DASAR KESELAMATAN ICT (DKICT) VERSI 3.0
PEJABAT KETUA PEGAWAI KESELAMATAN KERAJAAN MALAYSIA

CGSO
CHIEF GOVERNMENT SECURITY OFFICE

PERUTUSAN

KETUA PENGARAH KESELAMATAN KERAJAAN

PEJABAT KETUA PEGAWAI KESELAMATAN KERAJAAN MALAYSIA

Salam Sejahtera dan Salam Kegemilangan,

Pertama sekali saya ingin mengucapkan syabas dan tahniah kepada Bahagian Keselamatan ICT dan Rahsia Rasmi, Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia yang telah selesai menghasilkan Dasar Keselamatan ICT (DKICT) versi 3.0 iaitu penambahbaikan daripada versi sebelum ini. Penghasilan DKICT versi 3.0 ini merupakan kesinambungan garis panduan kepada semua warga Pejabat CGSO mengenai pengurusan keselamatan ke atas aset ICT Jabatan seperti data, peralatan, rangkaian dan perkhidmatan.

Kemajuan teknologi ICT yang begitu pesat berkembang memberikan kesan kepada sistem penyampaian perkhidmatan Kerajaan. Soal keselamatan ICT terutamanya berkaitan data dan maklumat memerlukan mekanisme pengurusan yang sistematik dan teratur. DKICT ini disediakan sebagai garis panduan memberi penjelasan terperinci mengenai tatacara tadbir urus ICT dan peraturan yang perlu dipatuhi oleh semua warga Jabatan dalam melaksanakan tugas dan tanggungjawab harian.

Saya berharap dengan adanya DKICT ini maka semua pengguna Jabatan akan sentiasa merujuk kepada peraturan keselamatan ICT yang telah digariskan bagi memastikan sebarang insiden keselamatan ICT dapat diminimakan.

Akhir kata, setinggi-tinggi penghargaan dan ucapan tahniah atas kerjasama daripada ahli- ahli Jawatankuasa Kerja dan urus setia DKICT, pihak-pihak tertentu serta orang perseorangan yang terlibat sama ada secara langsung atau tidak langsung dalam memberikan kerjasama dan pandangan ke arah penambahbaikan DKICT versi 3.0 ini.

Sekian, terima kasih.

RAHIMI BIN ISMAIL

SEJARAH DOKUMEN

TARIKH	NO. SEMAKAN	KELULUSAN
25 Februari 2009	Versi 2.0	JPICT CGSO BIL 1/2009
30 September 2012	Versi 2.1	Mesyuarat Khas DKICT
6 Januari 2022	Versi 3.0	JKICT CGSO Bil. 1 Tahun 2022

JADUAL PINDAAN

TARIKH	VERSI	BUTIRAN TAMBAHAN DAN PINDAAN
2022	3.0	1. Pindaan bagi memenuhi keperluan standard **ISO/IEC 27001:2013** ***Information Security Management System*** **(ISMS)** 2. **Tambahan 3 bidang** 3. Tambahan sub bidang bagi **4-3-4 Media Mudah Alih Persendirian (*Bring Your Own Device*)** 4. Tambahan sub bidang bagi **5-1-3 Pengkomputeran Awan (*Cloud Computing*)**

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang MESTI DIBACA dan DIPATUHI dalam menggunakan aset ICT. Dasar ini juga menerangkan kepada semua pengguna di Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT CGSO.

OBJEKTIF

Dasar Keselamatan ICT CGSO diwujudkan bertujuan untuk:

i. Menerangkan kepada semua pengguna merangkumi warga CGSO, pembekal/vendor dan pihak yang mempunyai urusan dengan perkhidmatan ICT CGSO mengenai tanggungjawab dan peranan mereka dalam melindungi maklumat diruang siber;

ii. Menjamin kesinambungan urusan perkhidmatan CGSO dengan meminimumkan kesan insiden keselamatan ICT;

iii. Memudahkan perkongsian maklumat bersesuaian dengan operasi jabatan;

iv. Melindungi kepentingan pihak-pihak yang bergantung pada sistem maklumat dari kesan kegagalan atau kelemahan yang berlaku dari segi kerahsiaan, integriti, ketersediaan kebolehsediaan, kesahihan maklumat dan komunikasi; dan

v. Mencegah salah guna atau kecurian aset ICT Kerajaan.

PERNYATAAN DASAR

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

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

i. Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan dari capaian tanpa kuasa yang sah;
ii. Menjamin setiap maklumat adalah tepat dan sempurna;
iii. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
iv. Memastikan akses kepada hanya pengguna-pengguna yang sah atau menerima maklumat dari sumber yang sah.

Dasar Keselamatan ICT CGSO sehingga kini mempunyai versi seperti berikut:

TARIKH	NO. SEMAKAN	KELULUSAN	TARIKH KUAT KUASA
25 Februari 2009	Versi 2.0	JPICT CGSO BIL 1/2009	25 Februari 2009
30 September 2012	Versi 2.1	Mesyuarat Khas DKICT	30 September 2012
6 Januari 2022	Versi 3.0	JKICT CGSO Bil. 1/ 2022	6 Januari 2022

Penambahbaikan versi ini selaras dengan penambahbaikan Standard Antarabangsa iaitu ***Information Security Management System (ISMS)*** **ISO/IEC 27001**. Ia juga dibentangkan kepada Pihak Pengurusan Tertinggi CGSO melalui Mesyuarat Jawatankuasa Keselamatan ICT (JKICT) CGSO.

Ia merangkumi perlindungan ke atas semua bentuk maklumat digital dan keselamatan fizikal yang bertujuan untuk menjamin keselamatan maklumat tersebut dan ketersediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

i. Kerahsiaan – Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan di akses tanpa kebenaran;
ii. Integriti – Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;
iii. Tidak Boleh Disangkal – Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;
iv. Kesahihan – Data dan maklumat hendaklah dijamin kesahihannya; dan
v. Ketersediaan – Data dan maklumat hendaklah boleh di akses pada bila-bila masa.

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

SKOP

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

i. Data dan maklumat hendaklah boleh di akses secara berterusan dengan cepat, tepat, mudah dan boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti; dan
ii. Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan

ketepatan maklumat serta untuk melindungi kepentingan Kerajaan, perkhidmatan dan masyarakat.

Bagi menentukan aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT CGSO ini merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, di akses, diedarkan, dalam penghantaran dan yang dibuat salinan keselamatan. Ini dilakukan melalui perwujudan dan penguatkuasaan sistem kawalan dan prosedur pengendalian semua perkara-perkara berikut:

i. **Perkakasan**

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan CGSO. (Contohnya: komputer, server, peralatan komunikasi dan sebagainya).

ii. **Perisian**

Program, prosedur atau peraturan yang ditulis dan didokumentasikan yang mana berkaitan dengan sistem operasi komputer yang mana disimpan di dalam sistem ICT. (Contohnya: perisian aplikasi, perisian sistem, operating system, sistem pangkalan data, perisian sistem rangkaian atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat).

iii. **Perkhidmatan**

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi- fungsinya. (Contohnya: perkhidmatan rangkaian, sistem akses dan sebagainya).

iv. **Data atau Maklumat**

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif CGSO. (Contohnya: Sistem dokumentasi, prosedur operasi, rekod-

rekod, profil pelanggan, pangkalan data dan fail-fail data, maklumat arkib dan lain-lain).

v. Manusia

Individu yang mempunyai pengetahuan dan kemahiran dalam melaksanakan skop kerja harian CGSO bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-tugas dan fungsi yang dilaksanakan.

vi. Premis Komputer dan Komunikasi

Semua kemudahan serta premis yang digunakan untuk menempatkan perkara-perkara (i) – (vi) di atas. Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai pelanggaran langkah-langkah kawalan keselamatan.

PRINSIP-PRINSIP

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

i. Akses Atas Dasar Perlu Mengetahui

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

ii. Hak Akses Minimum

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

semasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas.

iii. Akauntabiliti

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

a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
b. Memeriksa maklumat dan menentukan ianya 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.

iv. Pengasingan

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

v. Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, router, firewall dan peralatan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau audit trail;

vi. Pematuhan

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

vii. Pemulihan

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

viii. Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

CGSO hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari 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 ke pihak lain seperti pembekal, pakar runding dan pihak lain yang berkepentingan.

BIDANG 1 PEMBANGUNAN DAN PENYELARASAN DASAR

1-1 DASAR KESELAMATAN ICT CGSO

Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan CGSO dan perundangan yang berkaitan.

1-1-1 Pelaksanaan Dasar	
Pengarah CGSO adalah bertanggungjawab ke atas pelaksanaan arahan dengan dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik.	Pihak Pengurusan Tertinggi CGSO
1-1-2 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna CGSO termasuk pembekal, pakar runding dan lain-lain yang berurusan dengan CGSO semua pengguna merangkumi warga CGSO, pembekal/vendor dan pihak yang mempunyai urusan dengan perkhidmatan ICT CGSO.	Pihak Pengurusan Tertinggi Bahagian CGSO/ Jabatan Pengarah CGSO Negeri/ Fasiliti / Institusi CGSO
1-1-3 Penyelenggaraan Dasar	
Dasar Keselamatan ICT CGSO adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT CGSO: a) Mengkaji semula dasar ini sekurang-kurangnya tiga (3) tahun sekali atau mengikut keperluan bagi mengenal pasti dan menentukan perubahan yang diperlukan; b) Mengemukakan cadangan perubahan kepada CIO	ICTSO

untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Keselamatan ICT (JKICT) CGSO; dan c) Memaklumkan perubahan dasar yang telah dipersetujui oleh JKICT kepada semua pengguna CGSO.	
1-1-4 Pengecualian Dasar	
DKICT CGSO ini hendaklah dibaca, difahami dan dipatuhi oleh semua warga pengguna merangkumi warga CGSO, pembekal/vendor dan pihak yang mempunyai urusan dengan perkhidmatan ICT CGSO serta tiada pengecualian diberikan. Dasar Keselamatan ICT CGSO adalah terpakai kepada semua pengguna ICT CGSO dan tiada pengecualian diberikan.	Semua

BIDANG 2 ORGANISASI KESELAMATAN

2-1 ORGANISASI DALAMAN	
Objektif: Mewujudkan pengurusan organisasi keselamatan untuk melaksana serta mengawal pelaksanaan dan operasi keselamatan maklumat dalam organisasi.	
2-1-1 Peranan Dan Tanggungjawab Organisasi Keselamatan Maklumat	
Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut: a) Memastikan semua pengguna memahami dan mematuhi Dasar Keselamatan ICT CGSO; b) Memastikan pengguna mematuhi DKICT CGSO; c) Memastikan semua keperluan organisasi	Ketua Pengarah

seperti sumber kewangan, kakitangan dan perlindungan keselamatan adalah mencukupi; d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT CGSO; dan e) Mempengerusikan Jawatankuasa Keselamatan ICT (JKICT), CGSO	
Ketua Pegawai Maklumat (CIO) CGSO adalah disandang oleh Timbalan Ketua Pengarah (Dasar). Peranan dan tanggungjawab Ketua Pegawai Maklumat (CIO) adalah seperti berikut: a) Menasihati Ketua Pengarah dan Pengarah Negeri dalam melaksanakan tugas- tugas yang melibatkan keselamatan ICT; b) Menentukan keperluan keselamatan ICT; c) Menyelaras pembangunan dan pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT CGSO.	CIO
Pegawai Keselamatan ICT (ICTSO) CGSO adalah disandang oleh Pengarah Bahagian Keselamatan ICT dan Rahsia Rasmi (BKICTRR). Peranan dan tanggungjawab Pegawai Keselamatan ICT (ICTSO) CGSO yang dilantik adalah seperti berikut: a) Mengurus keseluruhan program-program keselamatan ICT CGSO;	ICTSO

b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT CGSO; c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT CGSO kepada semua pengguna; d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT CGSO; e) Menjalankan pengurusan risiko; f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h) Melaporkan insiden keselamatan ICT kepada Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara dan memaklumkan kepada CIO; i) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan j) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	

Pengurus ICT CGSO adalah disandang oleh Ketua Seksyen Teknologi Maklumat CGSO. Peranan dan tanggungjawab Pengurus ICT yang dilantik adalah seperti berikut: a) Melaksanakan kawalan keselamatan ICT selaras dengan keperluan CGSO; b) Memberi penerangan dan pendedahan berkenaan DKICT CGSO kepada semua pengguna; c) Menjalankan pengurusan risiko; d) Menjalankan audit dalaman, mengkaji semula, merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; e) Melaporkan insiden keselamatan ICT kepada CERT CGSO; f) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; g) Memantau pematuhan DKICT CGSO; h) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan i) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan dan pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baharu dapat dielakkan.	Pengurus ICT

Penyelaras ICT Fasiliti adalah disandang oleh Pegawai/Penolong Pegawai Teknologi Maklumat di Seksyen Teknologi Maklumat CGSO. Peranan dan tanggungjawab Penyelaras ICT Fasiliti adalah seperti berikut: a) Melaksanakan kawalan keselamatan ICT selaras dengan keperluan CGSO; b) Melaksanakan kawalan akses semua pengguna terhadap aset ICT di fasiliti; 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.	Penyelaras ICT Fasiliti
Pentadbir Sistem ICT adalah disandang oleh Pegawai/Penolong Pegawai Teknologi Maklumat di Seksyen Teknologi Maklumat CGSO. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a) Memastikan kerahsiaan kata laluan aset ICT; b) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; c) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek;	Pentadbir Sistem ICT

d) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT CGSO; e) Memantau aktiviti capaian harian sistem aplikasi pengguna; f) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; g) Menyimpan dan menganalisis rekod audit trail; h) Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; i) Bertanggungjawab memantau setiap peralatan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; dan j) Bertanggungjawab memastikan setiap perolehan perisian ICT adalah tulen.	
Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT CGSO; b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;	Pengguna

c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rahsia rasmi; d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat CGSO; e) Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan mengesahkan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberi perhatian kepada maklumat rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada	

ICTSO dengan segera; g) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan h) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT CGSO.	
Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain). Ini bertujuan untuk memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi adalah seperti 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 ketiga. Perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai: i. Dasar Keselamatan ICT CGSO; ii. Tapisan Keselamatan;	CIO, ICTSO CGSO, Pengurus ICT, Penyelaras ICT Fasiliti, Pentadbir Sistem ICT dan Pihak Ketiga

iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. v. Mematuhi kehendak undang-undang lain yang sedang berkuat kuasa.	
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 Bahagian Keselamatan ICT dan Rahsia Rasmi. **Bidang kuasa:** a) Memperakukan/meluluskan dokumen DKICT CGSO; b) Memantau tahap pematuhan keselamatan ICT; c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi khusus dalam CGSO	JKICT 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.	
Keanggotaan Pasukan Tindak Balas Insiden Keselamatan ICT (CERT) CGSO adalah seperti berikut: **Pengerusi:** ICTSO CGSO **Ahli :** 1. Pegawai Teknologi Maklumat di Seksyen Teknologi Maklumat, STM BKP 2. Pegawai Teknologi Maklumat di Seksyen Pengurusan Keselamatan ICT, BKICTRR 3. Timbalan Pengarah Seksyen Pengurusan Keselamatan ICT, BKICTRR 4. Penolong Pegawai Teknologi Maklumat Kanan di Seksyen Teknologi Maklumat 5. Penolong Pegawai Keselamatan	CERT CGSO

Kerajaan di Seksyen Pengurusan Keselamatan ICT, BKICTRR **Urusetia:** Seksyen Teknologi Maklumat, BKP Peranan dan tanggungjawab CERT CGSO adalah seperti berikut: a) Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; b) Merekodkan dan menjalankan siasatan awal insiden yang diterima; c) Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d) Menasihati ICTSO CGSO mengambil tindakan pemulihan dan pengukuhan; e) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada CGSO; dan f) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
2-1-2 Pengasingan Peranan Dan Tanggungjawab	
Peranan dan tanggungjawab dalam bidang tugas hendaklah diasingkan untuk mengurangkan peluang bagi pengubahsuaian atau penyalahgunaan yang tidak dibenarkan ke atas aset organisasi. Perkara yang perlu dipatuhi	CIO, ICTSO, Pengurus ICT, Penyelaras ICT Fasiliti dan Pentadbir Sistem

adalah seperti berikut: a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian; b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat rahsia rasmi atau dimanipulasikan; dan c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai produksi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	
2-1-3 Senarai Perhubungan Dengan Pihak Berkuasa	
CGSO hendaklah memastikan senarai perhubungan dengan pelbagai pihak yang berkaitan diwujudkan dan dikemas kini. Ia merupakan sumber rujukan pengguna CGSO mengetahui senarai perhubungan pihak berkuasa yang berdekatan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Menyediakan senarai perhubungan pihak berkuasa dan sentiasa mengemas kini senarai tersebut; dan b) Memastikan senarai perhubungan pihak berkuasa diedarkan kepada semua pengguna atau pengguna yang berkaitan.	Semua pengguna

BIDANG 3 KESELAMATAN SUMBER MANUSIA

3-1 KESELAMATAN SUMBER MANUSIA SEBELUM PERKHIDMATAN

Objektif:

Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan CGSO, pihak ketiga (Pembekal, Pakar Runding dan lain-lain) memahami tanggungjawab dan peranan masing-masing. Mereka hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

3-1-1 Tapisan

CGSO hendaklah memastikan pegawai, kakitangan dan pihak ketiga melaksanakan tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	CIO, ICTSO CGSO, Pengurus ICT, Penyelaras ICT Fasiliti

3-1-2 Terma Dan Syarat Pelantikan

Memastikan pegawai, kakitangan CGSO dan pihak ketiga memahami tanggungjawab masing-masing ke atas keselamatan ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT Kerajaan. Perkara yang mesti dipatuhi termasuk yang berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan CGSO dan pihak ketiga ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan saringan dan pengesahan latar belakang calon untuk pegawai dan kakitangan CGSO serta pihak ketiga hendaklah dilakukan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan c) Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Semua Pengguna/ Pihak Ketiga

3-2 KESELAMATAN SUMBER MANUSIA DALAM PERKHIDMATAN

Objektif:

Memastikan pegawai, kakitangan dan pihak ketiga mengetahui tanggungjawab keselamatan maklumat.

3-2-1 Tanggungjawab Pihak Pengurusan	
Perkara yang perlu dipatuhi adalah seperti berikut: d) ICTSO hendaklah memastikan semua pengguna CGSO mematuhi DKICT CGSO; dan e) Memastikan pengguna CGSO mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh CGSO.	CIO, ICTSO CGSO, Pengurus ICT, Penyelaras ICT Fasiliti
3-2-2 Pembudayaan, Latihan Dan Sesi Kesedaran Keselamatan Maklumat	
CGSO perlu melaksanakan perkara seperti berikut: a) Melaksanakan sesi kesedaran dan pendidikan berkaitan dengan pengurusan keselamatan ICT kepada pengguna CGSO secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka; b) CGSO perlu menyediakan sesi kesedaran, latihan atau pendidikan keselamatan ICT sekurang-kurangnya sekali setahun; dan c) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul bagi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Khidmat Pengurusan.	CIO, ICTSO CGSO, Pengurus ICT, Penyelaras ICT Fasiliti
3-2-3 Tindakan Tatatertib	
CGSO boleh mengambil tindakan perundangan atau tatatertib ke atas pengguna CGSO sekiranya berlaku pelanggaran ke atas dasar-dasar Kerajaan, peraturan, serta undang-undang semasa yang masih berkuat kuasa berhubung dengan	CIO, ICTSO CGSO, Pengurus ICT, Penyelaras

Keselamatan ICT.	ICT Fasiliti, Pengguna

3-3 PENAMATAN ATAU PERUBAHAN PERKHIDMATAN

Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua aset ICT yang dikembalikan kepada CGSO mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh CGSO dan/atau terma perkhidmatan; dan c) Menguruskan urusan keluar, berhenti, pertukaran peranan dan tanggungjawab pengguna CGSO.	Semua pihak berkenaan

BIDANG 4 PENGURUSAN ASET

4-1 AKAUNTABILITI ASET

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT CGSO sentiasa di dalam keadaan baik dan selamat.

4-1-1 Inventori Aset ICT

Ini bertujuan untuk memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh setiap pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a) Merekod dan mengemas kini maklumat aset menggunakan borang daftar harta modal dan inventori; dan b) Setiap aset ICT hendaklah mempunyai maklumat berikut:	Semua pengguna

i. Pemilik yang sah; dan ii. Rekod penempatan yang betul.	
4-1-2 Hak Milik Aset ICT	
CGSO perlu memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja.	Semua pengguna
4-1-3 Penggunaan Aset ICT	
Perkara berikut perlu dipatuhi dalam penggunaan aset ICT: a) CGSO perlu memastikan penggunaan aset ICT dan kemudahan pemprosesan maklumat dikenal pasti, di dokumentasi dan dilaksanakan. Setiap pengguna bertanggungjawab terhadap penggunaan semua aset ICT di bawah tanggungjawabnya; dan b) Pengendalian aset ICT hendaklah merujuk peraturan atau pekeliling semasa yang masih berkuat kuasa.	Semua pengguna
4-1-4 Pemulangan Aset ICT	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Pengguna bertanggungjawab untuk mengembalikan aset ICT setelah bertukar keluar atau meninggalkan perkhidmatan; dan b) Semua pengguna hendaklah memulangkan semua aset ICT kepada Pegawai Aset atau pegawai bertanggungjawab selepas penamatan pekerjaan, kontrak atau perjanjian.	Pentadbir Sistem dan semua pengguna
4-2 PENGELASAN DAN PENGENDALIAN MAKLUMAT	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	

4-2-1 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan (Semakan dan Pindaan 2017). Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan (Semakan dan Pindaan 2017) yang sedang berkuat kuasa seperti berikut: a) Rahsia Besar; b) Rahsia; c) Sulit; dan d) Terhad. Selain daripada maklumat rahsia rasmi adalah dikelaskan sebagai terbuka.	Semua pengguna
4-2-2 Penandaan Maklumat	
Maklumat hendaklah ditanda dan dikendali berasaskan peringkat keselamatan yang dikenal pasti selaras dengan peraturan prosedur yang ditetapkan Arahan Keselamatan (Semakan dan Pindaan 2017).	Semua pengguna
4-2-3 Pengendalian Aset Atau Maklumat	
Aktiviti pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengambil kira langkah- langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa, menyemak maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c) Memastikan menentukan maklumat sedia untuk digunakan;	Semua pengguna

d) Menjaga kerahsiaan kata laluan; e) Mematuhi piawaian, prosedur, tatacara dan garis panduan keselamatan yang dikeluarkan dari semasa ke semasa; f) Memberi perhatian kepada pengendalian maklumat rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g) Menjaga kerahsiaan langkah-langkah pengurusan pengendalian maklumat rahsia rasmi dari diketahui umum.	

4-3 PENGURUSAN MEDIA MUDAH ALIH

Objektif:

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

4-3-1 Pengurusan Media Mudah Alih (*Removable Media*)

Media mudah alih merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat dan media storan yang boleh alih. Peraturan yang perlu dipatuhi dalam pengurusan media mudah alih adalah berdasarkan Arahan Keselamatan (Semakan dan Pindaan 2017) dan seperti berikut: a) Media mudah alih hendaklah disimpan di bekas penyimpanan yang selamat dan dibenarkan; b) Akses untuk memasuki kawasan penyimpanan media mudah alih hendaklah terhad kepada Pentadbir dan pegawai yang dibenarkan sahaja; c) Media mudah alih perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; d) Media mudah alih yang mengandungi data rahsia rasmi	Semua pengguna

hendaklah disimpan di dalam bekas keselamatan yang mempunyai ciri-ciri keselamatan; e) Akses dan pergerakan media mudah alih hendaklah direkodkan; f) Peralatan *backup* bagi media mudah alih hendaklah diletakkan di tempat yang terkawal; g) Mengadakan salinan atau pendua pada media mudah alih bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; dan h) Hanya maklumat rasmi dibenarkan untuk disimpan dalam media mudah alih yang dibekalkan oleh Jabatan.	
4-3-2 Pelupusan Media Mudah Alih	
Pelupusan media mudah alih perlu mendapat kelulusan dari Ketua Pengarah dan mengikut prosedur Kerajaan yang mana berkenaan. Peraturan yang perlu dipatuhi dalam pelupusan media adalah seperti berikut: a) Media mudah alih yang mengandungi maklumat rahsia rasmi yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul serta selamat dengan merujuk mana-mana peraturan yang berkuat kuasa berkaitan sanitasi media; b) Semua media mudah alih yang hendak dilupuskan hendaklah memastikan data rahsia rasmi / sensitif dihapuskan (*wipe data*) dengan teratur dan selamat; c) Pelupusan media mudah alih dalam aset ICT hendaklah dilaksanakan mengikut Pekeliling Pengurusan Aset Alih Kerajaan yang berkuat kuasa; dan d) Penghapusan maklumat atau kandungan media mudah alih mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	Semua pengguna

4-3-3 Penghantaran Dan Pemindahan	
Peraturan yang perlu dipatuhi dalam penghantaran dan pemindahan media adalah berdasarkan Arahan Keselamatan (Semakan dan Pindaan 2017) dan seperti berikut: a) Media penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu; b) Memastikan penghantaran atau pemindahan media ke luar pejabat mempunyai rekod; dan c) Memastikan media yang mengandungi maklumat rahsia rasmi dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa proses pemindahan.	Semua pengguna
4-3-4 Media Mudah Alih Persendirian (*Bring Your Own Device*)	
Pengguna BYOD perlu mematuhi tatacara penggunaan BYOD seperti berikut: a) Semua maklumat rasmi kerajaan adalah hak milik Kerajaan; b) Sebarang bahan rasmi yang dimuat naik/ edar/ kongsi hendaklah mendapat kebenaran Ketua Pengarah dan Pengarah Negeri; c) Menandatangani Surat Akuan Pematuhan DKICT dan Akta Rahsia Rasmi 1972 [Akta 88]; d) Memastikan peranti yang digunakan mempunyai kawalan keselamatan seperti berikut: i. Menetapkan mekanisme kawalan akses bagi BYOD dan akan mengunci secara automatik apabila tidak digunakan; ii. Melaksanakan enkripsi dan/atau perlindungan ke	Semua pengguna

atas *folder* yang mempunyai maklumat rasmi Kerajaan yang disimpan di dalam peranti BYOD; dan iii. Memastikan BYOD mempunyai ciri-ciri keselamatan standard seperti *antivirus*, *patching* terkini dan *anti theft*. e) Pengguna adalah **dilarang** daripada melakukan perkara berikut: i. Menyimpan maklumat rasmi yang sensitif dan rahsia rasmi di dalam BYOD; ii. Menggunakan BYOD untuk mengakses, menyimpan dan menyebarkan maklumat rasmi yang sensitif dan rahsia rasmi; iii. Menjadikan BYOD sebagai medium sandaran (*backup*) bagi maklumat rasmi; iv. Merakam komunikasi dan dokumen rasmi untuk tujuan peribadi; dan v. Menjadikan BYOD sebagai *access point* kepada aset ICT jabatan untuk capaian ke Internet tanpa kebenaran. f) Pengguna adalah tertakluk kepada perkara seperti berikut: i. Menggunakan BYOD secara berhemah sepanjang masa dan mematuhi mana-mana peraturan/dasar yang berkuat kuasa; ii. Memadamkan segala maklumat yang berkaitan dengan urusan rasmi jabatan sekiranya bertukar/ditamatkan perkhidmatan/bersara ATAU sewaktu dihantar ke pusat servis untuk penyelenggaraan; iii. Bertanggungjawab dan boleh dikenakan tindakan	

tatatertib atau tindakan undang-undang sekiranya didapati menyalahgunakan BYOD yang menyebabkan kehilangan/ kerosakan/ pendedahan maklumat rasmi Kerajaan; iv. CGSO berhak merampas mana-mana BYOD pengguna sekiranya didapati atau disyaki tidak mematuhi peraturan yang telah ditetapkan atau untuk tujuan siasatan; v. CGSO tidak bertanggungjawab atas kehilangan, kerosakan data atau aplikasi dalam BYOD yang digunakan; dan vi. Membenarkan pihak Kerajaan untuk membuat analisa risiko ke atas BYOD yang digunakan.	

BIDANG 5 KAWALAN CAPAIAN

5-1 KEPERLUAN KE ATAS KAWALAN CAPAIAN

Objektif:

Mengawal capaian ke atas maklumat dan kemudahan pemprosesan maklumat.

5-1-1 Polisi Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Kawalan capaian ke atas peralatan ICT menepati keperluan keselamatan dan peranan pengguna; b) Kawalan capaian ke atas perkhidmatan rangkaian	Pentadbir Sistem ICT, ICTSO, Pengurus ICT

dalaman dan luaran; c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; d) Kawalan ke atas kemudahan pemprosesan maklumat; e) Kawalan ke atas capaian aplikasi; dan f) Kawalan kebenaran untuk menyebarkan maklumat.	
5-1-2 Kawalan Capaian Rangkaian Dan Perkhidmatan Rangkaian	
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari Pengurus ICT CGSO. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a) Memastikan hanya pengguna yang dibenarkan sahaja boleh mendapat perkhidmatan rangkaian; b) Menempatkan, mengasingkan atau memasang peralatan ICT yang bersesuaian untuk kawalan keselamatan antara rangkaian CGSO, rangkaian agensi lain dan rangkaian awam; dan c) Mewujud, menguatkuasakan dan memantau mekanisme untuk pengesahan pengguna, ID pengguna, kata laluan atau peralatan ICT yang dihubungkan ke rangkaian termasuk rangkaian tanpa wayar.	ICTSO, Pengurus ICT dan Pentadbir Rangkaian
5-1-3 Pengkomputeran Awan (*Cloud Computing*)	
Pengkomputeran Awan adalah perkhidmatan sumber-sumber ICT yang dimayakan tanpa penyediaan infrastruktur di pihak pengguna paradigma atau model pengkomputeran yang membolehkan capaian rangkaian kepada himpunan sumber pengkomputeran yang fleksibel dan elastik dengan cara perkongsian sumber bersama, sama ada secara fizikal atau maya dengan keupayaan pembekalan secara layan diri dan / atau pengurusan oleh pihak ketiga mengikut permintaan pengguna [Rujukan Bab	Pentadbir Sistem ICT, Pentadbir Rangkaian dan Keselamatan, ICTSO

1 Tafsiran Arahan Keselamatan (Semakan dan Pindaan 2017)] Penggunaan dan penyediaan perkhidmatan pengkomputeran awan perlu mendapat kelulusan daripada pihak Kerajaan. Pengkomputeran awan hendaklah dipastikan selamat bagi menjamin keselamatan maklumat. Penggunaan pengkomputeran awan (c*loud computing)* seperti perkongsian maklumat, pemprosesan data dan sebagainya bagi tujuan rahsia rasmi tidak dibenarkan sama sekali kecuali pengkomputeran awan yang dibangunkan dan dibenarkan oleh pihak Kerajaan dan tertakluk kepada arahan-arahan yang dikeluarkan oleh Kerajaan dari semasa ke semasa [Rujuk Perenggan 139 Arahan Keselamatan (Semakan dan Pindaan 2017)]. Bagi perlaksanaan pengkomputeran awan yang menyeluruh hendaklah merujuk kepada Garis Panduan Pengurusan Keselamatan Maklumat Melalui Pengkomputeran Awan (*Cloud Computing*) Dalam Perkhidmatan Awam.	

5-2 PENGURUSAN CAPAIAN PENGGUNA

Objektif:

Memastikan kawalan capaian pengguna yang diperakukan sahaja dan menghalang capaian yang tidak dibenarkan kepada perkhidmatan ICT.

5-2-1 Pendaftaran Dan Pembatalan Akaun Pengguna

Mewujudkan prosedur pendaftaran dan pembatalan pengguna bagi menguruskan capaian dan pembatalan hak capaian. Perkara yang perlu dipatuhi adalah seperti berikut: a) Pendaftaran dan penamatan akaun pengguna hendaklah menggunakan borang yang dibenarkan sahaja; b) Akaun pengguna yang diperuntukkan oleh CGSO hendaklah digunakan untuk tujuan rasmi;	Pentadbir Sistem ICT, ICTSO dan Pengurus ICT

c) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna;

d) Akaun pengguna luar yang diwujudkan diberi tahap capaian dan tempoh masa mengikut peranan dan tanggungjawab pengguna dengan kelulusan pengurusan tertinggi;

e) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ianya tertakluk kepada peraturan dan arahan semasa. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan yang telah ditetapkan;

f) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang kecuali atas sebab-sebab tertentu; dan

g) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut:

i. Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh Ketua Jabatan;

ii. Pengguna yang bercuti belajar melebihi tempoh enam (6) bulan seperti mana yang diluluskan oleh Ketua Jabatan;

iii. Bertukar bidang tugas kerja;

iv. Bertukar ke agensi lain;

v. Bersara;

vi. Ditamatkan perkhidmatan serta merta pembatalan;

vii. Dalam prosiding dan/atau dikenakan tindakan tatatertib bagi tujuan dibuang kerja: serta merta pembatalan; dan

viii. Meninggal dunia. h) Akaun hendaklah didaftarkan atau dibatalkan kebenaran menerusi sistem direktori. Contoh: *Active Directory*, LDAP atau sebagainya.	
5-2-2 Penyediaan Dan Semakan Capaian Pengguna	
Mewujudkan prosedur penyediaan capaian pengguna atau pembatalan capaian pengguna kepada perkhidmatan ICT. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan hak capaian pengguna hanya kepada yang dibenarkan sahaja atau mengikut bidang tugas; b) Mengemas kini hak capaian pengguna secara berkala atau mengikut keperluan; dan c) Membatalkan hak capaian pengguna sekiranya bertukar bidang tugas, bertukar keluar, tamat perkhidmatan, dibuang kerja atau bersara.	Pentadbir Sistem ICT
5-2-3 Pengurusan Hak Capaian Khas Pengguna	
Peruntukan dan penggunaan *Priviledge Access Rights* perlu dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan bidang tugas. Hak capaian khas pengguna adalah seperti *Administrators Priviledge, Super User Priviledge* dan *Root User Priviledge*.	Pentadbir Sistem ICT
5-2-4 Pengurusan Kata Laluan Pengguna	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang telah ditetapkan seperti berikut: a) Dalam apa jua keadaan dan sebab, kata laluan	Semua pengguna dan Pentadbir Sistem ICT

hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau telah dikompromi; c) Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara besar dan kecil, angka dan aksara khusus kecuali bagi perkakasan dan perisian yang mempunyai pengurusan kata laluan terhad; d) Kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e) Kata laluan tertingkap (*windows*) dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan; g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan dengan pengenalan identiti pengguna; i) Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem dan selepas had itu, sesi ditamatkan); dan j) Tempoh masa aktif akan tamat selepas melebihi tempoh lima belas (15) minit melahu (*idle*).	
5-2-5 Kajian Semula Hak Capaian Pengguna	
Mengkaji semula hak capaian pengguna secara berkala atau sekurang- kurangnya satu (1) kali setahun atau	Pentadbir Sistem ICT

mengikut keperluan.	
5-2-6 Pembatalan Atau Pelarasan Hak Capaian Pengguna	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Hak capaian pengguna CGSO untuk kemudahan pemprosesan data dan maklumat hendaklah dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian; dan b) Pelarasan hak capaian pengguna perlulah dilakukan apabila berlaku perubahan dalaman atau perubahan bidang tugas.	Pentadbir Sistem ICT
5-3 TANGGUNGJAWAB PENGGUNA	
Objektif: Memastikan pengguna bertanggungjawab untuk melindungi maklumat yang digunakan untuk pengesahan identiti.	
5-3-1 Pematuhan Kata Laluan Pengguna	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan yang selamat; b) Memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; dan c) Mematuhi amalan *clear desk/clear screen policy*.	Semua
5-3-2 Kawalan Penggunaan Program Atau Perisian Khas Utiliti	
Penggunaan program utiliti dikawal dan perlu mematuhi perkara berikut: a) Hanya program atau perisian khas utiliti yang selamat sahaja digunakan; dan b) Penggunaan program atau perisian khas utiliti yang membebankan kapasiti (*bandwidth*) rangkaian perlu	ICTSO

dihadkan.	
5-3-3 Kawalan Capaian Kepada *Source Code* Program	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Pembangunan *source code* program perlu diselia dan dipantau oleh pemilik sistem; b) *Source code* bagi semua aplikasi dan program adalah menjadi hak milik CGSO [Rujuk Perenggan 60 (Arahan Keselamatan (Semakan dan Pindaan 2017)]; c) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan selamat; d) Sebarang pindaan *source code* mestilah mengikut prosedur yang ditetapkan; dan e) Log audit perlu dikekalkan kepada semua capaian kepada *source code.*	Pentadbir Sistem dan Pengurus ICT

BIDANG 6 KRIPTOGRAFI

6-1 KAWALAN KRIPTOGRAFI

Objektif:

Memastikan penggunaan kriptografi yang betul dan berkesan untuk melindungi kerahsiaan, kesahihan dan/atau integriti maklumat.

6-1-1 Polisi Kawalan Penggunaan Kriptografi	
CGSO perlu memastikan penggunaan kriptografi dilaksanakan dengan mematuhi perkara seperti berikut: a) Melaksanakan peraturan enkripsi untuk melindungi maklumat Rahsia Rasmi atau sensitif menggunakan kaedah kriptografi yang sesuai; b) Mengenal pasti tahap perlindungan penggunaan kriptografi dengan mengambil kira jenis, kekuatan dan	CIO, ICTSO dan Pentadbir Sistem ICT

kualiti algoritma yang diperlukan; dan c) Pengguna hendaklah menggunakan kriptografi ke atas maklumat sensitif atau maklumat rahsia rasmi atau maklumat sensitif pada setiap masa.	
6-1-2 Pengurusan Kunci Kriptografi (*Key Management*)	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Pengurusan ke atas kunci kriptografi hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut; b) Memastikan kaedah yang selamat dan berkesan untuk pengurusan kunci yang menyokong teknik kriptografi diguna pakai di CGSO; dan c) Setiap urusan transaksi maklumat sensitif hendaklah menggunakan tandatangan digital atau kunci kriptografi supaya mendapat perlindungan dan pengiktirafan undang- undang. Penggunaan tandatangan digital hendaklah dilaksanakan bagi pengurusan transaksi maklumat rahsia rasmi secara elektronik.	CIO, ICTSO dan Pentadbir Sistem ICT

BIDANG 7 KESELAMATAN FIZIKAL DAN PERSEKITARAN

7-1 KESELAMATAN KAWASAN	
Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
7-1-1 Kawalan Keselamatan Fizikal	
Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara yang perlu dipatuhi adalah seperti berikut: a) Kawasan keselamatan fizikal hendaklah dikenal pasti	Pegawai Keselamatan Kementerian, CIO dan ICTSO

dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung pada keperluan untuk melindungi aset dan hasil penilaian risiko; b) Menggunakan keselamatan parameter (halangan seperti dinding, pagar kawalan, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c) Memasang alat penggera atau kamera (CCTV); d) Menghadkan jalan keluar masuk; e) Mengadakan kaunter kawalan; f) Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g) Mewujudkan perkhidmatan kawalan keselamatan; h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; j) Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau dan bencana; k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad *(kenal pasti lokasi kawasan terhad)*; dan l) Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	

7-1-2 Kawalan Masuk Fizikal	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Setiap pengguna CGSO hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b) Semua pas keselamatan hendaklah diserahkan balik kepada CGSO apabila pengguna berhenti atau bersara; c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama premis CGSO. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan d) Kehilangan pas mestilah dilaporkan dengan segera.	Semua
7-1-3 Kawalan Keselamatan Bagi Pejabat, Bilik Dan Kemudahan ICT	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Kawasan tempat bekerja, bilik dan kemudahan ICT perlu dihadkan daripada akses oleh pengguna yang tidak berkaitan; dan b) Penunjuk ke lokasi dan tempat larangan tidak harus menonjol dan hanya memberi petunjuk minimum.	Pegawai Keselamatan Kementerian, CIO, ICTSO, Pengurus ICT dan Pentadbir Sistem
7-1-4 Kawalan Perlindungan Terhadap Ancaman Luar Dan Bencana Alam	
Perkara yang perlu dipatuhi adalah seperti berikut: a) CGSO perlu mereka bentuk dan melaksanakan pelan perlindungan fizikal dari kebakaran, banjir dan bencana alam; dan b) CGSO perlu memastikan pelan tindakan perlindungan bagi ancaman berbahaya seperti letupan, kacau bilau, rusuhan dan sebagainya.	Pegawai Keselamatan Kementerian, CIO dan ICTSO

7-1-5 Kawalan Tempat Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kepada pegawai-pegawai tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. a) Akses kepada kawasan larangan hanya kepada pegawai- pegawai yang dibenarkan sahaja; b) Pihak ketiga adalah dilarang untuk memasuki kawasan larangan kecuali dengan kebenaran untuk kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah di pantau sehingga tugas di kawasan berkenaan selesai; c) Kawasan tempat larangan perlu dikunci pada setiap masa; d) Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk; dan e) Pengguna CGSO yang perlu berurusan di pusat data hendaklah mendapatkan kebenaran dan mengisi buku log keluar masuk Pusat Data [Rujuk Garis Panduan Pengurusan Pusat Data MAMPU].	Pegawai Keselamatan Kementerian, CIO dan ICTSO
7-1-6 Kawasan Penghantaran Dan Pemunggahan	
CGSO hendaklah memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Pegawai Keselamatan Kementerian, CIO dan ICTSO

7-2 KESELAMATAN PERALATAN ICT

Objektif:

Melindungi peralatan ICT dan peranti perubatan yang mempunyai fungsi ICT CGSO dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan

yang menyebabkan perkhidmatan fasiliti terjejas.

7-2-1 Penempatan Dan Perlindungan Peralatan ICT	
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 ditetapkan; c) Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang peralatan 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 anti virus di dalam komputer mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan. Kerahsiaan kata laluan adalah di bawah tanggungjawab pengguna dan dilarang berkongsi; h) Semua aset sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptible Power Supply* (UPS);	Semua

j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan dalam rak khas. dan berkunci; k) Semua peralatan ICT yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; l) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO, Pengurus ICT dan Pegawai Aset dengan segera; m) Pengendalian aset ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; n) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pengurus ICT Pentadbir Sistem ICT; o) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk baik pulih; p) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin aset tersebut sentiasa berkeadaan baik; q) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; r) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem ICT; s) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;	

t) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan dimatikan (*Off*) apabila meninggalkan pejabat; dan u) Memastikan plug dicabut daripada suis utama (main switch) bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
7-2-2 Peralatan Sokongan ICT	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; b) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptible Power Supply*; c) Peralatan sokongan seperti *Uninterruptible Power Supply* atau penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; d) Semua alat sokongan perlu disemak dan di selenggara dari masa ke semasa (sekurang-kurangnya setahun sekali); dan e) Peralatan sokongan ICT perlulah di selenggara secara berkala.	ICTSO, Pengurus ICT dan Pentadbir Pusat Data
7-2-3 Kawalan Keselamatan Kabel Telekomunikasi Dan Elektrik	
Kabel termasuk kabel elektrik atau telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah keselamatan yang perlu diambil adalah seperti berikut: a) Memastikan hanya pengguna CGSO atau pihak ketiga yang dibenarkan boleh melaksanakan pemasangan	ICTSO, Pentadbir Rangkaian, Pentadbir Pusat Data dan Pihak Ketiga

atau penyelenggaraan kabel; b) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; c) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; d) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan e) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	
7-2-4 Penyelenggaraan Peralatan ICT	
Peralatan ICT hendaklah diselenggarakan bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara yang perlu dipatuhi adalah seperti berikut: a) Semua peralatan yang di selenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b) Memastikan peralatan hanya boleh di selenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c) Pengurusan tertinggi fasiliti bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d) Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan; dan e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pegawai aset dan Pengurus ICT

7-2-5 Pengalihan Peralatan ICT	
Bagi memastikan keselamatan peralatan ICT yang boleh dialihkan, perkara berikut hendaklah dipatuhi: a) Peralatan ICT yang hendak dibawa keluar dari premis CGSO, perlulah mendapat kelulusan dan direkodkan serta diperakukan pegawai yang dilantik; b) Peralatan ICT yang hendak dialihkan kedudukan hendaklah dimaklumkan kepada Pegawai Aset; c) Peralatan ICT yang dibawa keluar dari premis CGSO hendaklah bagi tujuan rasmi sahaja perlu mendapatkan kelulusan dan direkodkan; dan d) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang dilantik.	Semua
7-2-6 Keselamatan Peralatan ICT Di Luar Premis	
Peralatan yang dibawa keluar dari premis CGSO adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan peralatan ICT tersebut direkodkan oleh pegawai yang dilantik ke atas peralatan ICT tersebut; b) Peralatan ICT tersebut perlu dilindungi dan dikawal sepanjang masa; c) Penyimpanan atau penempatan peralatan ICT tersebut mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan d) Menyemak peralatan yang dipulangkan berada dalam keadaan baik dan lengkap.	Semua
7-2-7 Keselamatan Semasa Pelupusan Dan Penggunaan Semula	
Pelupusan atau penggunaan semula peralatan ICT melibatkan semua peralatan yang usang, rosak dan tidak boleh dibaiki.	Pengurus ICT, ICTSO dan

Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa dan perkara yang perlu dipatuhi adalah seperti berikut: a) Semua kandungan peralatan khususnya maklumat buangan rahsia rasmi hendaklah melalui proses sanitasi media dihapuskan terlebih dahulu sebelum pelupusan; b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; c) Data-data dalam storan peralatan ICT yang akan dilupuskan secara pindah milik hendaklah dihapuskan dengan cara yang selamat; d) Peralatan yang hendak di lupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; e) Pegawai yang dilantik hendaklah merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori Sistem Pengurusan Aset (SPA); f) Pelupusan peralatan ICT hendaklah mengikut tatacara pelupusan semasa yang berkuat kuasa; dan g) Pengguna adalah dilarang daripada melakukan 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, hard disk, motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan; iii. Memindah keluar dari premis mana-mana peralatan	Pegawai Aset

ICT yang hendak dilupuskan; dan iv. Memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua sebelum maklumat tersebut dihapuskan daripada peralatan ICT.	
7-2-8 Peralatan ICT Gunasama Atau Tiada Pengguna	
Pengguna perlu memastikan bahawa peralatan ICT guna sama atau tiada pengguna dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: a) Menggunakan id pengguna dan kata laluan yang diberikan; dan b) Memastikan peralatan ICT tersebut digunakan oleh pengguna CGSO yang dibenarkan sahaja.	Semua
7-2-9 Clear Desk Dan Clear Screen	
Maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Clear Desk dan Clear Screen hendaklah dilaksanakan bagi memastikan tiada bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan ciri-ciri keselamatan yang bersesuaian seperti penetapan password apabila meninggalkan komputer; b) Menyimpan bahan-bahan sensitif seperti ‘electronic storage media’ dan dokumen rahsia rasmi terperingkat mengikut tatacara yang ditetapkan Penyimpanan Dokumen Rahsia Rasmi Terperingkat; c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin penyalin fotostat; dan	Semua

d) Menghalang penggunaan mesin penyalin fotokopi dan teknologi penghasilan semula (seperti mesin pengimbas dan kamera digital) tanpa kebenaran.	
7-2-10 Kawalan Peralatan Sewaan/Ujicuba *(Proof Of Concept)*	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Penerimaan i. peralatan yang diterima bebas daripada virus, *backdoor*, *worm* dan perkara-perkara yang boleh memberi ancaman kepada perkhidmatan ICT CGSO. b) Penyelenggaraan i. capaian melalui rangkaian luar CGSO adalah tidak dibenarkan namun tertakluk kepada kebenaran Ketua Pengarah ; dan ii. aktiviti penyelenggaraan adalah di bawah pengawasan pegawai CGSO. c) Pemulangan i. maklumat yang tersimpan dalam storan perlu dihapuskan secara kekal (*secured delete*); dan ii. memastikan semua maklumat organisasi tidak tertinggal pada peralatan.	Semua

BIDANG 8 KESELAMATAN OPERASI

8-1 TANGGUNGJAWAB DAN PROSEDUR OPERASI

Objektif:

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

8-1-1 Dokumen Prosedur Operasi	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Semua prosedur pengurusan operasi yang diwujudkan, dikenal pasti dan dipakai hendaklah didokumenkan, disimpan dan dikawal; b) Setiap prosedur hendaklah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; c) Memastikan hanya pengguna yang dibenarkan sahaja boleh mengakses dokumen prosedur operasi; dan d) Semua prosedur operasi hendaklah dikemas kini dari semasa ke semasa mengikut keperluan. Semakan semula perlu dilakukan secara berkala.	Semua
8-1-2 Kawalan Perubahan	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Perubahan struktur organisasi perlu direkodkan, diperakui, disimpan dan dikawal; b) Perubahan ke atas proses kerja atau bidang tugas perlu di rekod diperakui, disimpan dan dikawal; c) Perubahan ke atas sistem atau aplikasi perlu direkodkan diperakui, disimpan dan dikawal; d) Perubahan dan pengubahsuaian yang melibatkan perkakasan, sistem perisian dan prosedur pemprosesan maklumat, hendaklah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; e) Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen	Semua

sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; f) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan g) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan, diperakui, disimpan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
8-1-3 Perancangan Kapasiti	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Kapasiti sesuatu komponen atau sistem atau aplikasi ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang yang dilantik dan diberi kuasa; b) Memastikan perancangan kapasiti ini mencukupi dan bersesuaian untuk pengoperasian, pembangunan, keupayaan serta kegunaan sistem atau aplikasi ICT pada masa akan datang; dan c) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT dan ICTSO
8-1-4 Pengasingan Persekitaran Pembangunan, Pengujian, Latihan Dan Operasi	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Mewujudkan persekitaran yang berasingan bagi: i. Pembangunan ii. Pengujian iii. Latihan iv. Operasi b) Menggunakan kaedah keselamatan ICT yang mengawal	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

persekitaran ini bagi mengurangkan risiko capaian tidak sah atau perubahan yang tidak dibenarkan.	

8-2 PERLINDUNGAN MALWARE ATAU VIRUS

Objektif:

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

8-2-1 Perlindungan Daripada Perisian Berbahaya

Perkara yang perlu dipatuhi adalah seperti berikut: a) Memasang kawalan keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS), *Intrusion Prevention System* (IPS), *Content Filtering* dan *Web Application Firewall* (WAF) dan mengikut prosedur penggunaan yang betul dan selamat; b) Memasang dan menggunakan hanya perisian keselamatan ICT bagi semua aset ICT; c) Penggunaan perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; d) Mengimbas semua perisian atau sistem dengan anti-virus sebelum instalasi atau penggunaannya; e) Mengemas kini anti virus dengan *pattern* anti virus yang terkini; f) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; g) Mengadakan program kesedaran kepada pengguna mengenai ancaman perisian berbahaya dan cara mengendalikannya;	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

h) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; i) Melaksanakan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan j) Memberi notifikasi kepada pegawai yang bertanggungjawab mengenai ancaman keselamatan ICT seperti serangan malware atau virus.	

8-3 SALINAN PENDUA (BACKUP)

Objektif:

Memastikan sistem, aplikasi, data, imej dan maklumat mempunyai salinan pendua, berkeupayaan untuk *restore* semula dan melindungi daripada kehilangan maklumat.

8-3-1 Maklumat Pendua (*Backup*)

Bagi melindungi data atau maklumat hilang, *backup* hendaklah dilaksanakan ke atas sistem dan aplikasi. Perkara yang perlu dipatuhi adalah seperti berikut: a) Membuat polisi *backup* keselamatan ke atas semua sistem dan aplikasi kritikal seperti berikut: i. Harian (*Incremental*); ii. Mingguan (*Full*); dan iii. Bulanan (*Full*). b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi dan tahap kritikal maklumat; c) Menguji sistem *backup* dan prosedur *restore* sekurang-kurangnya sekali setahun; d) Memastikan sistem *backup* berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

digunakan khususnya pada waktu kecemasan; e) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan f) Merekodkan dan menyimpan salinan *backup* di lokasi yang berlainan (*off-site*) dan selamat.	

8-4 LOG DAN PEMANTAUAN

Objektif:

Memastikan log direkodkan dan menjana pembuktian melalui pemantauan.

8-4-1 Log Aktiviti

Memastikan setiap peralatan ICT menyimpan log bagi merekod aktiviti pengguna, *exceptions, faults* dan log keselamatan maklumat. Log ini hendaklah dijana, disimpan dan disemak secara berkala. Perkara yang perlu dipatuhi adalah seperti berikut: a) Merekod setiap aktiviti transaksi secara berpusat atau tertakluk kepada keperluan; b) Mengandungi ID pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c) Memastikan aktiviti capaian pengguna ke atas sistem ICT adalah sah; d) Mengenal pasti aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. e) Menyimpan log audit untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; f) Memastikan masa (*time stamp*) dalam sistem di CGSO diselaraskan dengan suatu masa yang dipersetujui;	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

dan g) Memastikan analisa ke atas log dilaksanakan secara berkala atau mengikut keperluan.	
8-4-2 Kawalan Perlindungan Log	
Perkara yang mesti dipatuhi adalah seperti berikut: a) Melindungi maklumat log daripada capaian yang tidak dibenarkan; b) Capaian ke atas log fail *server* hanya kepada pengguna yang dibenarkan sahaja; c) Memastikan log fail tidak boleh diubah; d) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan e) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
8-4-3 Log Pentadbir Dan Pengendali (Operator)	
Perkara yang mesti dipatuhi adalah seperti berikut: a) Memastikan setiap aktiviti log bagi pentadbir dan pengendali sistem direkodkan; b) Melindungi aktiviti log pentadbir dan pengendali sistem daripada capaian yang tidak sah atau hanya yang dibenarkan sahaja; dan c) Memastikan log ini sentiasa dipantau dan disemak secara berkala atau mengikut keperluan.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
8-4-4 Penyeragaman Waktu (*Clock Synchronisation*)	
Waktu bagi sistem, aplikasi atau peralatan	Pentadbir

ICT hendaklah diselaraskan dengan Masa Standard Malaysia.	Sistem ICT, Pengurus ICT

8-5 KAWALAN PERISIAN OPERASI

Objektif:

Melindungi sistem operasi dan memastikan integriti sistem operasi.

8-5-1 Instalasi Perisian Pada Sistem Operasi

Memastikan pelaksanaan kawalan ke atas instalasi perisian pada sistem operasi. Perkara yang mesti dipatuhi adalah seperti berikut: a) Pengemaskinian perisian operasi, aplikasi dan program *libraries* hanya boleh dilakukan oleh pentadbir terlatih setelah mendapat kelulusan pengurusan; b) Sistem operasi hanya boleh memegang "*executable code*"; c) Instalasi perisian hendaklah mendapat kebenaran daripada Pentadbir Sistem ICT dan ICTSO; d) Memastikan penggunaan perisian mempunyai lesen sah; e) Penggunaan aplikasi dalam sistem operasi hanya boleh dilaksanakan selepas ujian yang terperinci dan diperakui berjaya; f) Setiap konfigurasi ke atas sistem operasi perlu dikawal dan didokumentasikan melalui prosedur perubahan kawalan konfigurasi. Konfigurasi hanya boleh dilaksanakan selepas mendapat persetujuan dari pihak berkaitan; dan g) Satu '*rollback*' strategi harus diadakan sebelum perubahan dilaksanakan.	Semua

8-6 PENGURUSAN KETERDEDAHAN TEKNIKAL (TECHNICAL VULNERABILITY)

Objektif:

Melindungi dan mencegah daripada berlaku eksploitasi pada keterdedahan teknikal.

8-6-1 Pengurusan Ancaman Keterdedahan Teknikal

Perkara yang mesti dipatuhi adalah seperti berikut: a) Menggunakan kawalan keselamatan ICT untuk mengenal pasti keterdedahan teknikal pada sistem maklumat yang digunakan; b) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; c) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan d) Mengambil tindakan pengawalan dan pengukuhan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

8-6-2 Kawalan Pemasangan Perisian

Perkara yang mesti dipatuhi adalah seperti berikut: a) Hanya perisian yang diperakui oleh ICTSO sahaja dibenarkan bagi kegunaan pengguna di CGSO; b) Memasang dan menggunakan hanya perisian yang tulen, berlesen dan dilindungi di bawah mana-mana undang- undang bertulis yang berkuat kuasa; dan c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya.	Semua

8-7 KEPERLUAN AUDIT PADA SISTEM MAKLUMAT

Objektif:

Mengurangkan impak bagi aktiviti audit ke atas sistem operasi.	
8-7-1 Kawalan Audit Pada Sistem Maklumat	
Perkara yang mesti dipatuhi adalah seperti berikut: a) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan; b) Meminimumkan gangguan dan kesan daripada kawalan audit yang dilaksanakan; dan c) Capaian ke atas audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

BIDANG 9 KESELAMATAN KOMUNIKASI

9-1 PENGURUSAN KESELAMATAN RANGKAIAN	
Objektif: Memastikan kawalan keselamatan dan perlindungan maklumat termasuk kemudahan pemproses maklumat dalam rangkaian.	
9-1-1 Kawalan Rangkaian	
Perkara yang mesti dipatuhi adalah seperti berikut: a) Menggunakan kawalan keselamatan rangkaian ICT yang bersesuaian di antara rangkaian ICT CGSO, rangkaian agensi lain dan rangkaian awam; b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna; c) Menggunakan kawalan keselamatan rangkaian ICT yang menepati kesesuaian penggunaannya; d) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap rangkaian ICT;	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

e) Semua trafik keluar dan masuk dalam rangkaian ICT CGSO mestilah melalui *firewall* atau kawalan keselamatan rangkaian ICT yang bersesuaian; f) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran daripada Pegawai Keselamatan ICT (ICTSO); g) Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti- aktiviti lain yang boleh mengancam data dan maklumat CGSO; h) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; i) Sebarang penyambungan rangkaian (wired & wireless) yang bukan di bawah kawalan Pengurus ICT adalah tidak dibenarkan; j) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di CGSO sahaja dan penggunaan modem atau peralatan sambungan rangkaian yang lain adalah dilarang sama sekali; dan k) Kemudahan rangkaian tanpa wayar (*wireless*) hendaklah dipantau dan dikawal penggunaannya;	
9-1-2 Keselamatan Perkhidmatan Rangkaian	
d) Mekanisme keselamatan dan tahap perkhidmatan bagi semua perkhidmatan rangkaian sama ada oleh pihak ketiga atau secara dalaman hendaklah dikenal pasti serta dimasukkan dalam perjanjian perkhidmatan rangkaian. Perkara yang mesti dipatuhi adalah seperti berikut: e) Memastikan keselamatan maklumat organisasi diambil kira dalam setiap perjanjian perkhidmatan rangkaian dengan pihak ketiga;	Pentadbir Sistem ICT dan ICTSO

f) Menandatangani perjanjian bertulis untuk melindungi maklumat apabila berlaku pemindahan maklumat organisasi antara CGSO dengan pihak luar; g) Terma perkongsian maklumat dan perisian di antara CGSO dengan pihak ketiga hendaklah dimasukkan di dalam perjanjian; h) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi Service Level Agreement (SLA) yang telah dipersetujui; dan i) Mempunyai mekanisme pengurusan insiden sekiranya berlaku insiden keselamatan maklumat.	
9-1-3 Pengasingan Rangkaian	
Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian CGSO. Perkara yang mesti dipatuhi adalah seperti berikut: a) *Demilitarized Zone* (DMZ) untuk sistem atau aplikasi luaran; b) Server *Farm* dikhaskan untuk pelayan; c) Segmen Rangkaian Dalaman (LAN) digunakan untuk pengguna CGSO; d) Segmen Rangkaian Luaran (WAN) untuk akses ke Internet atau rangkaian luar CGSO; e) Segmen rangkaian tanpa wayar (*Wireless*) untuk pelawat; f) Segmen rangkaian tanpa wayar (*Wireless*) untuk pengguna; g) Segmen rangkaian untuk pengurusan peralatan (*Management Segment*); dan	Pentadbir Rangkaian

h) Lain-lain segmen rangkaian yang diperlukan bagi mengawal keselamatan maklumat.	

9-2 PERPINDAHAN MAKLUMAT

Objektif:

Memastikan kawalan keselamatan semasa perpindahan atau pertukaran maklumat antara CGSO dengan pihak ketiga.

9-2-1 Polisi Dan Prosedur Perpindahan Maklumat

Perkara yang mesti dipatuhi adalah seperti berikut: a) Dasar, prosedur dan kawalan perpindahan maklumat yang formal perlu diwujudkan untuk melindungi perpindahan maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; dan b) Tatacara dan syarat perpindahan maklumat antara CGSO dengan pihak ketiga perlu dimasukkan dalam perjanjian atau surat persetujuan.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

9-2-2 Perjanjian Dalam Perpindahan Maklumat

Memastikan keselamatan maklumat organisasi dengan mewujudkan perjanjian bertulis apabila berlaku perpindahan maklumat antara CGSO dengan pihak ketiga. Perkara yang mesti dipatuhi adalah seperti berikut: a) Pengurusan CGSO hendaklah mengawal penghantaran dan penerimaan maklumat organisasi; b) Prosedur bagi verifikasi maklumat organisasi semasa pemindahan maklumat; dan c) Tanggungjawab dan tindakan pengukuhan mesti dilaksanakan sekiranya berlaku insiden keselamatan maklumat seperti kehilangan data.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

9-2-3 Pengurusan Emel Atau Mesej Elektronik

Penggunaan emel di CGSO hendaklah dipantau secara berterusan oleh Pentadbir emel untuk memenuhi	Semua

keperluan etika penggunaan emel dan Internet yang terkandung dalam pekeliling dan semua undang-undang yang berkuat kuasa. Perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a) Akaun atau alamat emel yang diperuntukkan oleh CGSO sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang kecuali dengan kebenaran; b) Setiap emel yang disediakan hendaklah mematuhi format yang telah ditetapkan; c) Memastikan subjek dan kandungan emel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d) Penghantaran emel rasmi hendaklah menggunakan akaun emel rasmi dan pastikan alamat penerima emel adalah betul; e) Pengguna dinasihatkan menggunakan fail yang dikepilkan, sekiranya perlu tidak melebihi sepuluh megabait (10MB) semasa penghantaran. Kaedah pemampatan (zip) untuk mengurangkan saiz adalah disarankan; f) Pengguna hendaklah mengelak dari membuka emel daripada penghantar yang tidak diketahui atau diragui; g) Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui emel; h) Setiap emel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;	pengguna

i) emel 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 emel dengan cepat dan mengambil tindakan segera; l) Pengguna hendaklah memastikan alamat emel persendirian tidak boleh digunakan untuk tujuan rasmi; m) Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing; n) Bagi pengguna yang telah bertukar jabatan dan bersara, akaun emel mereka akan ditamatkan dalam tempoh empat belas (14) hari dari tarikh pertukaran atau persaraan kecuali bagi kes-kes tertentu yang telah mendapat kelulusan Pengurus ICT; dan o) Bagi pengguna yang telah ditamatkan perkhidmatan atau meninggal dunia, akaun emel mereka ditamatkan serta-merta.	
9-2-4 Kerahsiaan Dan Non-Disclosure Agreement	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Mewujudkan perjanjian kerahsiaan atau *non-disclosure agreement* (NDA) dengan pihak ketiga; b) Mengambil kira keperluan kerahsiaan maklumat organisasi dalam perjanjian; dan c) Mengkaji dan menyemak perjanjian dari masa semasa serta mendokumentasikan perjanjian.	CIO, Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

BIDANG 10 PEROLEHAN, PEMBANGUNAN, PENAMBAHBAIKAN DAN PENYELENGGARAAN SISTEM

10-1 KEPERLUAN KESELAMATAN SISTEM MAKLUMAT

Objektif:

Memastikan keperluan keselamatan sistem maklumat dikenal pasti, dipersetujui dan didokumenkan pada setiap peringkat perolehan, pembangunan, penambahbaikan dan penyelenggaraan. Pernyataan keperluan bagi sistem maklumat hendaklah menjelaskan mengenai kawalan jaminan keselamatan.

10-1-1 Analisis Keperluan Dan Spesifikasi Keselamatan Maklumat

Perkara yang perlu dipatuhi adalah seperti berikut: d) Perolehan baru, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira keperluan keselamatan maklumat bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; e) Ujian keselamatan atau keterdedahan 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 menghasilkan data yang telah diproses adalah tepat; f) Sistem maklumat perlu mengandungi semakan pengesahan (validation) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan g) 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.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

10-1-2 Keselamatan Perkhidmatan Aplikasi Dalam Rangkaian Umum

Maklumat dari perkhidmatan aplikasi yang menggunakan	Pemilik Sistem,

rangkaian umum hendaklah dilindungi daripada aktiviti-aktiviti ancaman keselamatan atau akses yang tidak dibenarkan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Menggunakan *encryption* untuk penghantaran atau penerimaan maklumat yang menggunakan rangkaian umum; b) Memastikan perkhidmatan aplikasi menggunakan *Secure Sockets Layer* (SSL) dalam setiap transaksi; c) Memastikan pengesahan berkaitan dengan pihak yang berhak untuk meluluskan kandungan maklumat, penerbitan atau menandatangani dokumen transaksi ; d) Memastikan setiap pengguna perkhidmatan aplikasi adalah pengguna yang betul dan sah; dan e) Memastikan pengguna mempunyai tahap akses mengikut kelulusan atau kebenaran pemilik sistem.	Pentadbir Sistem ICT dan ICTSO
10-1-3 Perlindungan Transaksi Perkhidmatan Aplikasi	
Transaksi bagi perkhidmatan aplikasi hendaklah dilindungi daripada penghantaran yang tidak lengkap (mis-routing), pengubahan maklumat, pendedahan yang tidak dibenarkan serta penduaan mesej. Perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi; b) Memastikan semua kriteria transaksi seperti di bawah dipatuhi: i. Maklumat pengguna adalah sah dan telah diperakukan; ii. Mengekalkan kerahsiaan maklumat; iii. Mengekalkan privasi pihak yang terlibat; iv. Komunikasi antara semua pihak yang terlibat telah di enkrip;	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

v. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi; c) Menggunakan mekanisme tambahan seperti *secret key*, kad pintar dan medium kawalan yang lain untuk pengesahan pengguna; dan d) Pihak yang mengeluar dan mengekalkan pensijilan digital atau tandatangan adalah dilantik oleh Kerajaan.	

10-2 KESELAMATAN PEMBANGUNAN SISTEM DAN PROSES SOKONGAN

Objektif:

Memastikan keperluan keselamatan sistem maklumat dikenal pasti, dipersetujui dan didokumenkan pada setiap kitaran hayat pembangunan sistem maklumat.

10-2-1 Tatacara Keselamatan Dalam Pembangunan Sistem

Peraturan atau tatacara pembangunan sistem hendaklah diwujudkan dan digunakan oleh CGSO. Perkara yang perlu dipatuhi adalah seperti berikut: a) Keperluan keselamatan maklumat semasa persekitaran kitaran hayat pembangunan; b) Panduan keselamatan dalam kitar hayat pembangunan sistem maklumat; c) Keselamatan maklumat dalam fasa reka bentuk; d) Pemeriksaan keselamatan dalam perkembangan projek; e) Keselamatan repositori atau ruang storan; f) Keselamatan dalam kawalan versi; g) Keperluan pengetahuan keselamatan dalam pembangunan sistem maklumat (*secure coding*); dan h) Kebolehan pengaturcara untuk mengenal pasti kelemahan dan mencadangkan penambahbaikan dalam pembangunan sistem.	Pemilik Sistem dan Pentadbir Sistem ICT, Pembangun Sistem ICT

10-2-2 Prosedur Kawalan Perubahan Sistem	
Perubahan ke atas sistem di dalam kitaran pembangunan hendaklah dikawal menggunakan prosedur kawalan perubahan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Mengenal pasti perubahan ke atas sistem yang hendak dilaksanakan melalui kajian keperluan pengguna (*user requirement study* – URS); b) Mendokumentasi dan mengesahkan URS sebelum dilaksanakan; c) Mengkaji impak operasi dan keselamatan maklumat bagi setiap perubahan yang dicadangkan; d) Melaksanakan perubahan sistem pada pelayan pembangunan untuk menguji keberkesanan operasi; e) Setiap permohonan perubahan/penambahbaikan sistem hendaklah menggunakan *Change Request Form* (CRF) bagi memantau dan mengawal perubahan/ penambahbaikan yang dilaksanakan oleh pengaturcara; dan f) Kawalan perlu dibuat ke atas sebarang perubahan atau pindaan ke atas sistem bagi memastikan ianya terhad mengikut keperluan sahaja.	Pemilik Sistem dan Pentadbir Sistem ICT
10-2-3 Kajian Teknikal Sistem Maklumat Selepas Perubahan Platform Operasi	
Perubahan platform operasi sama ada sistem pengoperasian atau rangka kerja (*framework*) hendaklah dikaji dan diuji bagi memastikan tiada sebarang masalah yang timbul terhadap operasi atau keselamatan sistem. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan perubahan platform operasi ini dilaksanakan dalam persekitaran pengujian; b) Kawalan aplikasi dan prosedur integriti disemak untuk memastikan sistem tidak terjejas apabila berlaku	Pemilik Sistem dan Pentadbir Sistem ICT

perubahan platform operasi; c) Perubahan platform dimaklumkan dari semasa ke semasa bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan d) Memastikan perubahan yang sesuai diselaraskan kepada pelan kesinambungan perkhidmatan.	
10-2-4 Kawalan Keselamatan Perubahan Pakej Perisian (*Software Packages*)	
Perubahan kepada pakej perisian adalah tidak digalakkan tetapi terhad kepada perubahan yang diperlukan dan semua perubahan hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan perubahan pakej perisian ini mengambil kira aspek keselamatan maklumat; b) Perubahan pakej perisian ini hanya dilaksanakan oleh pihak yang dibenarkan sahaja; c) Melaksanakan pengujian ke atas pakej perisian yang terkini sebelum dimaklumkan kepada semua pengguna mengenai perubahan versi pakej perisian; dan d) Memastikan perubahan pakej perisian ini tidak menjejaskan perkhidmatan operasi sistem maklumat.	Pemilik Sistem dan Pentadbir Sistem ICT
10-2-5 Prinsip Kejuruteraan Keselamatan Sistem	
Prinsip kejuruteraan yang selamat bagi pembangunan sistem maklumat hendaklah diwujudkan, di dokumentasi, di selenggara dan diguna pakai dalam pelaksanaan sistem. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan keselamatan seperti ancaman daripada bencana alam dan manusia diambil kira; b) Perlindungan maklumat dalam pembangunan sistem semasa pemprosesan, perpindahan dan penyimpanan; dan	Pemilik Sistem dan Pentadbir Sistem ICT

c) Mengambil kira kriteria di bawah dalam prinsip kejuruteraan pembangunan sistem. i. *Business Layer* - berdasarkan tahap pengesahan pengguna; hanya pengguna tertentu boleh melihat data peribadi; ii. *Data Layer* - hanya log masuk dengan kata laluan pangkalan data yang selamat untuk aktiviti penyelenggaraan pangkalan data dibenarkan; iii. *Application Layer* - penggunaan enkripsi untuk penghantaran maklumat; dan iv. *Technology Layer* - penggunaan perisian sumber terbuka dan infrastruktur rangkaian.	
10-2-6 Keselamatan Persekitaran Pembangunan Sistem	
Persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran hayat pembangunan sistem (*system development life cycle*). Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan persekitaran pembangunan sistem yang berbeza diasingkan dan mewujudkan mekanisme kawalan; b) Capaian ke persekitaran pembangunan ini hanya kepada pengguna yang dibenarkan sahaja; dan c) Memastikan pengaturcara menggunakan mekanisme yang selamat dalam perpindahan data atau maklumat.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO
10-2-7 Pembangunan Sistem Oleh Pihak Ketiga (*Outsourced*)	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Pembangunan sistem oleh pihak ketiga perlu diselia dan dipantau oleh CGSO; b) Memastikan perpindahan teknologi oleh pihak ketiga	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

kepada CGSO dilaksanakan; c) Kod sumber (*source code*) bagi semua sistem dan aplikasi yang dibangunkan menjadi hak milik CGSO; d) Memastikan pembangunan sistem menggunakan teknik *secure coding*; dan e) Pembangunan sistem maklumat disarankan dilaksanakan di dalam premis CGSO atau premis Kerajaan.	
10-2-8 Pengujian Keselamatan Sistem Maklumat	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Pengujian fungsi keselamatan sistem hendaklah dilaksanakan semasa fasa pembangunan; b) Semua sistem baru atau penambahbaikan sistem hendaklah menjalani ujian *Security Posture Assessment* (SPA); c) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; d) Mengenal pasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data; dan e) Menjalankan proses semakan ke atas *output data* daripada setiap proses aplikasi untuk menjamin ketepatan.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO
10-2-9 Pengujian Penerimaan Sistem Maklumat	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan proses kerja sistem memenuhi keperluan pengguna; b) Melaksanakan ujian fungsi ke atas sistem menggunakan	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

dummy input; c) Semakan ke atas sistem jika memenuhi keperluan perniagaan organisasi dan kebolehgunaan sistem; d) Melaksanakan integrasi dan pengujian dengan sistem yang lain sekiranya berkaitan; e) Merangkumi ujian alfa (*alpha testing*) dan ujian beta (*beta testing*); dan f) Melibatkan ujian prestasi (*performance test*) dan ujian stress (*stress test*).	

10-3 DATA UJIAN

Objektif:

Memastikan keselamatan data semasa pengujian.

10-3-1 Kawalan Data Ujian

Perkara yang perlu dipatuhi adalah seperti berikut: a) Data ujian yang hendak digunakan perlu dipilih dengan berhati-hati, diperakui, dilindungi dan dikawal; b) Pengunaan data ujian hendaklah dilaksanakan ke atas kod atur cara yang terkini; c) Mengaktifkan audit log bagi merekodkan semua aktiviti pengujian; d) Data ujian hanya boleh digunakan oleh pengguna yang dibenarkan sahaja; dan e) Data ujian perlu dihapuskan setelah proses pengujian dilaksanakan.	Pemilik Sistem dan Pentadbir Sistem ICT

BIDANG 11 PERHUBUNGAN DENGAN PEMBEKAL

11-1 KESELAMATAN MAKLUMAT PERHUBUNGAN DENGAN PEMBEKAL

Objektif:

Memastikan kawalan keselamatan ke atas aset CGSO yang boleh dicapai oleh pembekal.

11-1-1 Dasar Keselamatan Maklumat Untuk Pembekal

Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan perjanjian disediakan dan didokumentasikan dengan pembekal yang mempunyai capaian ke atas aset CGSO; b) Mengenal pasti tahap capaian mengikut kategori pembekal; c) Merekod dan memantau semua capaian pembekal; d) Memastikan pembekal diberikan taklimat keselamatan dan menandatangani Surat Akuan Pematuhan Dasar Keselamatan CGSO seperti di **Lampiran 1**; e) Memastikan setiap pembekal melaksanakan tapisan keselamatan menerusi melalui sistem *e-Vetting* yang disediakan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO) iaitu Sistem e-*Vetting*; dan f) Menandatangani Perakuan Akta Rahsia Rasmi 1972 seperti di **Lampiran 2**.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

11-1-2 Menangani Aspek Keselamatan Dalam Perjanjian Pembekal

Keperluan keselamatan maklumat hendaklah diwujudkan dan dipersetujui dengan pembekal yang akan mengakses, memproses, menyimpan, berkomunikasi atau menyediakan komponen infrastruktur di CGSO. Perkara yang perlu diambil kira seperti berikut: a) Mengadakan sesi taklimat keselamatan;	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

b) Mengklasifikasikan maklumat; c) Keperluan undang-undang dan peraturan yang sedang berkuat kuasa; d) Obligasi setiap pihak bagi kawalan akses, pemantauan, pelaporan dan pengauditan; e) Tapisan Keselamatan Vendor/Kontraktor (pembekal); dan f) Tindakan undang-undang.	
11-1-3 Rantaian Bekalan Atau Perkhidmatan Teknologi Maklumat Dan Komunikasi	
Perjanjian dengan pembekal hendaklah mengambil kira keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan rantaian bekalan atau perkhidmatan teknologi maklumat dan komunikasi. Perkara yang perlu diambil kira seperti berikut: a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan; b) Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada subkontraktor bagi perkhidmatan; c) Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada pembekal-pembekal lain bagi pembekalan produk; d) Melaksanakan satu kaedah pemantauan yang boleh mengesahkan pembekalan produk dan perkhidmatan mematuhi keperluan keselamatan maklumat CGSO; e) Mengenal pasti komponen produk dan perkhidmatan kritikal dan komponen tambahan; f) Memastikan jaminan dari pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik; dan	Pentadbir Sistem ICT, Pengurus ICT

g) Menentukan kaedah-kaedah bagi perkongsian maklumat mengenai rantaian bekalan (*supply chain*) antara CGSO dan pembekal.	

11-2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PEMBEKAL

Objektif:

Mengekalkan tahap keselamatan maklumat yang telah dipersetujui dalam penyampaian perkhidmatan selaras dengan perjanjian bersama pembekal.

11-2-1 Pemantauan Dan Kajian Perkhidmatan Pembekal

Perkara yang perlu diambil kira seperti berikut: a) Melaksanakan pemantauan, kajian semuladan pengauditan perkhidmatan pembekal mengikut keperluan; b) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian; dan c) Menyemak dan mengesahkan laporan perkhidmatan serta laporan insiden keselamatan yang dikemukakan oleh pembekal berdasarkan kepada status kemajuan perkhidmatan.	Pentadbir Sistem ICT, Pengurus ICT

11-2-2 Pengurusan Perubahan Dalam Perkhidmatan Pembekal

Perkara yang perlu diambil kira seperti berikut: a) Memastikan perubahan dalam perkhidmatan pembekal dipersetujui bersama dan menguntungkan bagi pihak CGSO; b) Memastikan perubahan dalam perjanjian dengan pembekal mengambil kira maklumat kritikal CGSO, sistem serta proses yang terlibat dan kajian risiko; c) Perubahan yang dilakukan oleh CGSO untuk meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

d) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.	
11-1-2 Menangani Aspek Keselamatan Dalam Perjanjian Pembekal	
Keperluan keselamatan maklumat hendaklah diwujudkan dan dipersetujui dengan pembekal yang akan mengakses, memproses, menyimpan, berkomunikasi atau menyediakan komponen infrastruktur di CGSO. Perkara yang perlu diambil kira seperti berikut: a) Mengadakan sesi taklimat keselamatan; b) Mengklasifikasikan maklumat; c) Keperluan undang-undang dan peraturan yang sedang berkuat kuasa; d) Obligasi setiap pihak bagi kawalan akses, pemantauan, e) pelaporan dan pengauditan; f) Tapisan Keselamatan Vendor/Kontraktor (pembekal); dan g) Tindakan undang-undang.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
11-1-3 Rantaian Bekalan Atau Perkhidmatan Teknologi Maklumat Dan Komunikasi	
Perjanjian dengan pembekal hendaklah mengambil kira keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan rantaian bekalan atau perkhidmatan teknologi maklumat dan komunikasi. Perkara yang perlu diambil kira seperti berikut: a) Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan;	Pentadbir Sistem ICT, Pengurus ICT

b) Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada subkontraktor bagi perkhidmatan; c) Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada pembekal-pembekal lain bagi pembekalan produk; d) Melaksanakan satu kaedah pemantauan yang boleh mengesahkan pembekalan produk dan perkhidmatan mematuhi keperluan keselamatan maklumat CGSO; e) Mengenal pasti komponen produk dan perkhidmatan kritikal dan komponen tambahan; f) Memastikan jaminan dari pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik; dan g) Menentukan kaedah-kaedah bagi perkongsian maklumat mengenai rantaian bekalan (*supply chain*) antara CGSO dan pembekal.	

11-2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PEMBEKAL

Objektif:

Mengekalkan tahap keselamatan maklumat yang telah dipersetujui dalam penyampaian perkhidmatan selaras dengan perjanjian bersama pembekal.

11-2-1 Pemantauan Dan Kajian Perkhidmatan Pembekal

Perkara yang perlu diambil kira seperti berikut: a) Melaksanakan pemantauan, kajian semula dan pengauditan perkhidmatan pembekal mengikut keperluan; b) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian; dan c) Menyemak dan mengesahkan laporan perkhidmatan serta laporan insiden keselamatan yang dikemukakan	Pentadbir Sistem ICT, Pengurus ICT

oleh pembekal berdasarkan kepada status kemajuan perkhidmatan.	
11-2-2 Pengurusan Perubahan Dalam Perkhidmatan Pembekal	
Perkara yang perlu diambil kira seperti berikut: a) Memastikan perubahan dalam perkhidmatan pembekal dipersetujui bersama dan menguntungkan bagi pihak CGSO; b) Memastikan perubahan dalam perjanjian dengan pembekal mengambil kira maklumat kritikal CGSO, sistem serta proses yang terlibat dan kajian risiko; c) Perubahan yang dilakukan oleh CGSO untuk meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan d) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan subkontraktor.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

BIDANG 12 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

12-1 MEKANISME PELAPORAN INSIDEN KESELAMATAN

Objektif:

Memastikan pendekatan yang konsisten dan berkesan untuk pengurusan insiden keselamatan maklumat termasuk mengenal pasti ancaman dan kelemahan.

12-1-1 Prosedur Dan Tanggungjawab	
Perkara yang perlu diambil kira seperti berikut: a) Menubuhkan prosedur dan pasukan yang mengendalikan serta menguruskan insiden keselamatan maklumat;	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

b) Memastikan tindakan pengukuhan serta maklum balas yang cepat, efektif dan teratur bagi setiap insiden keselamatan maklumat; dan c) Pemakluman kepada pihak berkuasa atau agensi yang bertanggungjawab dalam menangani insiden keselamatan.	
12-1-2 Mekanisme Pelaporan Insiden Keselamatan	
Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO. Tindakan oleh CERT, CGSO untuk melaporkan kepada Agensi Keselamatan Siber Negara (NACSA), Majlis Keselamatan Negara dengan kadar segera. Prosedur pelaporan insiden keselamatan ICT adalah 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 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
12-1-3 Pelaporan Kelemahan Keselamatan ICT	
Kakitangan dan pembekal yang menggunakan sistem dan perkhidmatan ICT CGSO dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT. Perkara yang perlu dilaporkan adalah seperti berikut: a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan atau disyaki hilang, dicuri atau	Semua

didedahkan; d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.	
12-1-4 Penilaian Dan Analisa Aktiviti Keselamatan Maklumat	
Aktiviti keselamatan maklumat hendaklah dinilai dan dianalisa sama ada akan diklasifikasikan sebagai insiden keselamatan maklumat. Perkara yang perlu diambil kira adalah seperti berikut: a) Merekod dan menyimpan semua aktiviti keselamatan maklumat secara berpusat atau pada peralatan ICT; dan b) Menganalisa setiap aktiviti keselamatan maklumat secara berkala bagi memastikan pihak yang berkaitan dapat mengklasifikasikan aktiviti tersebut.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
12-1-5 Tindakan Pada Insiden Keselamatan Maklumat	
Perkara yang perlu diambil kira adalah seperti berikut: a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; b) Menjalankan kajian dan analisa; c) Menghubungi pihak berkuasa atau agensi yang berkenaan dengan secepat mungkin; d) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; dan f) Menangani insiden keselamatan maklumat mengikut	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
12-1-6 Pengalaman Dari Insiden Keselamatan Maklumat	
Pengalaman serta pengetahuan yang diperolehi melalui proses menganalisis dan penyelesaian insiden keselamatan maklumat yang telah berlaku boleh digunakan untuk mengurangkan kebarangkalian (likelihood) atau kesan insiden pada masa akan datang. Perkara yang perlu diambil kira adalah seperti berikut: a) Menyimpan dan merekodkan tindakan pengukuhan yang telah dilaksanakan semasa berlaku insiden keselamatan; dan b) Menganalisa impak ke atas tindakan yang dilaksanakan.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
12-1-7 Pengumpulan Bahan Bukti	
Perkara yang perlu diambil kira adalah seperti berikut: a) Prosedur untuk mengenal pasti, mengumpul, mendapatkan dan menyimpan bahan bukti hendaklah dibangunkan bagi memastikan bahan bukti dilindungi dan tersedia; dan b) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

BIDANG 13 ASPEK KESELAMATAN DALAM PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

13-1 KESELAMATAN MAKLUMAT KESINAMBUNGAN

Objektif:

Memastikan keselamatan maklumat hendaklah diterapkan dalam sistem pengurusan kesinambungan perkhidmatan CGSO.

13-1-1 Perancangan Keselamatan Maklumat	
CGSO hendaklah menentukan keperluan untuk keselamatan maklumat dan kesinambungan pengurusan keselamatan maklumat semasa berlaku krisis dan bencana. Perkara yang perlu diambil kira adalah seperti berikut: a) Membangunkan Pelan Kesinambungan Perkhidmatan dengan mengenal pasti aspek keselamatan maklumat yang terlibat; b) Mengenal pasti keselamatan maklumat pada lokasi dan Pelan Kesinambungan Perkhidmatan; c) Memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan CGSO; dan d) Memastikan pelan ini diluluskan oleh pegawai yang bertanggungjawab.	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT
13-1-2 Pelaksanaan Keselamatan Maklumat	
CGSO hendaklah mewujud, mendokumentasi, melaksana dan mengekalkan proses, prosedur serta kawalan untuk memastikan tahap keselamatan maklumat bagi kesinambungan perkhidmatan dalam situasi yang terancam. Perkara yang perlu diambil kira adalah seperti berikut: a) Mengenal pasti aspek keselamatan dalam membangunkan pelan kesinambungan keselamatan; b) Mengenal pasti semua aset, tanggungjawab, struktur organisasi dan menetapkan prosedur kecemasan atau pemulihan amalan terbaik; c) Mengenal pasti ancaman yang boleh mengakibatkan gangguan terhadap proses organisasi; d) Mengenal pasti kemungkinan dan impak gangguan tersebut serta akibatnya terhadap keselamatan ICT; e) Menjalankan analisis impak organisasi; f) Melaksanakan prosedur kecemasan bagi	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; g) Mendokumentasikan proses dan prosedur yang telah ditetapkan; h) Mengadakan program latihan secara berkala kepada warga CGSO mengenai prosedur kecemasan; i) Membuat backup mengikut prosedur yang ditetapkan; dan j) Menguji, menyelenggara dan mengemas kini Pelan Pengurusan Bencana [Data Recovery Plan (DRP)] keselamatan ICT setahun sekali atau mengikut keperluan.	
13-1-3 Pengesahan, Kajian Dan Penilaian Keselamatan Maklumat	
CGSO hendaklah memeriksa serta mengesahkan secara berkala Pelan Pengurusan Kesinambungan Perkhidmatan yang dibangunkan dan kawalan keselamatan maklumat yang akan dilaksanakan bagi memastikan keberkesanan kawalan ini semasa berlaku bencana atau ancaman. Perkara yang perlu diambil kira adalah seperti berikut: a) Menyenaraikan senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; b) Senarai personel CGSO dan pembekal berserta nombor yang boleh dihubungi (faksimile, telefon dan emel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel yang 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) Menetapkan arahan pemulihan maklumat dan	ICTSO, Pengurus ICT dan Pentadbir Sistem ICT

kemudahan yang berkaitan; e) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; f) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh; g) Salinan pelan pengurusan kesinambungan perkhidmatan perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama; h) Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan; i) Pelan pengurusan kesinambungan perkhidmatan hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan; j) Ujian pelan hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan; dan k) CGSO hendaklah memastikan salinan pelan sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

13-2 REDUNDANCY

Objektif:

Memastikan ketersediaan perkhidmatan dan kemudahan pemprosesan atau sistem maklumat.

13-2-1 Ketersediaan Perkhidmatan Kemudahan Pemprosesan Maklumat

CGSO perlu memastikan pelaksanaan secara pertindihan	ICTSO,

(redundancy) untuk perkhidmatan utama dan kemudahan pemprosesan atau sistem maklumat boleh memenuhi ketersediaan yang ditetapkan. Perkara yang perlu diambil kira adalah seperti berikut: a) Pelan pengurusan kesinambungan perkhidmatan hendaklah diuji bagi memastikan ia sentiasa memenuhi tahap ketersediaan yang ditetapkan; dan b) Melaksanakan pengujian *failover test* untuk menguji tahap ketersediaan sistem maklumat.	Pengurus ICT dan Pentadbir Sistem ICT

BIDANG 14 PEMATUHAN

14-1 PEMATUHAN KEPADA KEPERLUAN PERUNDANGAN DAN KONTRAK

Objektif:

Mencegah pelanggaran obligasi perundangan, undang-undang, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat dan apa-apa keperluan keselamatan.

14-1-1 Mengenalpasti Keperluan Perundangan Dan Perjanjian Kontrak

Semua keperluan undang-undang berkanun, peraturan dan kontrak perjanjian yang berkaitan dengan CGSO perlu ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat. Senarai perundangan dan peraturan yang wajib dipatuhi oleh semua pengguna adalah seperti di **Lampiran 4**.	Semua

14-1-2 Hak Harta Intelek (Intellectual Property Rights – IPR)

Prosedur berkaitan perlu dibangunkan bagi memastikan pematuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelek serta pemilik perisian yang sah. Pengguna perlu mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. Perkara yang perlu dipatuhi adalah seperti berikut: a) Keperluan hak cipta yang berkaitan dengan bahan	Semua

proprietary, perisian dan reka bentuk yang diperoleh melalui CGSO; b) Keperluan pelesenan menghadkan penggunaan produk, perisian, reka bentuk dan bahan-bahan lain yang diperolehi oleh CGSO; c) Pematuhan yang berterusan dengan sekatan hak cipta produk dan keperluan pelesenan; dan d) Perisian atau sistem maklumat yang dibangunkan oleh CGSO adalah menjadi harta intelek CGSO.	
14-1-3 Perlindungan Rekod	
Rekod-rekod yang penting (fizikal atau media) hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, pelepasan yang tidak dibenarkan mengikut undang-undang, peraturan, kontrak dan keperluan perniagaan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat; b) Jadual penyimpanan rekod perlu dikenal pasti; dan c) Inventori rekod.	Semua
14-1-4 Privasi Dan Perlindungan Maklumat Peribadi	
CGSO perlu mengenal pasti privasi dan melindungi maklumat peribadi pengguna adalah terjamin seperti yang tertakluk dalam undang- undang kerajaan Malaysia dan peraturan-peraturan yang berkenaan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Tidak mendedahkan maklumat peribadi pengguna pada mana-mana pihak yang tidak berkaitan; b) Memastikan kawalan penyimpan rekod maklumat peribadi pengguna di tempat yang selamat; dan c) Maklumat peribadi pengguna hanya boleh digunakan	Semua

untuk tujuan rasmi dan dengan kebenaran.	
14-1-5 Peraturan Kawalan Kriptografi	
CGSO perlu memastikan kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang dan peraturan- peraturan. Perkara yang perlu dipatuhi adalah seperti berikut: a) Sekatan ke atas pengimport/pengeksport perkakasan dan perisian komputer yang melaksanakan fungsi-fungsi kriptografi tanpa kelulusan pihak berkuasa; b) Sekatan ke atas pengimport/pengeksport perkakasan dan perisian yang ditambah/direka untuk mempunyai fungsi kriptografi tanpa kelulusan pihak berkuasa; c) Sekatan penggunaan enkripsi yang tidak dibenarkan; dan d) Mematuhi kaedah akses oleh pihak berkuasa Malaysia bagi maklumat enkripsi perkakasan dan perisian.	Semua
14-2 KAJIAN KESELAMATAN MAKLUMAT	
Objektif: Memastikan keselamatan maklumat dilaksanakan dan beroperasi selaras dengan polisi atau prosedur CGSO.	
14-2-1 Kajian Keselamatan Maklumat Oleh Pihak Ketiga Atau Badan Bebas	
CGSO perlu memastikan kaedah pengurusan keselamatan maklumat serta pelaksanaannya seperti objektif kawalan, kawalan, polisi dan prosedur perlu dikaji secara bebas atau oleh pihak ketiga secara berkala atau sekiranya berlaku perubahan yang besar.	CIO, Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
14-2-2 Pematuhan Kepada Dasar Keselamatan Dan Standard	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Pentadbir Sistem ICT perlu memastikan kajian ke atas pematuhan dan prosedur pemprosesan maklumat di	CIO, Pentadbir Sistem ICT, Pengurus ICT

dalam bidang tanggungjawab mereka selaras dengan dasar keselamatan maklumat atau lain-lain keperluan keselamatan; b) Mengenal pasti punca-punca ketidakpatuhan; c) Menilai keperluan tindakan untuk mencapai pematuhan; d) Melaksanakan tindakan pembetulan yang sewajarnya; e) Mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti apa-apa kekurangan dan kelemahan; dan f) Setiap pengguna di CGSO hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT CGSO dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua pengguna dimestikan mengisi borang seperti di **Lampiran 1**.	dan ICTSO
14-2-3 Pematuhan Kajian Teknikal	
Perkara yang perlu dipatuhi adalah seperti berikut: a) Sistem maklumat hendaklah dikaji sekurang-kurangnya setahun sekali atau mengikut keperluan supaya selaras dengan pematuhan dasar dan standard; dan b) Keselamatan sistem maklumat hendaklah dikaji sekurang- kurangnya sekali setahun atau mengikut keperluan.	CIO, Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

DASAR KESELAMATAN ICT PEJABAT KETUA PEGAWAI KESELAMATAN KERAJAAN MALAYSIA

GLOSARI

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh: di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
BYOD	*Bring Your Own Device* (BYOD) Merujuk kepada peranti milik persendirian (komputer riba, tablet dan telefon pintar) yang dibawa oleh warga agensi ke pejabat atau tempat kerja dan menggunakan peranti ini untuk mencapai data, maklumat dan aplikasi CGSO.
CIO	*Chief Information Officer* (CIO) Ketua Pegawai Maklumat yang dilantik adalah bertanggungjawab terhadap ICT serta sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian atau fail.
Encryption	Pemprosesan suatu utusan oleh pengirimnya supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Fasiliti CGSO	Bahagian di Ibu Pejabat CGSO/ Pejabat Negeri/Institut Latihan Keselamatan Perlindungan Malaysia (ILKEM)

Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (*hub*) merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (*broadcast*) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan (*server*) atau komputer lain.
Internet Gateway	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.
***Intrusion Detection System* (IDS)**	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 host atau rangkaian.
LAN	*L*ocal *Area Network* (Rangkaian Kawasan Setempat). Rangkaian Kawasan Setempat yang menghubungkan komputer.

Logout	Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse*, *worm*, *spyware*, *malware* dan sebagainya.
NACSA	Agensi Keselamatan Siber Negara *(National Cyber Security Agency* (NACSA)) Agensi pusat yang bertanggungjawab ke atas semua aspek keselamatan siber bagi memantapkan pengurusan keselamatan siber negara.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perkakasan ICT	Merangkumi semua jenis perkakasan atau peranti elektronik yang diperlukan untuk melaksanakan sesuatu projek ICT iaitu peralatan input/output (contoh: pencetak, pengimbas, alat baca biometrik, Suara Melalui IP (VoIP), pemprosesan, storan data, multimedia [contoh: persidangan video (*video conferencing*)], perkakasan komunikasi mudah alih [contoh: jalur lebar tanpa wayar (*wireless broadband*)] dan perkakasan komunikasi berteknologi tinggi (contoh: radar, satelit).
Perisian ICT	Merangkumi semua jenis perisian sistem, perisian aplikasi dan lesen perisian (pembelian dan pembaharuan). Perisian sistem merangkumi sistem operasi, pangkalan data dan perisian bagi membangunkan sistem. Perisian aplikasi ialah perisian yang digunakan untuk menyokong kerja-kerja harian dalam urusan dan pentadbiran pejabat serta pengajaran dan pembelajaran.
Pihak Ketiga	Kontraktor, Pembekal, Perunding.
***Public-Key Infrastructure* (PKI)**	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan.(Contoh: pencapaian Internet).
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak

	digunakan dalam jangka masa tertentu.
Server	Pelayan komputer.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detectio*n (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu emel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply **(UPS)**	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video Conference	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video Streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN 1 : SURAT AKUAN PEMATUHAN DKICT CGSO

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT

PEJABAT KETUA PEGAWAI KESELAMATAN KERAJAAN MALAYSIA

Nama Penuh
(Huruf Besar) : ……..……..…..

No. Kad
Pengenalan : ……..……..…..

Jawatan : ……..……..…..

Bahagian : ……..……..…..

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

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

Tandatangan : ……..

Tarikh : ……..

Pengesahan Pegawai Keselamatan ICT

……
(Nama Pegawai Keselamatan ICT)
b.p. Ketua Pengarah
Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia

Tarikh :……..…

LAMPIRAN 2 : PERAKUAN AKTA RAHSIA RASMI 1972 (MULA PERKHIDMATAN)

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Saya faham bahawa segala rahsia rasmi dan suratan rasmi yang saya peroleh semasa berurusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan atau menyampaikan, sama ada secara lisan, bertulis atau dengan cara elektronik kepada sesiapa jua dalam apa-apa bentuk, sama ada dalam masa atau selepas berurusan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapatkan kebenaran bertulis daripada pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani satu akuan selanjutnya bagi maksud ini apabila urusan dengan perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia telah selesai.

Tandatangan : _____

Nama (huruf besar) : _____

No. Kad Pengenalan : _____

Jawatan : _____

Jabatan / Organisasi : _____

Tarikh : _____

Disaksikan oleh :

_____

(Tandatangan)

Nama (huruf besar) : _____

No. Kad Pengenalan : _____

Jawatan : _____

Jabatan / Organisasi : _____

Tarikh : _____

Cap Jabatan / Organisasi : _____

LAMPIRAN 3 : PERAKUAN AKTA RAHSIA RASMI 1972 (TAMAT PERKHIDMATAN)

PERAKUAN UNTUK DITANDATANGANI OLEH KOMUNITI KESELAMATAN ATAU MANA-MANA PIHAK LAIN YANG BERURUSAN DENGAN PERKHIDMATAN AWAM ATAU YANG BERKHIDMAT DI KEDIAMAN RASMI KERAJAAN APABILA TAMAT KONTRAK PERKHIDMATAN DENGAN KERAJAAN BERKAITAN DENGAN AKTA RAHSIA RASMI 1972 [AKTA 88]

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 [Akta 88] dan saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah dan tidak menjaga dengan cara yang berpatutan sesuatu rahsia rasmi dan suratan rasmi atau apa-apa tingkah laku yang membahayakan keselamatan atau kerahsiaan sesuatu rahsia rasmi adalah menjadi suatu kesalahan di bawah seksyen 8 Akta tersebut, yang boleh dihukum dengan penjara selama tempoh tidak kurang daripada satu tahun tetapi tidak lebih daripada tujuh tahun.

Dengan ini menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa rahsia rasmi atau suratan rasmi kepada mana-mana orang lain, sama ada atau tidak orang itu memegang jawatan dalam perkhidmatan Seri Paduka Baginda Yang di-Pertuan Agong atau mana-mana Kerajaan Malaysia, dan sama ada di Malaysia atau di negara luar, sebelum dan selepas saya tamat kontrak perkhidmatan dengan Seri Paduka Baginda Yang di-Pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyarat timbal, atau kata laluan rasmi yang rahsia, atau apa-apa benda, suratan atau maklumat, anak kunci, lencana, alat meteri, atau cap bagi atau yang dipunyai, atau diguna, dibuat atau diadakan oleh mana-mana jabatan Kerajaan atau oleh mana-mana pihak berkuasa diplomat yang dilantik oleh atau yang bertindak di bawah kuasa Kerajaan Malaysia atau Seri Paduka Baginda yang tidak dibenarkan berada dalam milikan atau kawalan saya.

Tandatangan : _____

Nama (huruf besar) : _____

No. Kad Pengenalan/ Pasport : _____

Jawatan : _____

Jabatan/Organisasi : _____

Tarikh : _____

Disaksikan oleh : _____

Nama (huruf besar) : _____

(Tandatangan)

No. Kad Pengenalan/ Pasport : _____

Jawatan : _____

Jabatan/Organisasi : _____

Tarikh : _____

Cap Jabatan / Organisasi : _____

LAMPIRAN 4 : SENARAI UNDANG-UNDANG, DASAR DAN PERATURAN

1) Akta Rahsia Rasmi 1972

2) Akta Tandatangan Digital 1997

3) Akta Jenayah Komputer 1997

4) Akta Hak Cipta (Pindaan) Tahun 1997

5) Akta Komunikasi dan Multimedia 1998

6) Akta Arkib Negara 2003 [Akta 629]

7) Akta Arkib Negara 2003 [Akta 629] - Seksyen 27(1) Dan (3) Jadual Pelupusan Rekod

8) Akta Perlindungan Data Peribadi 2010

9) Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan

10) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)

11) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan

12) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam

13) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam

14) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian Dan Sistem ICT Sektor Awam

15) Surat Pekeliling Am Bil 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK)

16) Surat Pekeliling Am Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia Bil 1 Tahun 2016 – Tatacara Pelaksanaan Projek ICT Di Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO)

17) Surat Pekeliling Am Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia Bil 2 Tahun 2016 – Garis Panduan Kesediaan Infrastruktur Teknologi Maklumat Dan Komunikasi (ICT) Di Agensi Dan Fasiliti Pejabat Ketua Pegawai Keselamatan

Kerajaan Malaysia (CGSO)

18) 1Pekeliling Perbendaharaan (1PP) Tahun 2014 – PK Perolehan Kerajaan 2.1 Kaedah Perolehan Kerajaan

19) 1Pekeliling Perbendaharaan (1PP) Tahun 2014 – PS Tadbir Urus Kewangan 2.2 Terimaan Kerajaan Secara Elektronik Melalui Portal Kementerian atau Jabatan

20) Arahan Keselamatan (Semakan dan Pindaan 2017)

21) Arahan Perbendaharaan

22) Arahan Teknologi Maklumat 2007

23) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)

24) *Malaysia Public Sector Management of Information and Communications Technology Security Handbooks* (MyMIS) 2002

25) Perintah-Perintah Am

26) Surat Arahan Ketua Setiausaha Negara – Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-agensi Kerajaan yang bertarikh 20 Oktober 2006

27) Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 1 Jun 2007

28) Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 23 November 2007

29) Surat Arahan Ketua Pengarah MAMPU Tahun 2009 – Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT Di Agensi-Agensi Kerajaan

30) Surat Arahan Ketua Pengarah MAMPU Tahun 2010 – Pemantapan Penggunaan Dan Pengurusan E-mel Di Agensi-Agensi Kerajaan

31) Surat Arahan Ketua Pengarah MAMPU Tahun 2010 – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam

32) Surat Ketua Pengarah Keselamatan Negara, Majlis Keselamatan Negara – Pemakluman Pelaksanaan Fungsi Pengurusan Pengendalian *Government Computer Emergency Response Team (*GCERT) Oleh Agensi Keselamatan Siber Negara (NACSA) yang bertarikh 28 Januari 2019

33) Garis Panduan Keselamatan MAMPU 2004

34) *Standard Operating Procedure* (SOP) ICT

35) Garis Panduan *User Access Control Policy* (UACP), Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia Tahun 2011

PEJABAT KETUA PEGAWAI KESELAMATAN KERAJAAN MALAYSIA, JABATAN PERDANA MENTERI
Aras -1, 1 dan 2, Setia Perdana 7,Kompleks Setia Perdana, Pusat Pentadbiran Kerajaan Persekutuan,
62502 Wilayah Persekutuan Putrajaya.
Telefon: 03-8872 6038 | Faks: 03-8888 3258
Laman web: www.cgso.gov.my | e- mel: kic trr@cgso.gov.my