DASAR KESELAMATAN ICT

KEMENTERIAN WILAYAH PERSEKUTUAN (KWP)

27 MEI 2014

VERSI 4.2

Diterbitkan oleh:

Bahagian Pengurusan Maklumat
Kementerian Wilayah Persekutuan
Aras 2, Blok 2, Menara Seri Wilayah
62100 Presint 2, Putrajaya

TARIKH KUAT KUASA

27 Mei 2014

KATA-KATA ALUAN

Ketua Pegawai Maklumat Kementerian Wilayah Persekutuan

Bismillahirrahmannirahim. Assalamu'alaikum Warahmatullahi Wabarakatuh, Salam Sejahtera dan Salam 1Malaysia.

Menyedari hakikat bahawa keselamatan ICT memerlukan satu aspek kritikal pada masa kini, Dasar Keselamatan ICT (DKCIT) KWP ini diwujudkan bagi memberikan garis panduan yang boleh membantu kakitangan KWP secara khususnya dan Kementerian ini secara amnya dalam memahami keselamatan ICT secara menyeluruh, sesuai dengan kemajuan teknologi ICT terkini.

DKICT ini dirancang serta diwujudkan bagi memperkukuhkan keselamatan ICT dan sebagai panduan kepada seluruh warga Kementerian dalam tugasan seharian. DKICT ini juga diharapkan dapat mewujudkan kesedaran dikalangan warga Kementerian, memahami serta boleh mengaplikasikan aspek keselamatan ICT dalam tugasan dan berupaya untuk menghadapi ancaman keselamatan masa kini.

Adalah merupakan harapan saya semoga DKICT ini dapat dipatuhi oleh seluruh warga Kementerian dan seterusnya dapat melindungi aset Kementerian ini. Akhir kata, marilah kita bersama-sama berusaha berganding bahu dalam memperkukuh keselamatan ICT di Kementerian Wilayah Persekutuan ini.

Sekian, terima kasih.

DATUK HAJI HASIM B. HAJI ISMAIL
Ketua Pegawai Maklumat (CIO)

27 Mei 2014

KATA-KATA ALUAN

Pengurus ICT Kementerian Wilayah Persekutuan

Pewujudan Dasar Keselamatan ICT (DKICT) KWP ini merupakan pematuhan kepada keperluan Dasar Keselamatan ICT sebagaimana ditetapkan oleh MAMPU menerusi Pekeliling Am Bil 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan.

Tujuan DKICT ini adalah untuk memberikan panduan dan kesedaran kepada penggunaan ICT dalam melaksanalan tugas dan tanggungjawab harian. DKICT ini juga memberi penjelasan terperinci mengenai tatacara tadbir urus ICT dan larangan penggunaan ICT.

DKICT ini hendaklah dibaca bersekali dengan Akta, Pekeliling, Surat Pekeliling, Arahan, peraturan dan garis panduan Kerajaan Malaysia yang sedang berkuat kuasa.

Sesungguhnya, DKICT ini tidak akan berjaya disempurnakan tanpa sokongan padu dan kerjasama yang komited daripada ahli-ahli Jawatankuasa Kerja dan urus setia DKICT yang dibentuk, pihak-pihak tertentu serta orang perseorangan yang terlibat sama ada secara langsung atau tidak langsung dalam memberikan kerjasama dan pandangan ke arah penghasilan DKICT ini. Selaras itu, rakaman penghargaan dan ucapan terima kasih yang tidak terhingga kepada semua yang terlibat dalam menjayakan penghasilan dasar ini.

Sekian, terima kasih.

MOHD SORI BIN HUSAIN
Pengurus ICT

27 Mei 2014

KATA-KATA ALUAN

Pegawai Keselamatan ICT (ICTSO) Kementerian Wilayah Persekutuan

Setinggi-tinggi syukur ke hadrat Allah SWT kerana dengan izin-Nya, Dasar Keselamatan ICT (DKICT) KWP ini berjaya dihasilkan. Dasar ini dihasilkan sebagai panduan atau rujukan kepada semua warga Kementerian dalam aspek penggunaan kemudahan dan keselamatan ICT

Dalam membantu warga Kementerian dalam isu keselamatan ICT, Bahagian Pengurusan Maklumat (BPM) sentiasa komited dalam usaha untuk menambahbaik dasar ini dari semasa ke semasa supaya dapat dimanfaatkan sebaiknya. Sebagai usaha awal Kementerian, dasar ini merupakan satu dokumen yang dapat melindungi aset serta warga Kementerian daripada sebarang aktiviti ICT yang tidak bertanggungjawab.

Bagi pihak BPM dan selaku Pegawai Keselamatan ICT (ICTSO), saya ingin merakamkan setinggi-tinggi penghargaan kepada semua yang terlibat di atas usaha dalam menyediakan Dasar Keselamatan ICT (DKCIT) ini. Semoga dasar ini menjadi panduan yang dimanfaatkan dengan sebaik-baiknya oleh semua warga Kementerian.

Sekian, terima kasih

ROZILA BINTI MEGAT OTHMAN
Pegawai Keselamatan ICT (ICTSO)

27 Mei 2014

SEJARAH DOKUMEN

Tarikh	Versi	Kelulusan	Tarikh Kuatkuasa
18 Feb 2012	4.0	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Bil.1/2012	1 Mac 2012
5 Julai 2013	4.1	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Bil.3/2013	19 September 2013
16 Mei 2014	4.2	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Bil.2/2014	27 Mei 2014

JADUAL PINDAAN DASAR KESELAMATAN ICT KWP

Tarikh	Versi	Butiran Pindaan
18 Feb 2012	4.0	i) **Tajuk baru: Penilaian Risiko Keselamatan ICT,** muka surat 14 ii) **Perkara 2 – Penubuhan CERT KWP dan tanggung jawab CERT di dalam menangani insiden keselamatan ICT KWPKB,** muka surat 22 iii) **Semua Perkara – Penyeragaman tanggung jawab selaras dengan penstrukturan semula organisasi KWPKB.**
5 Julai 2013	4.1	i) **Semua perkara – penukaran Kementerian Wilayah Persekutuan dan Kesejahteraan Bandar (KWPKB) kepada Kementerian Wilayah Persekutuan (KWP)** selaras dengan pertukaran nama kementerian daripada Kementerian Wilayah Persekutuan dan Kesejahteraan Bandar kepada Kementerian Wilayah Persekutuan – muka surat berkaitan ii) **Tambahan penyataan versi** – muka surat 8 iii) **Tambahan perkataan Syarikat selepas Bahagian** – mukasurat 80 (Surat Akuan Pematuhan DKICT)

27 Mei 2014	4.2	i) **Perkara 2.1.7.1 (d) Keperluan Keselamatan Kontrak Dengan Pihak Ketiga,** muka surat 21: MAMPU di pinda kepada KWP. ii) **Perkara 5.1.3 (b) Kawasan Larangan**, muka surat 28, pindaan iaitu 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. iii) **Perkara 6.8.2 (a) Pengurusan Mel Elektronik (E-mel),** muka surat 49, pindaan iaitu Akaun atau alamat e-mel yang diperuntukkan oleh KWP sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang kecuali dengan kebenaran oleh pemilik akaun. iv) **Perkara 6.8.2 (n) Pengurusan Mel Elektronik (E-mel)**, muka surat 49, perenggan baru iaitu Bagi pengguna yang telah bertukar jabatan dan bersara, akaun e-mel 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. v) **Perkara 6.8.2 (o) Pengurusan Mel Elektronik (E-mel)**, muka surat 49, perenggan baru iaitu Bagi pengguna yang telah ditamatkan perkhidmatan atau meninggal dunia, akaun e-mel mereka akan ditamatkan serta-merta.

		vi) **Perkara 7.2.1 (f) (i) Akaun Pengguna**, muka surat 55, perenggan tersebut di mansuhkan. vii) **Perkara 7.2.1 (f) (iii) Akaun Pengguna**, muka surat 55, pindaan iaitu Pengguna yang bercuti belajar melebihi tempoh enam (6) bulan seperti mana yang diluluskan oleh Ketua Jabatan; viii) **Perkara 7.2.1 (f) (vii) Akaun Pengguna**, muka surat 55, perenggan baru iaitu Dalam prosiding dan/atau dikenakan tindakan tatatertib; ix) **Perkara 7.2.1 (g) Akaun Pengguna**, muka surat 55, perenggan baru iaitu Akaun hendaklah didaftarkan atau dibatalkan kebenaran menerusi sistem directori; contohnya Active Directory, LDAP atau sebagainya.

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 KWP mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KWP.

OBJEKTIF

Dasar Keselamatan ICT KWP diwujudkan bertujuan untuk:

i. Menjamin kesinambungan urusan KWP dengan meminimumkan kesan insiden keselamatan ICT;

ii. Memudahkan perkongsian maklumat;

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

iv. 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 KWP sehingga kini mempunyai 4 versi seperti berikut:

i. Versi 1.0 – 24 Ogos 2007
ii. Versi 2.0 – 1 Mac 2010
iii. Versi 3.0 – 29 April 2010
iv. Versi 4.0 – 1 Mac 2012
v. Versi 4.1 – 5 Julai 2013
vi. Versi 4.2 – 27 Mei 2014

Penambah baikan versi ini selaras dengan sebarang penambahan / pertukaran maklumat dan di bentang dan dilulus di dalam Mesyuarat Pengurusan Atasan.

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

i. Kerahsiaan – Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses 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 diakses pada bila- bila masa.

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

SKOP

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

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

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 KWP ini merangkumi perlindungan semua bentuk maklumat Kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dijana, dicetak, diakses, diedarkan, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan 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 KWP. (Contoh : 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 di simpan di dalam sistem ICT. (Contoh : 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. (Contoh : 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 KWP. (Contoh : Sistem dokumentasi, prosedur operasi, rekod-rekod, profil pelanggan, pangkalan data dan fail-fail data, maklumat- maklumat arkib dan lain-lain);

v. Manusia

Individu yang mempunyai pengetahuan dan kemahiran dalam melaksanakan skop kerja harian KWP 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 dianggar sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT KWP 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 askes hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat. seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

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, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke samasa berdasarkan kepada peranan dan tanggungjawab pengguna/bidang tugas;

iii. Akauntabiliti

Semua pengguna adalah bertanggunjawab ke atas semua tindakannya terhadap aset ICT KWP. 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 untukmengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

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

vi. Pematuhan

Dasar Keselamatan ICT KWP 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 sama 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

KWP hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu KWP 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.

KWP 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 KWP 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.

KWP 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.

KWP 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 pihaklain yang berkepentingan.

PERKARA 1 : PEMBANGUNAN DAN PENYELARASAN DASAR

1.1 DASAR KESELAMATAN ICT	
Objektif : Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan KWP dan perundangan yang berkaitan.	
1.1.1 Pelaksanaan Dasar	
Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha KWP dibantu oleh Pasukan Pengurusan Keselamatan ICT yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), Setiausaha Bahagian dan semua Ketua Bahagian.	Ketua Setiausaha
1.1.2 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna KWP termasuk pegawai, kakitangan, pembekal, pakar runding dan lain- lain.	ICTSO
1.1.3 Penyelenggaraan Dasar	
Dasar Keselamatan ICT KWP 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 KWP: (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KWP; (c) Perubahan yang telah dipersetujui oleh JPICT hendaklah dimaklumkan kepada semua pengguna; dan (d) Dasar ini hendaklah dikaji semula sekurang- kurangnya sekali setahun	ICTSO
1.1.4 Pengecualian Dasar	
Dasar Keselamatan ICT KWP adalah terpakai kepada semua pengguna ICT KWP dan tiada pengecualian diberikan.	Semua

PERKARA 2 : ORGANISASI KESELAMATAN

2.1 INFRASTRUKTUR ORGANISASI KESELAMATAN

Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.

2.1.1 Ketua Setiausaha KWP

Peranan dan tanggungjawab Ketua Setiausaha adalah seperti berikut: (a) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT KWP; (b) Memastikan semua pengguna mematuhi Dasar Keselamatan ICT KWP; (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT KWP; dan (e) Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), KWP.	Ketua Setiausaha

2.1.2 Ketua Pegawai Maklumat (CIO)

Timbalan Ketua Setiausaha Operasi KWP adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut: (a) Membantu Ketua Setiausaha dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Menentukan keperluan keselamatan ICT; (c) Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan Dasar Keselamatan ICT KWP; dan (d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT KWP.	CIO

2.1.3 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Mengurus keseluruhan program-program keselamatan ICT KWP; (b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT KWP; (c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT KWP kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT KWP; (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 Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU 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; (j) Menyedia dan melaksanakan program – program kesedaran mengenai keselamatan ICT.	ICTSO
2.1.4 Pengurus ICT	
Ketua Bahagian Pengurusan Maklumat adalah merupakan Pengurus ICT KWP. Peranan dan tanggungjawab Pengurus Komputer adalah seperti berikut: (a) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan KWP; (b) Menentukan kawalan akses semua pengguna terhadap aset ICT KWP; (c) Melaporkan sebarang perkara atau penemuan mengenai	Pengurus ICT

keselamatan ICT kepada ICTSO; dan (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT, KWP.	
2.1.5 Pentadbir Sistem ICT	
Pegawai Teknologi Maklumat (Seksyen Pembangunan Aplikasi & Multimedia dan Seksyen Rangkaian & Keselamatan) adalah merupakan Pentadbir Sistem ICT KWP. Peranan dan tanggungjawab pentadbir sistem ICT adalah seperti berikut: (a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; (b) Menentukan ketetapan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan milik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT KWP; (c) Memantau aktiviti capaian harian pengguna; (d) Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (e) Menyimpan dan menganalisis rekod jejak audit; (f) Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; dan (g) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan baik.	Pentadbir Sistem ICT
2.1.6 Pengguna	
Peranan dan tanggungjawab pengguna adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT KWP; (b) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat	Pengguna

(d) Melaksanakan prinsip – prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat KWP; (e) Melaksanakan langkah-langkah perlindungan seperti berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. (f) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (g) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan (h) Menandatangani surat akuan pematuhan Dasar Keselamatan ICT KWP seperti di **Lampiran A**.	
2.1.7 Pihak Ketiga	
Objektif: Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain). **2.1.7.1 Keperluan Keselamatan Kontrak Dengan Pihak Ketiga** Ini bertujuan untuk memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara – perkara yang perlu dipatuhi adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT KWP; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

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 KWP perlu berlandaskan kepada perjanjian kontrak; (e) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara – perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai: i. Dasar Keselamatan ICT KWP; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; iv. Hak Harta Intelek; (f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan KWP seperti di **Lampiran A.**	
2.1.8 Pasukan Tindak Balas Insiden Keselamatan ICT (CERT) KWP	
Peranan dan tanggungjawab CERT KWP 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 KWP mengambil tindakan pemulihan dan pengukuhan; (e) Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada KWP; 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.	CERT KWP

PERKARA 3 : PENGURUSAN ASET

3.1 AKAUNTABILITI ASET	
Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KWP	
3.1.1 Inventori Aset ICT	
Ini bertujuan untuk memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing- masing. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkodkan dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini; (b) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (c) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di KWP (d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumenkan dan dilaksanakan; dan (e) Setiap pengguna adalah bertanggungjawab keatas semua aset ICT di bawah kawalannya.	Pentadbir Sistem dan Semua
3.2 PENGELASAN DAN PENGENDALIAN MAKLUMAT	
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
3.2.1 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan sebagaimana yang telah ditetapkan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad	Semua

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

PERKARA 4 : KESELAMATAN SUMBER MANUSIA

4.1. KESELAMATAN SUMBER MANUSIA DALAM TUGAS SEHARIAN

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

4.1.1 Sebelum Perkhidmatan

Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan KWP serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan KWP serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang ditetapkan.	Semua

4.1.2 Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut : (a) Memastikan pegawai dan kakitangan KWP serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh KWP; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT KWP secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan/atau	Semua

undang-undang ke atas pegawai dan kakitangan KWP serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan oleh KWP; dan (d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	
4.1.3 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi adalah (a) Memastikan semua aset ICT yang dikembalikan kepada KWP mengikut peraturan dan / atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh KWP dan / atau terma perkhidmatan.	Semua

PERKARA 5 : KESELAMATAN FIZIKAL DAN PERSEKITARAN

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

(l) Memastikan kawasan – kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
5.1.2 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna KWP hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan balik kepada KWP apabila pengguna berhenti atau bersara; (c) Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di pintu kawalan utama KWP. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (d) Kehilangan pas mestilah dilaporkan dengan segera.	Semua
5.1.3 Kawasan 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; dan (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.	Semua
5.2 KESELAMATAN PERALATAN	
Objektif : Melindungi peralatan ICT KWP dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
5.2.1 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna;	Semua

(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 menanggalkan atau mengganti sebarang perkakasan ICT yang telah ditetapkan;	
(d)	Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;	
(e)	Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;	
(f)	Pengguna mesti memastikan perisian 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;	
(h)	Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;	
(i)	Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS);	
(j)	Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, hub, router* dan lain-lain perlu diletakkan dalam rak khas dan berkunci;	
(k)	Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai;	
(l)	Peralatan ICT yang hendak dibawa keluar dari premis KWP, perlulah mendapat kelulusan Pentadbir Sistem ICT dan direkodkan bagi tujuan pemantauan;	
(m)	Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;	

(n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; (o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT; (p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk baik pulih; (q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (r) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (s) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir *(administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT; (t) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (u) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan *OFF* apabila meninggalkan pejabat; (v) Sebarang bentuk penyelewengan atau salah guna hendaklah dilaporkan kepada ICTSO; dan (w) Memastikan plag dicabut daripada suis utama *(main switch)* bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
5.2.2 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk, flash disk*, *CDROM*, *thumb drive* dan media storan lain. Media storan perlu dipastikan berada dalam keadaan baik, selamat, terjamin kerahsiaan, integriti dan	Semua

kesediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan, bersesuaian dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan media storan adalah terhad kepada pengguna yang dibenarkan sahaja; (c) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; (e) Akses dan pergerakan media storan hendaklah direkodkan; (f) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; (g) Mengadakan salinan atau penduaan *(backup)* pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; (h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan (i) Penghapusan maklumat dan kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
5.2.3 Media Tandatangan Digital	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan (c) Sebarang insiden kehilangan yang berlaku hendaklah	Semua

dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	
5.2.4 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan KWP; (b) Sistem aplikasi dalaman tidak dibenarkan untuk di demonstrasi dan diagihkan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; (c) Lesen perisian(*registration code, serials, CD-keys)* perlu disimpan berasingan daripada *CDROM*, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan (d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua
5.2.5 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kesediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran	Semua

daripada Pengurus ICT.	
5.2.6 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis KWP adalah terdedah kepada pelbagai risiko. Perkara – perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri – ciri keselamatan yang bersesuaian.	Semua
5.2.7 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh KWP atau ditempatkan di KWP. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya semua maklumat tidak terlepas dari kawalan KWP. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding* atau pembakaran; (b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; (c) Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (d) Pegawai Aset ICT hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (e) Peralatan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan	Semua

tersebut;

(f) Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori MyAsset;

(g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan

(h) Pengguna ICT adalah dilarang sama sekali daripada melakukan perkara-perkara seperti berikut:

i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggalkan 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 ke mana- mana bahagian di KWP;

iii. Memindah keluar dari KWP mana-mana peralatan ICT yang hendak dilupuskan;

iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan adalah di bawah tanggung jawab KWP; dan

v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *thumb drive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang dilupuskan.

5.3 KESELAMATAN PERSEKITARAN

Objektif : Melindungi aset ICT KWP daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

5.3.1 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, perkara- perkara berikut hendaklah dipatuhi: (a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; (b) Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; (c) Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; (d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; (e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; (f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; (g) Semua peralatan perlindungan hendaklah disemak sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan (h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	Semua
5.3.2 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara- perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah	Semua

disalurkan kepada peralatan ICT; (b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana *(generator)* boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan (c) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	
5.3.3 Kabel	
Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat terdedah. Langkah-langkah keselamatan yang perlu diambil bagi adalah seperti berikut: (a) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (b) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (c) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Semua
5.2.4 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk Garis Panduan Keselamatan yang telah ditetapkan; dan (b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan yang dilantik mengikut aras.	Semua
5.4 KESELAMATAN DOKUMEN	
Objektif : Melindungi maklumat KWP dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	

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

PERKARA 6 : PENGURUSAN OPERASI DAN KOMUNIKASI

6.1 PENGURUSAN PROSEDUR OPERASI

Objektif : Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

6.1.1 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur pengurusan operasi yang diwujudkan, dikenalpasti 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) Semua prosedur hendaklah dikemas kini dari semasa ke semasa mengikut keperluan.	Semua

6.1.2 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur hendaklah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggarakan, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan ; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua

6.1.3 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (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 terperingkat atau dimanipulasikan; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pengurus ICT dan ICTSO

6.2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PIHAK KETIGA	
Objektif : Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
6.2.1 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa (c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikan sistem dan proses yang terlibat serta penilaian semula risiko.	Semua

6.3 PERANCANGAN DAN PENERIMAAN SISTEM	
Objektif : Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
6.3.1 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang.	Pentadbir Sistem ICT dan ICTSO
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.	
6.3.2 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemaskini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT dan ICTSO
6.4 PERISIAN BERBAHAYA	
Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, trojan dan sebagainya.	
6.4.1 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; (d) Mengemaskini anti virus dengan *pattern* anti virus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;	Semua

(f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (g) 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; (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (i) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
6.4.2 Perlindungan dari *Mobile Code*	
(a) Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua
6.5 HOUSEKEEPING	
Objektif : Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
6.5.1 Backup	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; (c) Menguji sistem*backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (d) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan (e) Merekodkan dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Semua

6.6 PENGURUSAN RANGKAIAN

Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan

6.6.1 Kawalan Infrastruktur Rangkaian

Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Sistem ICT; (f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan KWP; (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; (h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh atau aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat KWP; (i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan KWP adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian KWP sahaja dan penggunaan modem adalah dilarang sama sekali; dan	Pentadbir Sistem ICT dan ICTSO

(l) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatannya.	

6.7 PENGURUSAN MEDIA

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

6.7.1 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua
6.7.2 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Mengehadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Menyimpan semua media di tempat yang selamat; (f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Semua
6.7.3 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan sistem dokumentasi; (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Semua

6.8 PENGURUSAN PERTUKARAN MAKLUMAT

Objektif : Memastikan keselamatan pertukaran maklumat dan perisian antara KWP dan agensi luar terjamin.

6.8.1 Pertukaran Maklumat

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian antara KWP dengan agensi luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KWP; (d) Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua

6.8.2 Pengurusan Mel Elektronik (E-mel)

Penggunaan e-mel di KWP hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etikan penggunaan e-mel dan internet yang terkandung dalam pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk: Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan, dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: (a) Akaun atau alamat e-mel yang diperuntukkan oleh KWP sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang kecuali dengan kebenaran oleh pemilik akaun; (b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan; (c) Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;	Semua

(d)	Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat penerima e-mel adalah betul;	
(e)	Pengguna dinasihatkan menggunakan fail yang dikepilkan, sekiranya perlu tidak melebihi sepuluh megabait (10MB) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;	
(f)	Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;	
(g)	Pengguna hendaklah mengenalpasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;	
(h)	Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan;	
(i)	E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;	
(j)	Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;	
(k)	Mengambil tindakan dan memberi maklumbalas terhadap e-mel dengan cepat dan mengambil tindakan segera;	
(l)	Pengguna hendaklah memastikan alamat e-mel persendirian tidak boleh digunakan untuk tujuan rasmi; dan	
(m)	Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	
(n)	Bagi pengguna yang telah bertukar jabatan dan bersara, akaun e-mel 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;	
(o)	Bagi pengguna yang telah ditamatkan perkhidmatan atau meninggal dunia, akaun e-mel mereka akan ditamatkan serta-merta.	

6.9 PERKHIDMATAN E-DAGANG (ELECTRONIC COMMERCE SERVICES)	
Objektif : Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
6.9.1 E-Dagang	
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat Kerajaan untuk mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan ; (b) Maklumat yang terlibat dalam transaksi dalam talian *(online)* perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Semua
6.9.2 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; (b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (c) Memastikan segala maklumat yang hendak dipaparkan telah disahkan dan diluluskan sebelum dimuat naik ke laman web.	Semua

6.10 PEMANTAUAN	
Objektif : Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
6.10.1 Pengauditan dan Forensik ICT	
ICTSO hendaklah bertanggungjawab merekodkan dan menganalisis perkara-perkara berikut: (a) Sebarang cubaan pencerobohan kepada sistem ICT KWP; (b) Serangan kod perosak *(malicious code)*, halangan pemberian perkhidmatan *(denial of service), spam,* pemalsuan *(forgery, phishing)*, pencerobohan *(intrusion)*, ancaman *(threats)* dan kehilangan fizikal *(physical loss)*; (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan dan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti Kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar *(bandwidth)* rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel; dan (h) Aktiviti penukaran maklumat IP (IP address) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	ICTSO
6.10.2 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekodkan aktiviti- aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi ; (b) Maklumat jejak audit mengandungi kredit pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan;	Pentadbir Sistem ICT

(c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan dalam tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
6.10.3Sistem Log	
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT
6.10.4Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; (b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala; (c) Kemudahan merekodkan dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak	Pentadbir Sistem ICT

	dibenarkan; (d) Aktiviti pentadbiran dan operator sistem perlu direkodkan; (e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan (f) Waktu yang berkaitan dengan pemprosesan maklumat dalam KWP atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

PERKARA 7 : KAWALAN CAPAIAN

7.1 DASAR KAWALAN CAPAIAN

Objektif : Mengawal capaian ke atas maklumat.

7.1.1 Keperluan 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-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Kawalan ke atas kemudahan pemprosesan maklumat.	Pentadbir Sistem ICT, ICTSO, Pengurus ICT

7.2 PENGURUSAN CAPAIAN PENGGUNA

Objektif : Mengawal capaian pengguna ke atas aset ICT KWP

7.2.1 Akaun Pengguna

Setiap pengguna adalah bertanggungjawab kepada sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh KWP sahaja yang boleh digunakan; (b) Akaun pengguna mestilah unik dan mencerminkan identiti pengguna; (c) Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT	Semua dan Pentadbir Sistem ICT

terlebih dahulu; (d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan KWP. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan (f) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut: i. Pengguna 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; atau vi. Ditamatkan perkhidmatan. vii. Dalam prosiding dan/atau dikenakan tindakan tatatertib; (g) Akaun hendaklah didaftarkan atau dibatalkan kebenaran menerusi sistem directori; contohnya Active Directory, LDAP atau sebagainya.	
7.2.2 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
7.2.3 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang telah ditetapkan seperti berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromikan; (c) Panjang kata laluan mestilah sekurang- kurangnya dua	Semua dan Pentadbir Sistem ICT

belas (12) aksara dengan gabungan aksara, angka dan aksara khusus; Tiada pengecualian kepada mana-mana server. Lain-lain kata laluan : 8-12 aksara (d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; (e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (f) Katalaluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan dalam program; (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; Sesi ditamatkan selepas had masa melahu (idle) selama lima (5) minit atau mengikut kesesuaian sistem. (j) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan (k) Mengelakkan penggunaan semula kata laluan yang baru digunakan.	
7.2.4 Clear Desk dan Clear Screen	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *ClearDesk dan ClearScreen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer;	Semua

(b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	

7.3 KAWALAN CAPAIAN RANGKAIAN

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

7.3.1 Capaian Rangkaian

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

7.3.2 Capaian Internet

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan internet di KWP hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian KWP; (b) Kaedah *Content Filtering* mestlah digunakan bagi mengawal akses internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (c) Penggunaan teknologi *(packet shaper)* untuk mengawal aktiviti seperti *video conferencing, video streaming, chat, downloading,* adalah perlu bagi menguruskan penggunaan jalur lebar *(bandwidth)*, yang maksimum dan lebih berkesan; (d) Penggunaan internet hanyalah untuk kegunaan rasmi sahaja.	Pentadbir Rangkaian Pengurus ICT Semua

	Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan internet atau sebaliknya;	
(e)	Laman yang dilayari hendaklah hanya berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/pegawai yang diberi kuasa;	
(f)	Bahan yang diperoleh dari internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber internet hendaklah dinyatakan;	
(g)	Bahan rasmi hendaklah disemak dan mendapat pengesahan sebelum dimuat naik ke internet;	
(h)	Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar di bawah hakcipta terpelihara;	
(i)	Sebarang bahan yang dimuat turun dari internet hendaklah digunakan untuk tujuan yang dibenarkan oleh KWP sahaja;	
(j)	Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;	
(k)	Penggunaan modem untuk tujuan sambungan ke internet tidak dibenarkan sama sekali; dan Penggunaan peranti capaian rangkaian peribadi ke internet secara terus (broadband/modem/handphone dll) tidak dibenarkan sama sekali.	
(l)	Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	

7.4 KAWALAN CAPAIAN SISTEM PENGOPERASIAN

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

7.4.1 Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: (a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan (b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (a) Mengesahkan pengguna yang dibenarkan; (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan (c) Menjana amaran *(alert)* sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Mengawal dan mengehadkan penggunaan program; dan (d) Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	Pentadbir Sistem ICT dan ICTSO

7.4.2 Kad Pintar

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan;	Semua

(b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (c) Perkongsian kad pintar untuk sebarang capaian adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan (d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Bahagian Pengurusan Maklumat, KWP.	

7.5 KAWALAN CAPAIAN APLIKASI DAN MAKLUMAT

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

7.5.1 Capaian Aplikasi dan Maklumat

Bertujuan untuk melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); (c) Mengehadkan capaian sistem dan aplikasi kepada lima (5) kali percubaan atau bersesuaian. Sekiranya gagal, akaun pengguna akan disekat; (d) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan (e) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem ICT dan ICTSO

7.6 PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH	
Objektif : Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
7.6.1 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua
7.6.2 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua

PERKARA 8 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

8.1 KESELAMATAN DALAM MEMBANGUNKAN SISTEM

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

8.1.1 Keperluan Keselamatan Sistem Maklumat

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

8.1.2 Pengesahan Data Input dan Output

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan (b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem dan Pentadbir Sistem ICT

8.2 KAWALAN KRIPTOGRAFI	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
8.2.1 Enkripsi	
Pengguna hendaklah membuat enkripsi *(encryption)* ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
8.2.2 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua
8.2.3 Pengurusan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua
8.3 KESELAMATAN FAIL SISTEM	
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
8.3.1 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; (c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan (e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem dan Pentadbir Sistem ICT

8.4 KESELAMATAN DALAM PROSES PEMBANGUNAN DAN SOKONGAN	
Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
8.4.1 Prosedur Kawalan Perubahan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (d) Akses kepada kod sumber aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan (e) Menghalang sebarang peluang untuk membocorkan maklumat.	Pemilik Sistem dan Pentadbir Sistem ICT
8.4.2 Pembangunan Perisian Secara *Outsource*	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem. Kod sumber bagi semua aplikasi dan perisian adalah menjadi hak milik KWP.	Pentadbir Sistem ICT
8.5 KAWALAN TEKNIKAL KETERDEDAHAN *(VULNERABILITY)*	
Objektif : Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
8.5.1 Kawalan dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan;	Pentadbir Sistem ICT

(b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	

PERKARA 9 : PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

9.1 MEKANISME PELAPORAN INSIDEN KESELAMATAN	
Objektif : Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.	
9.1.1 Mekanisme Pelaporan	
Insiden keselamatan ICT bermaksud musibah yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin satu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan GCERT MAMPU dengan kadar segera: (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak- pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. 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.	Semua

9.2 PENGURUSAN MAKLUMAT INSIDEN KESELAMATAN ICT	
Objektif : Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
9.2.1 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KWP. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	ICTSO

PERKARA 10 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

10.1 DASAR KESINAMBUNGAN PERKHIDMATAN	
Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
10.1.1 Pelan Kesinambungan Perkhidmatan	
Pelan Kesinambungan Perkhidmatan (*Busniess Continuity Management*–BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Perkara-perkara berikut perlu diberi perhatian: (a) Mengenalpasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Mengenalpasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; (c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (d) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (f) Membuat *backup*; dan (g) Menguji dan mengemas kini pelan sekurang- kurangnya setahun sekali. Pelan BCM perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;	Pengurus ICT

(b) Senarai personel KWP dan pembekal berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). 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) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh. Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. KWP hendaklah memastikan salinan pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

PERKARA 11 : PEMATUHAN

11.1 PEMATUHAN DAN KEPERLUAN PERUNDANGAN	
Objektif : Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT KWP .	
11.1.1 Pematuhan Dasar	
Setiap pengguna di KWP hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT KWP dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua pengguna dimestikan mengisi borang **Lampiran 1**. Semua aset ICT di KWP termasuk maklumat yang disimpan adalah hak milik Kerajaan. Ketua Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT KWP selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber KWP.	Semua
11.1.2 Pematuhan Dengan Dasar, Piawaian dan Keperluan Teknikal	
ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO
11.1.3 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua

11.1.4Keperluan Perundangan	
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di KWP: (a) Arahan Keselamatan; (b) Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar KeselamatanTeknologi Maklumat dan Komunikasi Kerajaan; (c) *Malaysia Public Sector Management of Information and Communications Technology Security Handbooks* (MyMIS) 2002; (d) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); (e) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan; (f) Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; (g) Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; (h) 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; (i) Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 1 Jun 2007; (j) Surat Arahan Ketua Pengarah MAMPU – Langkah-langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-agensi Kerajaan yang bertarikh 23 November 2007; (k) Surat Pekeliling Am Bil 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK)	Semua

(l) Surat Pekeliling Perbendaharaan Bil 2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender; (m) Surat Pekeliling Perbendaharaan Bil 3/1995 – Peraturan Perolehan Perkhidmatan Perundingan; (n) Akta Tandatangan Digital 1997; (o) Akta Rahsia Rasmi 1972; (p) Akta Jenayah Komputer 1997; (q) Akta Hak Cipta (Pindaan) Tahun 1997; (r) Akta Komunikasi dan Multimedia 1998; (s) Perintah-perintah Am; (t) Arahan Perbendaharaan; (u) Arahan Teknologi Maklumat 2007; (v) Garis Panduan Keselamatan MAMPU 2004; (w) Standard *Operating Procedure* (SOP) ICT MAMPU.	
11.1.5Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT KWP boleh dikenakan tindakan tatatertib.	Semua

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.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
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.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
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 e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).

GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
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	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out* komputer 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* dan sebagainya.
MODEM	Modulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi- fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
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. Contohnya, 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 Detection* (CSMA/CD) yang merupakan satu protokol penghantaran dengan mengurangkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel 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
DASAR KESELAMATAN ICT KWP

Nama (Huruf Besar) : ……..

No. Kad Pengenalan : ……..

Jawatan : ……..

Bahagian/ Syarikat : ……..

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT KWP; dan
2. Jika saya ingkar atau melanggar mana-mana 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 Setiausaha KWP
Tarikh : …….