</i>	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
<i>Intrusion Detection System (IDS)</i>	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat <i>host</i> atau rangkaian.
<i>Intrusion Prevention System (IPS)</i>	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindakbalas menyekat atau menghalang aktiviti serangan atau <i>malicious code</i> . Contohnya: <i>Network-based IPS</i> yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	<i>Local Area Network</i> Rangkaian Kawasan Setempat yang menghubungkan komputer.
<i>Logout</i>	<i>Log-out</i> komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
<i>Malicious Code</i>	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	75 dari 84

	kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, <i>trojan horse</i> , <i>worm</i> , <i>spyware</i> dan sebagainya.
Media storan	Semua media storan dan peralatan yang berkaitan seperti disket, kartrij, CD-ROM, pita, cakera, pemacu cakera dan pemacu pita.
MODEM	Modulator DeModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
<i>Outsource</i>	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti <i>spreadsheet</i> dan <i>word processing</i> ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
<i>Public-Key Infrastructure (PKI)</i>	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perrkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
<i>Router</i>	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
<i>Screen saver</i>	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
<i>Server</i>	Pelayan komputer
<i>Switches</i>	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian Carrier Sense Multiple Access/Collision Detection (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
<i>Threat</i>	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
<i>Uninterruptible Power Supply (UPS)</i>	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan daripada sumber berlainan ketika ketiadaan bekalan kuasa ke

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	76 dari 84

	peralatan yang bersambung.
<i>Video Conference</i>	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
<i>Video Streaming</i>	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.
<i>Wireless LAN</i>	Jaringan komputer yang terhubung tanpa melalui kabel.

**SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT KERAJAAN**

Nama : é é é é é é é é é é é é é é é é é é é

No. Kad Pengenalan : é é é é é é é é é é é é é é é é é é é

Jawatan : é é é é é é é é é é é é é é é é é é é

Kementerian/Jabatan : é é é é é é é é é é é é é é é é é é é

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah mengikuti Taklimat Dasar Keselamatan ICT;
2. Saya juga telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT ; dan
3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....

(Tandatangan Pegawai)

Tarikh :

Pengesahan Pegawai Keselamatan ICT

.....

(Nama Pegawai Keselamatan ICT)

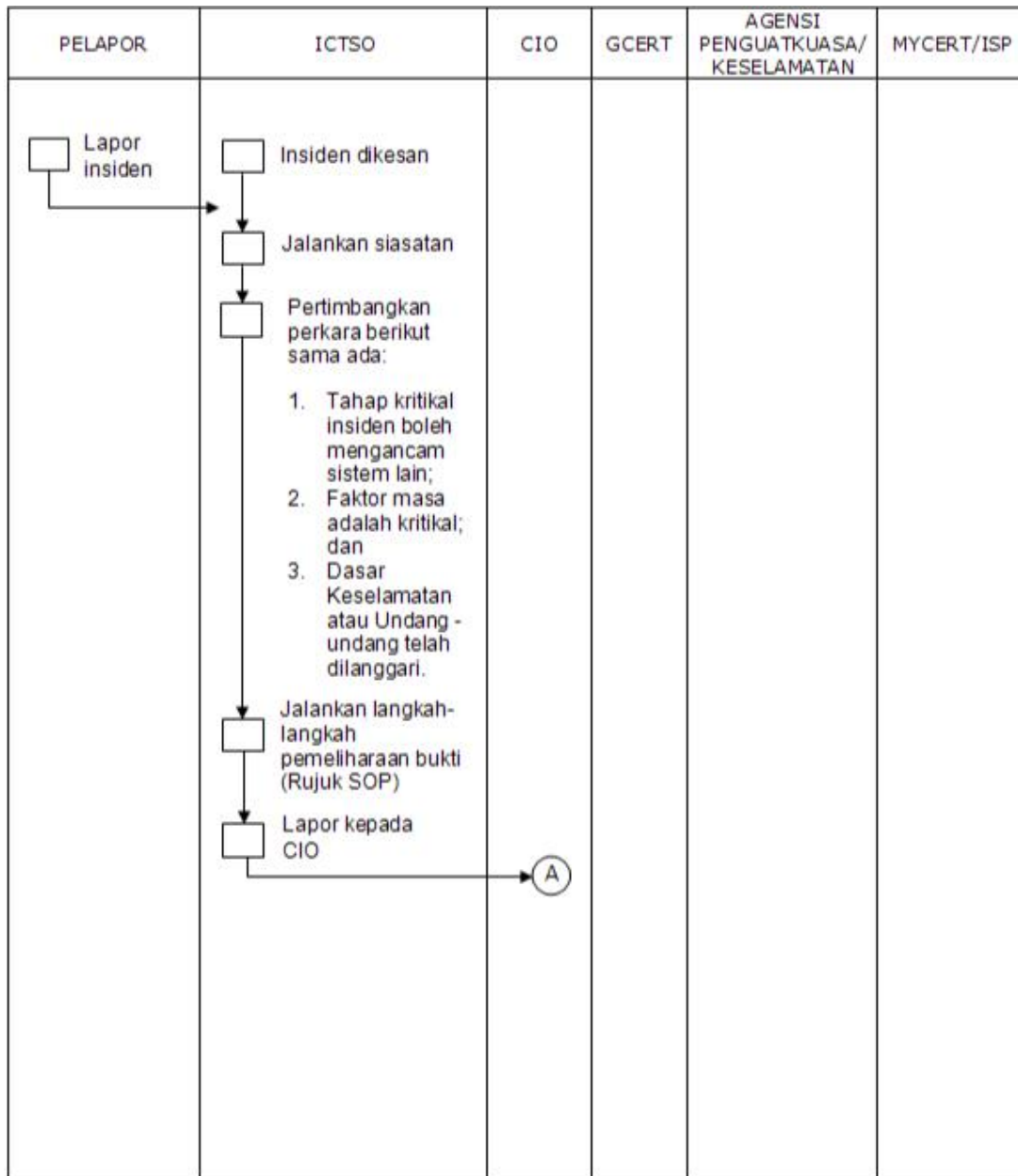
b.p Ketua Pengarah CGSO

Tarikh :

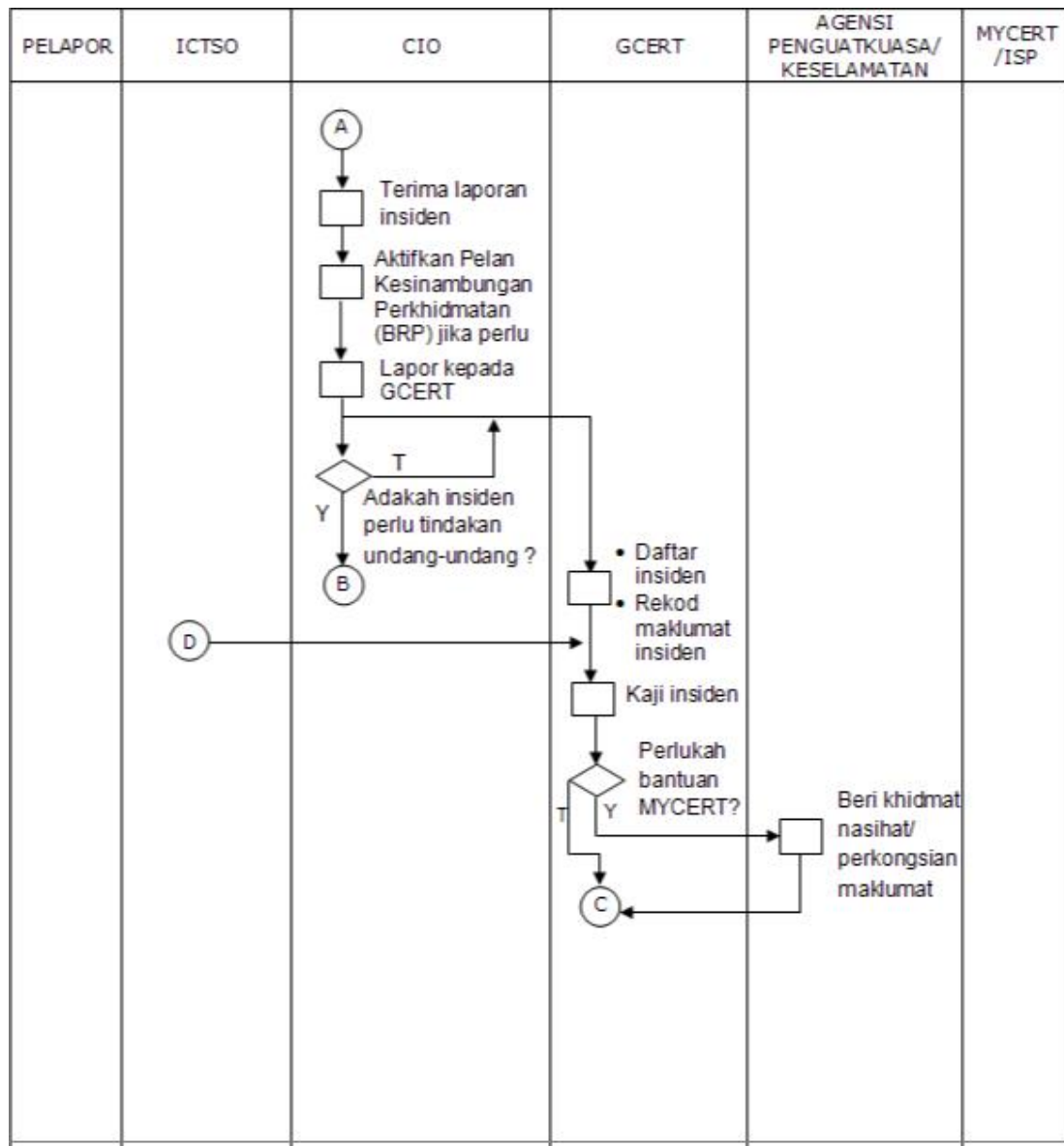
RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	78 dari 84

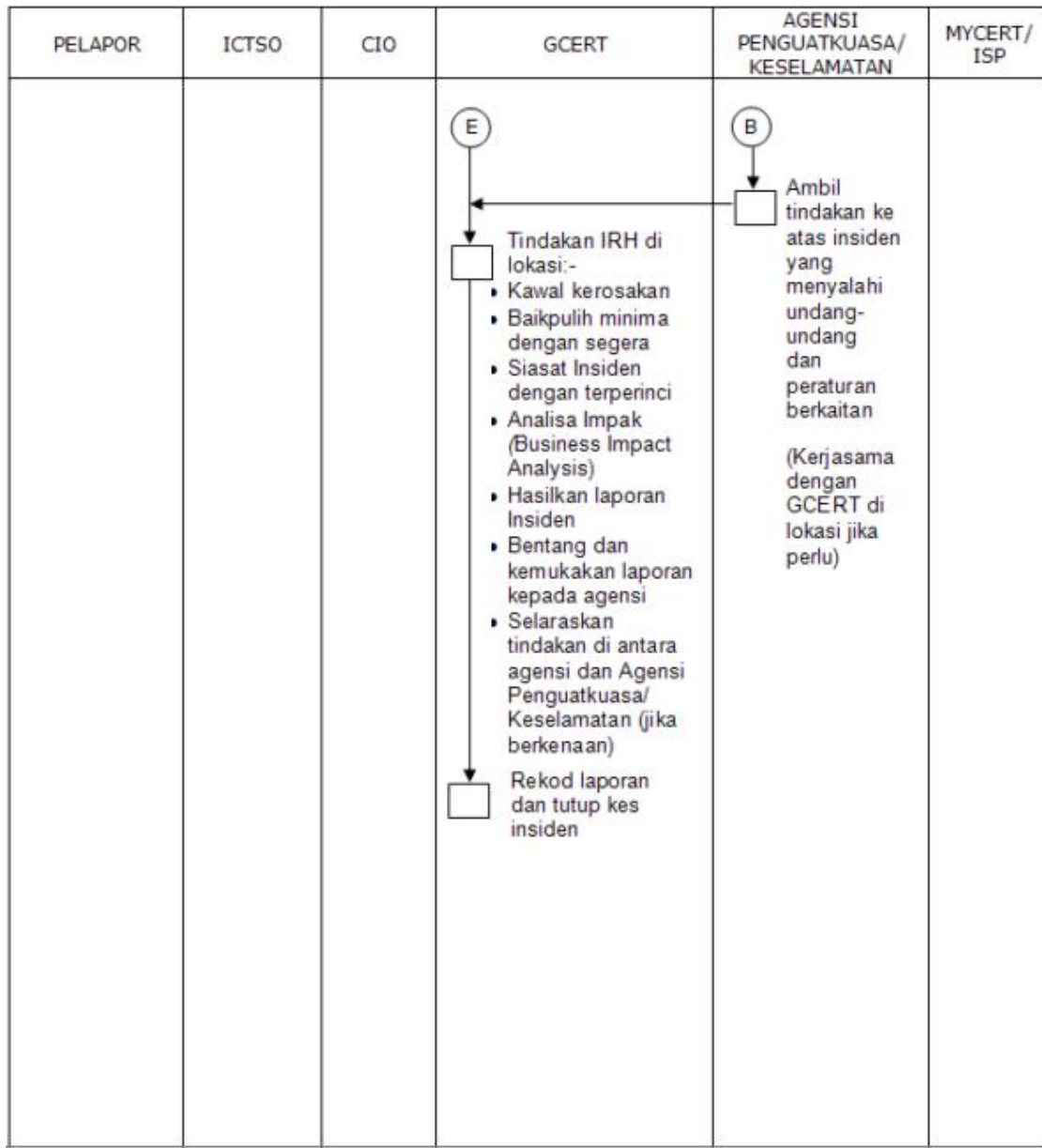
Lampiran 2

Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT CGSO



RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	79 dari 84





SENARAI PERUNDANGAN DAN PERATURAN

- i. Arahan Keselamatan;
- ii. Pekeliling Am Bilangan 3 Tahun 2000 Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
- iii. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002*;
- iv. Pekeliling Am Bilangan 1 Tahun 2001 Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
- v. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
- vi. Surat Pekeliling Am Bilangan 6 Tahun 2005 Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam;
- vii. Surat Pekeliling Am Bil. 4 Tahun 2006 Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;
- viii. Surat Arahan Ketua Setiausaha Negara Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan bertarikh 20 Oktober 2006;
- ix. Surat Arahan Ketua Pengarah MAMPU Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi Kerajaan yang bertarikh 1 Jun 2007;
- x. Surat Arahan Ketua Pengarah MAMPU Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
- xi. Surat Pekeliling Am Bil. 2 Tahun 2000 Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
- xii. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
- xiii. Surat Pekeliling Perbendaharaan Bil. 3/1995-Peraturan Perolehan Perkhidmatan Perundingan;
- xiv. Akta Tandatangan Digital 1997;
- xv. Akta Rahsia Rasmi 1972;

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	83 dari 84

- xvi. Akta Jenayah Komputer 1997;
- xvii. Akta Hak cipta (Pindaan) Tahun 1997;
- xviii. Akta Komunikasi dan Multimedia 1998;
- xix. Perintah-Perintah Am;
- xx. Arahan Perbendaharaan;
- xxi. Arahan Teknologi Maklumat;
- xxii. Surat Pekeliling Am Bilangan 3 Tahun 2009 Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
- xxiii. Surat Arahan Ketua Pengarah MAMPU Pengurusan Kesyinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
- xxiv. Garis Panduan Tatacara Pemilihan Kandungan Media Sosial MAMPU bertarikh 12 Oktober 2011;
- xxv. Surat Arahan Ketua Pengarah MAMPU : Amalan Terbaik Penggunaan Media Jaringan Sosial Bertarikh 8 April 2011;
- xxvi. Surat Arahan Ketua Pegawai Keselamatan Kerajaan Malaysia: Langkah-langkah Keselamatan Perlindungan Bagi Mencegah Kehilangan Komputer Riba dan Peranti Mudah Alih di Sektor Awam bertarikh 5 Jun 2012.

RUJUKAN	VERSI	TARIKH	M/SURAT
DKICT CGSO	Versi 2.1	30 Sept 2012	84 dari 84