KEMENTERIAN
WILAYAH
PERSEKUTUAN

DASAR KESELAMATAN ICT (DKICT)

Versi 5.1

12 DISEMBER 2017

KEMENTERIAN WILAYAH PERSEKUTUAN

DASAR KESELAMATAN ICT

KEMENTERIAN WILAYAH PERSEKUTUAN (KWP)

12 Disember 2017

VERSI 5.1

Diterbitkan oleh:

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

TARIKH KUAT KUASA

12 Disember 2017

KATA-KATA ALUAN

Ketua Pegawai Maklumat (CIO), Kementerian Wilayah Persekutuan

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

Dasar Keselamatan ICT (DKICT), Kementerian Wilayah Persekutuan (KWP) kini melangkah masuk ke versi 5.1 yang berteraskan kepada 14 domain ISO/IEC 27001:2013 *Information Security Management Systems (ISMS)* dan kesemuanya adalah mengenai keselamatan maklumat yang perlu diberikan perhatian. Menerusi domain ini juga, KWP berhasrat untuk memastikan keselamatan peralatan ICT sentiasa terjamin selain meningkatkan kesedaran mengenai tanggungjawab pengguna KWP ke atas keselamatan maklumat.

Menyedari hakikat bahawa arus perkembangan ICT yang begitu pesat berkembang pada masa kini, KWP sentiasa menambahbaik Dasar Keselamatan ICT (DKICT) dari semasa ke semasa bagi memastikan ia selari dengan kemajuan teknologi ICT.Langkah penambahbaikan ini juga selaras dengan Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) dan Pekeliling Am Bil. 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan".

Dengan penambahbaikan DKICT ini juga, KWP dapat meningkatkan keselamatan maklumat, mewujudkan kesedaran dikalangan pengguna, memahami serta boleh mengaplikasikan aspek keselamatan ICT dalam tugasan dan pematuhan dalam prosedur keselamatan ICT supaya berupaya untuk mengekang ancaman keselamatan ICT masa kini.

Akhir kata, tahniah dan syabas diucapkan kepada Bahagian Pengurusan Maklumat (BPM), KWP serta semua pihak yang telah berusaha bagi merealisasikan DKICT versi 5.1 ini. Semoga dengan penambahbaikan DKICT versi 5.1 ini akan dapat mempertingkatkan aspek pengurusan keselamatan ICT dan seterusnya melindungi peralatan ICT Kementerian ini. Semoga usaha ini disokong oleh semua pengguna di KWP dengan pematuhan kepada DKICT versi 5.1.

Sekian, terima kasih.

DATUK HAJAH ROSIDA BINTI JAAFAR
Ketua Pegawai Maklumat (CIO)

KATA-KATA ALUAN

Pengurus ICT, Kementerian Wilayah Persekutuan

Assalamu'alaikum Warahmatullahi Wabarakatuh dan Salam Sejahtera.

Alhamdulillah, segala puji bagi Allah di atas izin-Nya, saya ingin mengucapkan tahniah di atas usaha semua pihak yang terlibat dalam menghasilkan penambahbaikan Dasar Keselamatan ICT (DKICT) versi 5.1, Kementerian Wilayah Persekutuan (KWP).

Menjadi hasrat BPM, dengan penambahbaikan DKICT ini, dapat meningkatkan keberkesanan dan kecekapan sistem penyampaian melalui perkhidmatan ICT. Disamping pengurusan keselamatan ke atas peralatan ICT Kementerian seperti data, peralatan, rangkaian dan perkhidmatan dapat dilindungi pada tahap yang optimum.

Sejajar dengan kemajuan teknologi ICT yang begitu pesat berkembangan masa kini, pengguna ICT tidak terlepas dengan serangan siber. Antara bentuk ancaman yang sering berlaku adalah pencerobohan, pemalsuan (*forgery*), penghalangan capaian perkhidmatan (*Denial of Servie*), mel sampah (*spam*), kod jahat (*malicious code*) dan pelbagai bentuk ancaman yang boleh mengganggu keselamatan maklumat. Oleh itu, soal keselamatan ICT terutamanya berkaitan data dan maklumat memerlukan mekanisme pengurusan yang sistematik serta ditambahbaik dari semasa ke semasa.

Selaras dengan tujuan di atas, semoga penambahbaikan DKICT ini dapat dijadikan sebagai panduan kepada warga KWP dan memberikan pendedahan mengenai kaedah penggunaan ICT yang selamat dan insiden keselamatan ICT dapat diminimakan. Setinggi-tinggi penghargaan dan ucapan tahniah atas kerjasama daripada ahli-ahli Jawatankuasa Kerja dan urus setia DKICT, pihak-pihak tertentu serta orang perseorangan yang terlibat secara langsung atau tidak langsung dalam memberikan kerjasama dan pandangan ke arah penambahbaikan DKICT ini.

Sekian, terima kasih.

WAN ROSHIDAH BINTI WAN ISMAIL
Pengurus ICT

KATA-KATA ALUAN

Pegawai Keselamatan ICT (ICTSO) Kementerian Wilayah Persekutuan

Assalamu'alaikum Warahmatullahi Wabarakatuh dan Salam Sejahtera.

Segala puji bagi Allah Subhanahu Wata'ala Tuhan sekalian alam, selawat dan salam ke atas junjungan besar Nabi Muhammad Sallallahu 'alaihi wasallam. Dengan izin-Nya, penambahbaikan Dasar Keselamatan ICT (DKICT) KWP versi 5.1 ini berjaya direalisasikan dan sebagai panduan serta rujukan kepada semua pengguna KWP dalam aspek keselamatan ICT.

Terlebih dahulu, saya mengucapkan terima kasih kepada semua pihak yang telah menjayakan penghasilan DKICT versi 5.1 ini. Penambahbaikan ini merupakan salah satu usaha dan inisiatif berterusan daripada BPM dalam memastikan isu keselamatan ICT dapat ditangani serta diperkukuhkan pada setiap masa. Bahagian Pengurusan Maklumat (BPM) sentiasa komited dalam usaha untuk menambahbaik DKICT ini supaya dapat dimanfaatkan sebaiknya. Selain itu, DKICT ini merupakan satu dokumen yang dapat melindungi aset serta pengguna KWP daripada sebarang insiden keselamatan ICT.

Sebagai pengakhir kata, selaku Pegawai Keselamatan ICT (ICTSO), diharapkan supaya DKICT ini dapat dijadikan sebagai gerbang panduan kepada pengurusan keselamatan ICT bagi seluruh pengguna KWP selaras dengan hasrat Kerajaan untuk melindungi aset dan maklumat daripada pendedahan yang tidak dibenarkan.

Sekian, terima kasih

TENGKU NATRA BINTI TENGKU AWANG
Pegawai Keselamatan ICT (ICTSO)

SEJARAH DOKUMEN

Tarikh Kajian Semula	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
4 Ogos 2016	5.0	Mesyuarat Pagi KSU Bil. 24 / 2016	10 Ogos 2016
8 Ogos 2017	5.1	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Bil.3/2017	12 Disember 2017

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 direktori; contohnya Active Directory, LDAP atau sebagainya.
10 Ogos 2016	5.0	Perubahan keseluruhan struktur isi kandungan selaras dengan ISO/IEC 27001:2013 *Information Security Management Systems.*
8 Ogos 2017	5.1	i. **Kata-kata Aluan**, muka surat 3, 4 dan 5 : Perubahan CIO dan ICTSO KWP ii. **Perkara 2.1.1 – Peranan dan Tanggungjawab Organisasi Keselamatan Maklumat**, muka surat 27: Pindaan Nama Sektor pada column CIO bagi Timbalan Ketua Setiausaha Operasi KWP kepada Timbalan Ketua Setiausaha (Pengurusan dan Sosio Ekonomi).

		iii. **Perkara 2.1.1 – Peranan dan Tanggungjawab Organisasi Keselamatan Maklumat**, muka surat 29: Pindaan Nama Seksyen pada column Pentadbir Sistem ICT dari (Seksyen Pembangunan Aplikasi & Multimedia dan Seksyen Rangkaian & Keselamatan) kepada (Seksyen Aplikasi & Laman Web dan Seksyen Infrastruktur & Keselamatan). iv. **Perkara 2.1.2 – Pengasingan Peranan dan Tanggungjawab**, muka surat 32: perenggan baru (d) Capaian ke pelayan (server) perlu diasingkan antara pengguna dan pentadbir bagi mengelakkan berlaku pengubahsuaian yang tidak dibenarkan. v. **Perkara 3.2.2 – Pembudayaan Latihan dan Sesi Kesedaran,** muka surat 36: perenggan baru pada (b) hebahan menerusi emel atau desktop wallpaper. vi. **Perkara 4.1.3 – Penggunaan Aset ICT,** muka surat 37: perenggan baru (c) Setiap pengguna perlu menanggung kos pembaikan aset ICT sekiranya BPM mendapati kerosakan yang berlaku disebabkan oleh kecuaian. (d) Takrifan kecuaian pengguna adalah kegagalan mematuhi peraturan yang disengajakan, kegagalan penyeliaan atau penjagaan aset dan pengesahan oleh pihak ketiga berkaitan punca kerosakan akibat kecuaian. vii. **Perkara 4.1.4 – Pemulangan Aset ICT,** muka surat 38: pindaan pada para (c) Nota Serah Tugas atau borang yang berkaitan.

		viii. **Perkara 4.3.3 – Penghantaran dan Pemindahan,** muka surat 40: Pengemaskinian perenggan dengan menambah perkataan (offsite) pada para (a). ix. **Perkara 5.2.4 – Pengurusan Kata Laluan Pengguna,** muka surat 44: Pengemaskinian perenggan (c) Bagi lain-lain kata laluan yang tidak dapat menyokong adalah menggunakan 8 – 12 aksara. x. **Perkara 5.2.4 – Pengurusan Kata Laluan Pengguna,** muka surat 44: Pengemaskinian perenggan (l) (satu (1) kali sejarah). xi. **Perkara 5.4.1 – Kawalan Had Capaian Maklumat,** muka surat 46: Menambah perenggan mengikut keupayaan sistem pada para (c). xii. **Perkara 7.2.2 – Peralatan Sokongan ICT,** muka surat 54: menambah perenggan Persetujuan Tahap Keselamatan (SLA) pada para (d). xiii. **Perkara 9.1.2 – Keselamatan Perkhidmatan Rangkaian,** muka surat 67: menambah perenggan Persetujuan Tahap Keselamatan (SLA) pada para (d). xiv. Menambah **Perkara 15 - Kawalan Membawa Peranti Anda Sendiri (BYOD).** xv. **Glosari**, muka surat 92: Menambah perenggan baru bagi Peralatan Mudah Alih – Merujuk kepada IPad, laptop dan smartphone.

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 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
vii. Versi 5.0 – 10 Ogos 2016
viii. Versi 5.1 – 12 Disember 2017

Penambahbaikan 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 maklumat 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 untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ianya 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 kelemahan (*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 pihak lain 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 atau mengikut keperluan semasa.	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 MAKLUMAT

2.1 ORGANISASI DALAMAN

Objektif: Mewujudkan pengurusan organisasi keselamatan untuk melaksanakan serta mengawal pelaksanaan dan operasi keselamatan maklumat dalam organisasi.

2.1.1 Peranan dan Tanggungjawab Organisasi Keselamatan Maklumat

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
Timbalan Ketua Setiausaha (Pengurusan dan Sosio-Ekonomi) 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

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
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 keselamatan ICT kepada ICTSO; dan (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT, KWP.	Pengurus ICT

Pegawai Teknologi Maklumat (Seksyen Aplikasi & Laman Web dan Seksyen Infrastruktur & 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
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; (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;	Pengguna

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**.	
Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain). Ini bertujuan untuk memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara–perkara yang perlu dipatuhi adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT KWP; (b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; (d) Akses kepada aset ICT 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;	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

iii. Perakuan Akta Rahsia Rasmi 1972; iv. Hak Harta Intelek; (f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan KWP seperti di **Lampiran A.**	
Peranan dan tanggungjawab Pasukan Tindak Balas Insiden Keselamatan ICT (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

2.1.2 Pengasingan Peranan dan Tanggungjawab	
Peranan dan tanggungjawab dalam bidang tugas hendaklah diasingkan untuk mengurangkan peluang bagi pengubahsuaian atau penyalahgunaan yang tidak dibenarkan ke atas aset organisasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasikan; (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; dan (d) Capaian ke pelayan (*server*) perlu diasingkan antara pengguna dan pentadbir bagi mengurangkan berlaku pengubahsuaian yang tidak dibenarkan.	CIO, Pentadbir Sistem, ICTSO dan Pengurus ICT
2.1.3 Senarai Perhubungan Dengan Pihak Berkuasa	
KWP hendaklah memastikan senarai perhubungan dengan pelbagai pihak yang berkaitan diwujudkan dan dikemaskini. Ia merupakan sumber rujukan pengguna KWP mengetahui senarai perhubungan pihak berkuasa yang berdekatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyediakan senarai perhubungan pihak berkuasa dan sentiasa mengemaskini senarai tersebut; dan (b) Memastikan senarai perhubungan pihak berkuasa ini diedarkan kepada semua pengguna atau pengguna yang berkaitan.	Semua

2.1.4 Senarai Perhubungan Dengan Pihak Yang Berkepentingan	
Ini bertujuan untuk memastikan semua pengguna KWP mengetahui senarai perhubungan pihak yang berkepentingan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyediakan senarai perhubungan pihak yang berkepentingan dan sentiasa mengemaskini senarai tersebut; dan (b) Memastikan senarai pihak yang berkepentingan ini diedarkan kepada semua pengguna atau pengguna yang berkaitan.	Semua
2.1.5 Keselamatan Maklumat Dalam Pengurusan Projek	
Ini bertujuan untuk memastikan setiap pengurusan projek mengambilkira aspek keselamatan maklumat bermula daripada perancangan sehingga penyerahan projek. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengambil kira aspek keselamatan maklumat berdasarkan kepada peraturan atau pekeliling semasa yang berkuatkuasa dalam setiap projek di KWP; dan (b) Memastikan Pegawai Keselamatan ICT (ICTSO) dilibatkan dalam setiap projek di KWP bagi memberikan khidmat nasihat keselamatan ICT.	CIO, Pentadbir Sistem, ICTSO dan Pengurus ICT
2.2 PERALATAN MUDAH ALIH DAN KERJA JARAK JAUH	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.	
2.2.1 Peralatan Mudah Alih	
Semua peralatan mudah alih, sama ada dimiliki oleh KWP atau milik persendirian, yang mempunyai akses kepada rangkaian, data dan sistem perlu mematuhi peraturan seperti berikut: (a) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk melindungi dari ancaman keselamatan ICT; (b) Memastikan bahawa anti-virus digunakan dalam setiap peralatan mudah alih, sentiasa dikemaskini dan mempunyai lesen yang masih sah; (c) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan peralatan mudah alih;	Semua

(d) Setiap peralatan mudah alih milik KWP hendaklah mempunyai katalaluan; (e) Peralatan mudah alih milik persendirian tidak dibenarkan untuk terus disambungkan ke rangkaian LAN kecuali dengan kebenaran ICTSO; dan (f) Peralatan mudah alih yang dimiliki oleh KWP hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan;	
2.2.2 Kerja Jarak Jauh / *Teleworking*	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang akses dan capaian tidak sah melalui rangkaian luar KWP; (b) Memastikan bahawa tindakan keselamatan yang bersesuaian diambil kira untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat; dan (c) Kebenaran akses daripada luar rangkaian KWP kepada maklumat, rangkaian dan aplikasi dalaman hanya boleh dicapai melalui (*Virtual Private Network*) atau aplikasi desktop yang menggunakan *Secure Socket Layer (SSL).*	Semua

PERKARA 3: KESELAMATAN SUMBER MANUSIA

3.1. KESELAMATAN SUMBER MANUSIA SEBELUM PERKHIDMATAN

Objektif: Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan KWP, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan masing-masing. Semua pengguna KWP hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

3.1.1 Tapisan	
KWP hendaklah memastikan pegawai, kakitangan dan pihak ketiga melaksanakan tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	SUB (KP), Pengurus ICT dan ICTSO
3.1.2 Terma dan Syarat Pelantikan	
Perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan KWP serta pengguna luar yang terlibat dalam menjamin keselamatan informasi maklumat; (b) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	SUB(KP)

3.2. KESELAMATAN SUMBER MANUSIA DALAM PERKHIDMATAN

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

3.2.1 Tanggungjawab Pihak Pengurusan	
Perkara yang perlu dipatuhi termasuk yang berikut: (a) ICTSO hendaklah memastikan semua pengguna KWP mematuhi DKICT KWP; (b) Memastikan pengguna KWP mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh KWP.	ICTSO dan Pengurus ICT

3.2.2 Pembudayaan, Latihan dan Sesi Kesedaran Keselamatan Maklumat	
KWP perlu melaksanakan perkara-perkara berikut: (a) Melaksanakan sesi kesedaran dan pendidikan berkaitan dengan pengurusan keselamatan ICT kepada pengguna KWP secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. (b) KWP perlu menyediakan sesi kesedaran (hebahan menerusi e-mel atau *desktop wallpaper*), latihan atau pendidikan keselamatan ICT sekurang-kurangnya sekali setahun. (c) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul bagi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Khidmat Pengurusan.	ICTSO dan Pengurus ICT
3.2.3 Tindakan Tatatertib	
KWP hendaklah memastikan adanya proses tindakan perundangan atau tatatertib ke atas pengguna KWP sekiranya berlaku perlanggaran Peraturan-peraturan Pegawai Awam (Kelakuan dan Tatatertib) 1993, dasar-dasar Kerajaan, peraturan, serta undang-undang semasa yang masih berkuatkuasa.	
3.3. PENAMATAN ATAU PERUBAHAN PERKHIDMATAN	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT yang dikembalikan kepada KWP mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh KWP dan / atau terma perkhidmatan; dan (c) Menguruskan urusan keluar, berhenti, pertukaran peranan dan tanggungjawab pengguna KWP;	Semua

PERKARA 4: PENGURUSAN ASET

4.1 AKAUNTABILITI ASET	
Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KWP	
4.1.1 Inventori Aset ICT	
Ini bertujuan untuk memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh setiap pemilik atau pemegang amanah masing-masing. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Merekod dan mengemas kini maklumat aset menggunakan borang daftar harta modal dan inventori; (b) Setiap aset ICT hendaklah mempunyai maklumat berikut; (i) Pemilik yang sah; dan (ii) Rekod penempatan.	Semua
4.1.2 Hak Milik Aset ICT	
KWP perlu memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja;	Semua
4.1.3 Penggunaan Aset ICT	
Perkara-perkara berikut perlu dipatuhi dalam penggunaan aset ICT adalah seperti berikut: (a) Memastikan penggunaan aset ICT dan kemudahan pemprosesan maklumat dikenal pasti, didokumen dan dilaksana. Setiap pengguna bertanggungjawab terhadap penggunaan semua aset ICT di bawah tanggungjawabnya. (b) Pengendalian aset ICT hendaklah merujuk kepada peraturan atau pekeliling semasa yang masih berkuat kuasa. (c) Setiap pengguna perlu menanggung kos pembaikan aset ICT sekiranya BPM mendapati kerosakan yang berlaku disebabkan oleh kecuaian pengguna. (d) Takrifan kecuaian pengguna adalah kegagalan mematuhi peraturan yang disengajakan, kegagalan penyeliaan atau penjagaan aset dan pengesahan oleh pihak ketiga berkaitan	Semua

punca kerosakan akibat kecuaian.	
4.1.4 Pemulangan Aset ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna bertanggungjawab untuk mengembalikan aset ICT setelah bertukar keluar atau ditamatkan perkhidmatan melalui Nota Serah Tugas atau borang yang berkaitan. (b) Semua pengguna hendaklah memulangkan semua aset ICT kepada Pegawai Aset atau pegawai bertanggungjawab selepas penamatan pekerjaan, kontrak atau perjanjian.	Pentadbir Sistem dan Semua
4.2 PENGELASAN DAN PENGENDALIAN MAKLUMAT	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
4.2.1 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan sebagaimana yang telah ditetapkan seperti berikut: (a) Rahsia Besar; (b) Rahsia; (c) Sulit; atau (d) Terhad	Ketua Setiausaha, CIO, Pengurus ICT dan ICTSO
4.2.2 Pelabelan Maklumat	
Prosedur pelabelan maklumat hendaklah dibangunkan dan dilaksanakan mengikut skim klasifikasi maklumat yang diguna pakai oleh KWP.	Ketua Setiausaha, CIO, Pengurus ICT dan ICTSO
4.2.3 Pengendalian Aset atau Maklumat	
Tatacara bagi pengendalian aset atau maklumat hendaklah dibangunkan dan dikuatkuasakan mengikut skim klasifikasi maklumat yang diguna pakai oleh KWP. Tatacara ini hendaklah mengambilkira 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;	Ketua Setiausaha, CIO, Pengurus ICT dan ICTSO

(c) Menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; (f) Memastikan keselamatan maklumat terperingkat semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah keselamatan ICT dari diketahui umum.	

4.3 PENGURUSAN MEDIA

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

4.3.1 Pengurusan Media Mudah Alih (*Removable Media*)

Media mudah alih merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat dan media storan yang boleh alih. Peraturan yang perlu dipatuhi dalam pengurusan media mudah alih adalah berdasarkan Arahan Keselamatan 1985 dan seperti berikut: (a) Media mudah alih hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; (b) Akses untuk memasuki kawasan penyimpanan media mudah alih hendaklah terhad kepada Pentadbir dan pegawai yang dibenarkan sahaja; (c) Media mudah alih perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (d) Media mudah alih yang mengandungi data terperingkat hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan; (e) Akses dan pergerakan media mudah alih hendaklah direkodkan; (f) Peralatan *backup* bagi media mudah alih hendaklah diletakkan di tempat yang terkawal; (g) Mengadakan salinan atau pendua pada media mudah alih bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; dan	Semua

(h) Hanya maklumat rasmi dibenarkan untuk disimpan dalam media mudah alih yang dibekalkan oleh Jabatan.	
4.3.2 Pelupusan Media	
Pelupusan media perlu mendapat kelulusan dari pihak pengurusan ICT dan mengikut prosedur Kerajaan yang mana berkenaan. Peraturan yang perlu dipatuhi dalam pelupusan media adalah seperti berikut: (a) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul serta selamat dengan merujuk mana-mana peraturan yang berkuatkuasa. (b) Semua media yang hendak dilupuskan hendaklah memastikan data terperingkat/sensitif dihapuskan (*wipe data*) dengan teratur dan selamat; (c) Pelupusan media dalam aset ICT hendaklah dilaksanakan mengikut Pekeliling Pengurusan Aset Alih Kerajaan yang berkuatkuasa; dan (d) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu;	Semua
4.3.3 Penghantaran dan Pemindahan	
Peraturan yang perlu dipatuhi dalam penghantaran dan pemindahan media adalah berdasarkan Arahan Keselamatan 1985 dan seperti berikut: (a) Media penghantaran atau pemindahan media keluar pejabat (*off-site*) hendaklah mendapat kebenaran daripada pemilik terlebih dahulu; (b) Memastikan penghantaran atau pemindahan media ke luar pejabat mempunyai rekod; dan (c) Memastikan media yang mengandungi maklumat terperingkat dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa proses pemindahan.	Semua

PERKARA 5: KAWALAN CAPAIAN

5.1 KEPERLUAN KE ATAS KAWALAN CAPAIAN	
Objektif: Mengawal capaian ke atas maklumat dan kemudahan pemprosesan maklumat.	
5.1.1 Polisi Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada. Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara-perkara yang perlu dipatuhiadalah seperti berikut: (a) Kawalan capaian ke atas peralatan 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; (d) Kawalan ke atas kemudahan pemprosesan maklumat; (e) Kawalan ke atas capaian aplikasi KWP; dan (f) Kebenaran untuk menyebarkan maklumat.	Pentadbir Sistem ICT, ICTSO, Pengurus ICT
5.1.2 Kawalan Capaian Rangkaian dan Perkhidmatan Rangkaian	
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari KWP. Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Memastikan hanya pengguna KWP yang dibenarkan sahaja boleh mendapat perkhidmatan rangkaian; (b) Menempatkan atau memasang peralatan ICT yang bersesuaian untuk kawalan keselamatan antara rangkaian KWP, rangkaian agensi lain dan rangkaian awam;	ICTSO, Pengurus ICT dan Pentadbir Rangkaian

(c) Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna, ID pengguna, kata laluan atau peralatan ICT yang dihubungkan ke rangkaian termasuk rangkaian tanpa wayar; dan (d) Memantau kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	
5.2 PENGURUSAN CAPAIAN PENGGUNA	
Objektif: Memastikan kawalan capaian pengguna yang dibenarkan sahaja dan untuk menghalang capaian yang tidak dibenarkan kepada sistem dan perkhidmatan ICT.	
5.2.1 Pendaftaran dan Pembatalan Akaun Pengguna	
KWP hendaklah mewujudkan prosedur pendaftaran dan pembatalan pengguna bagi menguruskan capaian dan pembatalan hak capaian. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Pendaftaran dan penamatan akaun pengguna hendaklah menggunakan borang yang dibenarkan sahaja; (b) Akaun yang diperuntukkan oleh KWP hendaklah digunakan untuk tujuan rasmi; (c) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (d) Akaun pengguna luar yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan terlebih dahulu; (e) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ianya tertakluk kepada peraturan dan arahan semasa. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; (f) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang kecuali atas sebab-sebab tertentu; dan (g) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna dalam tempoh satu (1) bulan 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	Pentadbir Sistem ICT, ICTSO dan Pengurus ICT

(6) bulan seperti mana yang diluluskan oleh Ketua Jabatan; iii. Bertukar bidang tugas kerja; iv. Bertukar ke agensi lain; v. Bersara; vi. Ditamatkan perkhidmatan: serta merta pembatalan. vii. Dalam prosiding dan/atau dikenakan tindakan tatatertib: serta merta pembatalan. (h) Akaun hendaklah didaftarkan atau dibatalkan kebenaran menerusi sistem direktori; contohnya Active Directory, LDAP atau sebagainya.	
5.2.2 Penyediaan dan Semakan Capaian Pengguna	
KWP perlu mewujudkan prosedur penyediaan capaian pengguna atau pembatalan capaian pengguna kepada perkhidmatan ICT. Perkara berikut perlu dipatuhi: (a) Memastikan hak capaian pengguna hanya kepada yang dibenarkan sahaja atau mengikut bidang tugas; (b) Mengemaskini hak capaian pengguna secara berkala atau mengikut keperluan; dan (c) Membatalkan hak capaian pengguna sekiranya bertukar bidang tugas, bertukar keluar, tamat perkhidmatan atau bersara.	Pentadbir Sistem ICT
5.2.3 Pengurusan Hak Capaian Khas Pengguna	
Peruntukan dan penggunaan *Priviledge Access Rights* perlu dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan bidang tugas. Hak capaian khas pengguna adalah seperti *Administrators Priviledge, Super User Priviledge dan Root User Priviledge.*	Pentadbir Sistem ICT
5.2.4 Pengurusan Kata Laluan Pengguna	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang telah ditetapkan seperti	

berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan 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 belas (12) aksara dengan gabungan nombor, abjad dan simbol kecuali bagi peralatan atau perisian yang mempunyai pengurusan katalaluan yang terhad; Tiada pengecualian kepada mana-mana server. Bagi lain-lain kata laluan yang tidak dapat menyokong, adalah menggunakan 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) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan dalam program; (g) Penguatkuasaan bagi pertukaran kata laluan semasa log masuk 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); (j) Sesi ditamatkan selepas had masa melahu (*idle*) antara lima (5) sehingga lima belas (15) minit; (k) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian (pengecualian kepada sistem e-mel); dan (l) Mengelakkan penggunaan semula kata laluan yang telah digunakan (satu (1) kali sejarah).	

5.2.5 Kajian Semula Hak Capaian Pengguna	
KWP hendaklah mengkaji semula hak capaian pengguna secara berkala atau sekurang-kurangnya satu (1) kali setahun atau mengikut keperluan.	Pentadbir Sistem ICT
5.2.6 Pembatalan atau Pelarasan Hak Capaian Pengguna	
Perkara berikut perlu dipatuhi: (a) Hak capaian pengguna KWP untuk kemudahan pemprosesan data dan maklumat hendaklah dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian; dan (b) Pelarasan hak capaian pengguna perlulah dilakukan apabila berlaku perubahan dalaman atau perubahan bidang tugas.	Pentadbir Sistem ICT
5.3 TANGGUNGJAWAB PENGGUNA	
Objektif: Memastikan pengguna bertanggungjawab untuk melindungi maklumat yang digunakan untuk pengesahan identiti.	
5.3.1 Penggunaan Ciri Kata Laluan Pengguna	
Pengguna KWP perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi maklumat yang digunakan untuk pengesahihan identiti Pengguna perlu: (a) Merahsiakan kata laluan; (b) Kata laluan hendaklah diingat dan tidak didedahkan dengan apa cara sekalipun; (c) Tukar kata laluan apabila terdapat tanda-tanda kebocoran atau kompromi kata laluan; (d) Panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan nombor, abjad dan simbol kecuali bagi peralatan atau perisian yang mempunyai pengurusan katalaluan yang terhad; (e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (f) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;	Semua

(g) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; dan (h) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian (pengecualian kepada sistem e-mel).	

5.4 KAWALAN CAPAIAN SISTEM DAN APLIKASI

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

5.4.1 Kawalan Had Capaian Maklumat

Bertujuan untuk melindungi had capaian maklumat dalam sistem dan aplikasi dari sebarang bentuk capaian yang tidak dibenarkan. Kawalan had capaian ini adalah berdasarkan kepada polisi kawalan capaian KWP. Bagi memastikan kawalan had capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem 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 maksimum lima (5) kali percubaan atau mengikut keupayaan sistem. 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 tidak digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem ICT dan ICTSO

5.4.2 Prosedur Log Masuk Yang Selamat

KWP hendaklah memastikan prosedur capaian kepada sistem dan aplikasi hendaklah mengikut polisi kawalan capaian. Perkara yang perlu dipatuhi adalah: (a) Mengawal capaian ke atas sistem dan aplikasi menggunakan	Pentadbir Sistem ICT dan ICTSO

prosedur log masuk yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Mengenal pasti identiti, terminal atau lokasi bagi setiap log masuk yang dibenarkan; (d) Merekodkan capaian log masuk yang berjaya dan gagal; (e) Notifikasi keselamatan jika berlaku percubaan atau pencerobohan; (f) Menamatkan sesi yang tidak aktif selepas tempoh yang tertentu; (g) Menghadkan sesi sambungan sekatan untuk aplikasi yang berisiko tinggi; dan (h) Tidak menghantar kata laluan dalam "*clear-text*" melalui rangkaian.	
5.4.3 Sistem Pengurusan Kata Laluan	
Mewujudkan sistem pengurusan kata laluan yang interaktif dan menjamin kata laluan yang berkualiti dengan mematuhi perkara seperti berikut: (a) Memastikan kata laluan sekurang-kurangnya dua belas (12) aksara dengan gabungan nombor, abjad dan simbol kecuali bagi perkakasan atau perisian yang mempunyai pengurusan katalaluan yang terhad; (b) Penguatkuasaan pertukaran kata laluan semasa log masuk kali pertama atau selepas log masuk kali pertama atau selepas kata laluan diset semula kecuali bagi perkakasan atau perisian yang mempunyai pengurusan kata laluan yang terhad; (c) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian (pengecualian kepada sistem e-mel);dan (d) Memaklumkan pertukaran kata laluan menerusi e-mel atau lain-lain medium yang selamat.	Pentadbir Sistem ICT dan ICTSO

5.4.4 Kawalan Penggunaan Program atau Perisian Khas Utiliti	
Penggunaan program utiliti seperti di bawah yang mungkin mampu *Over-Riding System* adalah dihadkan dan perlu mematuhi perkara berikut: (a) Hanya program atau perisian khas utiliti yang diperakui sahaja dibenarkan bagi kegunaan KWP; dan (b) Penggunaan program atau perisian khas utiliti yang membebankan kapasiti *(bandwidth)* rangkaian perlu dihadkan.	ICTSO
5.4.5 Kawalan Capaian Kepada *Source Code* Program	
Perkara berikut hendaklah dipatuhi: (a) Pembangunan *source code* program perlu diselia dan dipantau oleh pemilik sistem; (b) *Source code* bagi semua aplikasi dan program adalah menjadi hak milik KWP; (c) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan selamat; (d) Sebarang pindaan *source code* mestilah mengikut prosedur yang ditetapkan; dan (e) Log audit perlu dikekalkan kepada semua capaian kepada *source code*.	Pentadbir Sistem dan Pengurus ICT

PERKARA 6: KRIPTOGRAFI

6.1 KAWALAN KRIPTOGRAFI	
Objektif: Memastikan penggunaan kriptografi yang betul dan berkesan untuk melindungi kerahsiaan, kesahihan dan/atau integriti maklumat.	
6.1.1 Polisi Kawalan Penggunaan Kriptografi	
KWP perlu memastikan penggunaan kriprografi dilaksanakan dengan mematuhi perkara seperti berikut: (a) Membangun dan melaksanakan peraturan enkripsi untuk melindungi maklumat sensitif menggunakan kaedah kriptografi yang sesuai; (b) Mengenal pasti tahap perlindungan pengunaan kriptografi dengan mengambil kira jenis, kekuatan dan kualiti algoritma yang diperlukan; dan (c) Pengguna hendaklah menggunakan kriptografi ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	CIO, ICTSO, Pentadbir Sistem ICT dan Pengurus ICT
6.1.2 Pengurusan Kunci Kriptografi (*Key Management*)	
Perkara berikut hendaklah dipatuhi: (a) Pengurusan ke atas kunci kriptografi hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut. (b) Memastikan kaedah yang selamat dan berkesan untuk pengurusan kunci yang menyokong teknik kriptografi di KWP; dan (c) Setiap urusan transaksi maklumat sensitif hendaklah menggunakan tandatangan digital atau kunci kriptografi supaya mendapat perlindungan dan pengiktirafan undang-undang.	CIO, ICTSO, Pentadbir Sistem ICT dan Pengurus ICT

PERKARA 7: KESELAMATAN FIZIKAL DAN PERSEKITARAN

7.1 KESELAMATAN KAWASAN

Objektif: Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

7.1.1 Kawalan Keselamatan Fizikal

Ini bertujuan untuk menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-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 (l) Memastikan kawasan–kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Pegawai Keselamatan Kementerian, CIO dan ICTSO

7.1.2 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
7.1.3 Kawalan Keselamatan Bagi Pejabat, Bilik dan Kemudahan ICT	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawasan tempat berkerja, bilik dan kemudahan ICT perlu dihadkan daripada akses oleh pengguna yang tidak berkaitan; dan (b) Penunjuk ke lokasi dan tempat larangan tidak harus menonjol dan hanya memberi petunjuk minimum.	Pegawai Keselamatan Kementerian, CIO dan ICTSO
7.1.4 Kawalan Perlindungan Terhadap Ancaman Luar Dan Bencana Alam	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) KWP perlu merekabentuk dan melaksanakan pelan perlindungan fizikal dari kebakaran, banjir dan bencana alam. (b) KWP perlu memastikan pelan tindakan perlindungan bagi ancaman berbahaya seperti letupan, kacau bilau, rusuhan dan sebagainya.	Pegawai Keselamatan Kementerian, CIO dan ICTSO
7.1.5 Kawalan Tempat Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kepada pegawai-pegawai tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. (a) Akses kepada kawasan larangan hanya kepada pegawai-pegawai yang dibenarkan sahaja; (b) Pihak ketiga adalah dilarang untuk memasuki kawasan larangan kecuali dengan kebenaran untuk kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah di pantau sehingga tugas di	Pegawai Keselamatan Kementerian, CIO dan ICTSO

kawasan berkenaan selesai; (c) Kawasan tempat larangan perlu dikunci pada setiap masa; (d) Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk melainkan dengan kebenaran; dan (e) Pengguna KWP yang perlu berurusan di pusat data hendaklah mendapatkan kebenaran dan mengisi buku log keluar masuk Pusat Data.	
7.1.6 Kawasan Penghantaran dan Pemunggahan	
KWP hendaklah memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Pegawai Keselamatan Kementerian, CIO dan ICTSO
7.2 KESELAMATAN PERALATAN ICT	
Objektif: Melindungi peralatan ICT KWP dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
7.2.1 Penempatan dan Perlindungan Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang ditetapkan; (c) Pengguna dilarang sama sekali menambah menanggalkan atau mengganti sebarang peralatan ICT yang telah ditetapkan; (d) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT; (e) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (f) Pengguna mesti memastikan perisian anti-virus di dalam	Semua

	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 aset 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 ICT yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai;	
(l)	Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;	
(m)	Pengendalian aset ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;	
(n)	Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran Pentadbir Sistem ICT;	
(o)	Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk baik pulih. Setiap pengguna perlu menanggung kos pembaikan aset ICT sekiranya BPM mendapati kerosakan yang berlaku disebabkan oleh kecuaian pengguna;	
(p)	Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin komputer tersebut sentiasa berkeadaan baik;	
(q)	Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;	

(r) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir *(administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT; (s) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (t) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan *OFF* apabila meninggalkan pejabat; (u) Memastikan plug dicabut daripada suis utama *(main switch)* bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
7.2.2 Peralatan Sokongan ICT	
Perkara-perkara berikut perlu dipatuhi: (a) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (b) Peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); (c) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) atau penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan (d) Semua alat sokongan perlu disemak dan diselenggara dari masa ke semasa (sekurang-kurangnya setahun sekali atau mengikut Persetujuan Tahap Perkhidmatan (SLA) dalam kontrak perjanjian).	ICTSO dan Pentadbir Pusat Data
7.2.3 Kawalan Keselamatan Kabel Telekomunikasi dan Elektrik	
Kabel termasuk kabel elektrik atau telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. Langkah keselamatan yang perlu diambil adalah seperti berikut:	ICTSO, Pentadbir Rangkaian, Pentadbir Pusat Data dan Pihak Ketiga

(a) Memastikan hanya pengguna KWP atau pihak ketiga yang dibenarkan boleh melaksanakan pemasangan atau penyelenggaraan kabel; (b) Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; (c) Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; (d) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan (e) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	
7.2.4 Penyelenggaraan Peralatan ICT	
Peralatan ICT hendaklah diselenggarakan bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua peralatan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan peralatan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan; dan (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pegawai Aset dan Pengurus ICT
7.2.5 Pengalihan Peralatan ICT	
Bagi memastikan keselamatan peralatan ICT yang boleh dialihkan, perkara-perkara berikut hendaklah dipatuhi: (a) Peralatan ICT yang hendak dibawa keluar dari premis KWP, perlulah mendapat kelulusan dan direkodkan pengguna yang bertanggungjawab;	Semua

(b) Peralatan ICT yang hendak dialihkan kedudukan hendaklah dimaklumkan kepada Pegawai Aset; (c) Peralatan ICT yang dibawa keluar dari premis KWP hendaklah bagi tujuan rasmi sahaja; dan (d) Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkaitan.	
7.2.6 Keselamatan Peralatan ICT Di Luar Premis	
Peralatan yang dibawa keluar dari premis KWP adalah terdedah kepada pelbagai risiko. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan direkodkan pegawai bertanggungjawab ke atas peralatan ICT tersebut; (b) Peralatan ICT tersebut perlu dilindungi dan dikawal sepanjang masa; dan (c) Penyimpanan atau penempatan peralatan ICT tersebut mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
7.2.7 Keselamatan Semasa Pelupusan dan Penggunaan Semula	
Pelupusan atau penggunaan semula peralatan ICT melibatkan semua peralatan yang using, rosak dan tidak boleh dibaiki. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa dan perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan; (b) Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; (c) Peralatan ICT yang akan dilupuskan secara dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan ICT boleh dilupuskan atau sebaliknya;	Pengurus ICT, ICTSO dan Pegawai Aset

(e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (f) Pegawai Aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori Sistem Pengurusan Aset; (g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan (h) Pengguna adalah dilarang daripada melakukan perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan; iii. Memindah keluar dari premis KWP mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab KWP; dan v. 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 ICT yang hendak dilupuskan.	
7.2.8 Peralatan ICT Gunasama atau Tiada Pengguna	
Pengguna perlu memastikan bahawa peralatan ICT gunasama atau tiada pengguna dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: (a) Menggunakan id pengguna dan katalaluan yang diberikan;	Semua

(b) Memastikan peralatan ICT tersebut digunakan oleh pengguna KWP yang dibenarkan sahaja; (c) Tamatkan sesi aktif dan klik log keluar apabila selesai tugas;	
7.2.9 *Clear Desk* dan *Clear Screen*	
Maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* hendaklah dilaksanakan bagi memastikan tiada bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau log keluar apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif seperti '*electronic storage media'* dan dokumen terperingkat di dalam laci atau kabinet fail yang berkunci; (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat. (d) E-mel masuk dan keluar hendaklah dikawal; dan (e) Menghalang penggunaan tanpa kebenaran mesin fotostat dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	Semua

PERKARA 8: KESELAMATAN OPERASI

8.1 TANGGUNGJAWAB DAN PROSEDUR OPERASI	
Objektif: Memastikan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman.	
8.1.1 Dokumentasi Prosedur Operasi	
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) Memastikan hanya pengguna yang dibenarkan sahaja boleh mengakses dokumen prosedur operasi; dan (d) Semua prosedur operasi hendaklah dikemas kini dari semasa ke semasa mengikut keperluan.	Semua
8.1.2 Kawalan Perubahan	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan struktur organisasi perlu direkodkan dan dikawal; (b) Perubahan ke atas proses kerja atau bidang tugas perlu direkod dan dikawal; (c) Perubahan ke atas kemudahan pemprosesan maklumat perlu direkod dan dikawal; (d) Perubahan ke atas sistem atau aplikasi perlu direkodkan dan dikawal; (e) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur hendaklah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;	Semua

(f) 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; (g) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan ; dan (h) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
8.1.3 Perancangan Kapasiti	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kapasiti sesuatu komponen atau sistem atau aplikasi ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan; (b) Memastikan perancangan kapasiti ini mencukupi dan bersesuaian untuk pembangunan, keupayaan serta kegunaan sistem atau aplikasi ICT pada masa akan datang; dan (c) Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem ICT dan ICTSO
8.1.4 Pengasingan Persekitaraan Pembangunan, Pengujian dan Operasi	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mewujudkan persekitaran yang berasingan bagi: i. Pembangunan. ii. Pengujian. iii. Operasi. (b) Menggunakan peralatan keselamatan ICT yang mengawal persekitaran ini bagi mengurangkan risiko capaian tidak sah atau perubahan yang tidak dibenarkan.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

8.2 PERLINDUNGAN MALWARE ATAU VIRUS	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang peralatan keselamatan rangkaian ICT untuk mengesan perisian atau program berbahaya seperti malware atau anti virus; (b) Memasang dan menggunakan hanya perisian keselamatan ICT bagi semua aset ICT; (c) Penggunaan perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang- undang bertulis yang berkuat kuasa; (d) Mengimbas semua perisian atau sistem dengan anti-virus sebelum menggunakannya; (e) Mengemaskini anti-virus dengan *pattern* anti virus yang terkini; (f) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (g) Mengadakan sesi kesedaran kepada pengguna mengenai ancaman perisian berbahaya dan cara mengendalikannya; (h) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (i) Melaksanakan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (j) Memberi notifikasi mengenai ancaman keselamatan ICT seperti serangan *malware* atau virus.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

8.3 SALINAN PENDUA (*BACKUP*)	
Objektif: Memastikan sistem, aplikasi, data, imej dan maklumat yang kritikal mempunyai salinan pendua, berkeupayaan untuk *restore* semula dan melindungi daripada kehilangan maklumat.	
8.3.1 Maklumat Pendua (*Backup*)	
Bagi melindungi data atau maklumat hilang, *backup* hendaklah dilaksanakan ke atas sistem dan aplikasi. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Membuat polisi *backup* keselamatan ke atas semua sistem dan	Pentadbir Sistem ICT, Pengurus ICT dan

aplikasi kritikal seperti berikut: i. Harian (*Incremental*); ii. Mingguan (*Full*); dan iii. Bulanan (Full). b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi dan tahap kritikal maklumat; c) Menguji sistem *backup* dan prosedur *restore* sekurang-kurangnya sekali setahun; d) Memastikan sistem *backup* berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; e) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan f) Merekodkan dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	ICTSO

8.4 Log dan Pemantauan

Objektif: Memastikan log direkodkan dan menjana pembuktian melalui pemantauan.

8.4.1 Log Aktiviti

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

mengikut keperluan.	
8.4.2 Kawalan Perlindungan Log	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Melindungi maklumat log daripada capaian yang tidak dibenarkan; (b) Capaian ke atas log fail *server* hanya kepada pengguna yang dibenarkan sahaja; (c) Memastikan log fail tidak boleh diubah. (d) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (e) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
8.4.3 Log Pentadbir dan Pengendali (*Operator*)	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Memastikan setiap aktiviti log bagi pentadbir dan pengendali sistem direkodkan; (b) Melindungi aktiviti log pentadbir dan pengendali sistem daripada capaian yang tidak sah atau hanya yang dibenarkan sahaja; dan (c) Memastikan log ini sentiada dipantau dan disemak secara berkala atau mengikut keperluan.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
8.4.4 Penyeragaman Waktu (*Clock Synchronisation*)	
Waktu bagi sistem, aplikasi atau peralatan ICT hendaklah diselaraskan dengan Masa Standard Malaysia kecuali bagi peralatan yang tidak mempunyai fungsi *Network Time Protocol (NTP)*.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

8.5 KAWALAN PERISIAN OPERASI	
Objektif: Melindungi sistem operasi dan memastikan integriti sistem operasi.	
8.5.1 Instalasi Perisian Pada Sistem Operasi	
KWP perlu memastikan pelaksanaan kawalan ke atas instalasi perisian pada sistem operasi. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Pengemaskinian perisian operasi, aplikasi dan *program libraries* hanya boleh dilakukan oleh pentadbir terlatih setelah mendapat kelulusan pengurusan; (b) Sistem operasi hanya boleh memegang "*executable code*" dan tidak kod pembangunan atau penyusun. (c) Instalasi perisian hendaklah mendapat kebenaran daripada Pentadbir Sistem ICT dan ICTSO; (d) Memastikan penggunaan perisian yang mempunyai lesen sah sahaja; (e) Penggunaan aplikasi dalam sistem operasi hanya boleh dilaksanakan selepas ujian yang terperinci dan diperakui berjaya; (f) Setiap konfigurasi ke atas sistem operasi perlu dikawal dan didokumentasikan melalui prosedur perubahan kawalan konfigurasi. Konfigurasi hanya boleh dilaksanakan selepas mendapat persetujuan dari pihak berkaitan; dan (g) Satu '*rollback*' strategi harus diadakan sebelum perubahan dilaksanakan.	Semua
8.6 PENGURUSAN KETERDEDAHAN TEKNIKAL (*TECHNICAL VULNERABILITY*)	
Objektif: Melindungi dan mencegah daripada berlaku eksploitasi pada keterdedahan teknikal.	
8.6.1 Pengurusan Ancaman Keterdedahan Teknikal	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Menggunakan peralatan keselamatan ICT untuk mengenal pasti keterdedahan teknikal pada sistem maklumat yang digunakan; (b) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; (c) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

(d) Mengambil tindakan pengawalan dan pengukuhan untuk mengatasi risiko berkaitan.	
8.6.2 Kawalan Pemasangan Perisian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui oleh ICTSO sahaja dibenarkan bagi kegunaan pengguna di KWP; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; dan (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya.	Semua
8.7 KEPERLUAN AUDIT PADA SISTEM MAKLUMAT	
Objektif: Mengurangkan impak bagi aktiviti audit ke atas sistem operasi.	
8.7.1 Kawalan Audit Pada Sistem Maklumat	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan; (b) Meminimumkan gangguan dan kesan daripada kawalan audit yang dilaksanakan; dan (c) Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

PERKARA 9: KESELAMATAN KOMUNIKASI

9.1 PENGURUSAN KESELAMATAN RANGKAIAN	
Objektif: Memastikan kawalan keselamatan dan perlindungan maklumat termasuk kemudahan pemproses maklumat dalam rangkaian.	
9.1.1 Kawalan Rangkaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Menempatkan atau memasang antara peralatan kawalan keselamatan rangkaian ICT yang bersesuaian di antara rangkaian ICT KWP, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna; (c) Menggunakan peralatan keselamatan rangkaian ICT yang menepati kesesuaian penggunaannya; (d) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap rangkaian ICT; (e) Semua trafik keluar dan masuk dalam rangkaian ICT KWP hendaklah melalui *firewall* atau peralatan keselamatan rangkaian ICT yang bersesuaian; (f) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran daripada ICTSO; (g) Memasang perisian *Intrusion Prevention System* (h) (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data 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 Pengurus ICT adalah tidak dibenarkan; (k) Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di KWP sahaja dan penggunaan modem atau peralatan sambungan rangkaian yang adalah dilarang; dan (l) Kemudahan rangkaian tanpa wayar (*wireless)* hendaklah dipantau	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

dan dikawal penggunaannya;	
9.1.2 Keselamatan Perkhidmatan Rangkaian	
Mekanisme keselamatan dan tahap perkhidmatan bagi semua perkhidmatan rangkaian sama ada oleh pihak ketiga atau secara dalaman hendaklah dikenalpasti serta dimasukkan dalam perjanjian perkhidmatan rangkaian. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Memastikan keselamatan maklumat organisasi diambil kira dalam setiap perjanjian perkhidmatan rangkaian dengan pihak ketiga; (b) Menandatangani perjanjian bertulis untuk melindungi maklumat apabila berlaku pemindahan maklumat organisasi antara KWP dengan pihak luar; (c) Terma perkongsian maklumat dan perisian di antara KWP dengan pihak ketiga hendaklah dimasukkan di dalam perjanjian; (d) Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi Persetujuan Tahap Perkhidmatan (SLA) yang telah dipersetujui; dan (e) Mempunyai mekanisme pengurusan insiden sekiranya berlaku insiden keselamatan maklumat.	Pentadbir Sistem ICT dan ICTSO
9.1.3 Pengasingan Rangkaian	
Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian KWP. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) *Demilitarized Zone* (*DMZ*) untuk sistem atau aplikasi luaran; (b) *Server Farm* dikhaskan untuk pelayan; (c) Segmen rangkaian Dalaman (LAN) digunakan untuk pengguna KWP; (d) Segmen rangkaian Luaran (WAN) untuk akses ke Internet atau rangkaian luar KWP; (e) Segmen rangkaian tanpa wayar (*Wireless*) untuk pelawat; (f) Segmen rangkaian tanpa wayar (*Wireless*) untuk pengguna; (g) Segmen rangkaian untuk pengurusan peralatan (*Management Segment*); dan	

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

9.2 PERPINDAHAN MAKLUMAT

Objektif: Memastikan kawalan keselamatan semasa perpindahan atau pertukaran maklumat antara KWP dengan pihak ketiga.

9.2.1 Polisi dan Prosedur Perpindahan Maklumat	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan perpindahan maklumat yang formal perlu diwujudkan untuk melindungi perpindahan maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; (b) Tatacara dan syarat perpindahan maklumat antara KWP dengan pihak ketiga perlu dimasukkan dalam perjanjian atau surat persetujuan; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa perpindahan keluar dari KWP; (d) Maklumat yang terdapat dalam e-mel perlu dilindungi sebaik-baiknya;	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
9.2.2 Perjanjian Dalam Perpindahan Maklumat	
KWP perlu mengambil kira keselamatan maklumat organisasi dengan mewujudkan perjanjian bertulis apabila berlaku pemindahan maklumat antara KWP dengan pihak ketiga. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Pengurusan KWP hendaklah mengawal penghantaran dan penerimaan maklumat organisasi; (b) Prosedur bagi verifikasi maklumat organisasi semasa pemindahan maklumat; (c) Menggunapakai prinsip dan tatacara *escrow*; dan (d) Tanggungjawab dan tindakan pengukuhan sekiranya berlaku insiden keselamatan maklumat seperti kehilangan data.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
9.2.3 Pengurusan E-mel atau Mesej Elektronik	
Penggunaan e-mel di KWP hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel	Semua

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;

(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; dan (o) Bagi pengguna yang telah ditamatkan perkhidmatan atau meninggal dunia, akaun e-mel mereka akan ditamatkan serta-merta.	
9.2.4 Kerahsiaan dan *Non-Disclosure* Agreement	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mewujudkan perjanjian kerahsiaan atau *non-disclosure agreement (NDA)* dengan pihak ketiga; (b) Mengambil kira keperluan kerahsiaan maklumat organisasi dalam perjanjian; dan (c) Mengkaji dan menyemak perjanjian dari masa semasa serta mendokumentasikan perjanjian.	CIO, Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

PERKARA 10: PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

10.1 KEPERLUAN KESELAMATAN SISTEM MAKLUMAT

Objektif: Memastikan keselamatan maklumat merupakan sebahagian daripada keseluruhan kitaran hayat sistem maklumat. Ini termasuk keperluan untuk sistem maklumat yang menyediakan perkhidmatan melalui rangkaian awam.

10.1.1 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan baru, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira keperluan keselamatan maklumat bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (b) Ujian keselamatan atau keterdedahan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan sistem output untuk menghasilkan data yang telah diproses adalah tepat; (c) Sistem maklumat 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
10.1.2 Keselamatan Perkhidmatan Aplikasi Dalam Rangkaian Umum	
Maklumat dari perkhidmatan aplikasi yang menggunakan rangkaian umum hendaklah dilindungi daripada aktiviti-aktiviti ancaman keselamatan atau akses yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan *encryption* untuk penghantaran atau penerimaan maklumat yang menggunakan rangkaian umum;	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

(b) Memastikan perkhidmatan aplikasi menggunakan *Secure Socket Layer* (*SSL*) dalam setiap transaksi; (c) Memastikan pengesahan berkaitan dengan pihak yang berhak untuk meluluskan kandungan maklumat, penerbitan atau menandatangani dokumen transaksi ; (d) Memastikan setiap pengguna perkhidmatan aplikasi adalah pengguna yang betul dan sah; dan (e) Memastikan pengguna mempunyai tahap akses mengikut kelulusan atau kebenaran pemilik sistem.	
10.1.3 Perlindungan Transaksi Perkhidmatan Aplikasi	
KWP perlu memastikan transaksi bagi perkhidmatan aplikasi hendaklah dilindungi daripada penghantaran yang tidak lengkap (*mis-routing)*, pengubahan mesej, pendedahan yang tidak dibenarkan serta penduaan mesej. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi; (b) Memastikan semua kriteria transaksi seperti di bawah dipatuhi: i. Maklumat pengguna adalah sah dan telah diperakukan; ii. Mengekalkan kerahsiaan maklumat; iii. Mengekalkan privasi pihak yang terlibat; iv. Komunikasi antara semua pihak yang terlibat telah di enkrip; v. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi; (c) Menggunakan mekanisme tambahan seperti *secret key*, kad pintar dan medium kawalan yang lain untuk pengesahan pengguna; dan (d) Pihak yang mengeluar dan mengekalkan pensijilan digital atau tandatangan adalah dilantik oleh Kerajaan.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

10.2 KESELAMATAN PEMBANGUNAN SISTEM DAN PROSES SOKONGAN	
Objektif: Memastikan keselamatan maklumat diambil kira dan dilaksanakan dalam kitaran hayat pembangunan sistem maklumat.	
10.2.1 Tatacara Keselamatan Dalam Pembangunan Sistem	
Peraturan atau tatacara pembangunan sistem hendaklah diwujudkan dan digunakan oleh KWP. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Keperluan keselamatan maklumat semasa persekitaran kitaran hayat pembangunan; (b) Panduan keselamatan dalam kitar hayat pembangunan sistem maklumat; (c) Keselamatan maklumat dalam fasa reka bentuk; (d) Pemeriksaan keselamatan dalam perkembangan projek; (e) Keselamatan repositori atau ruang storan; (f) Keselamatan dalam kawalan versi; (g) Keperluan pengetahuan keselamatan dalam pembangunan sistem maklumat; dan (h) Kebolehan pengaturcara untuk mengenalpasti kelemahan dan mencadangkan penambahbaikan dalam pembangunan sistem.	Pemilik Sistem dan Pentadbir Sistem ICT
10.2.2 Prosedur Kawalan Perubahan Sistem	
Perubahan ke atas sistem di dalam kitaran pembangunan hendaklah dikawal menggunakan prosedur kawalan perubahan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenalpasti perubahan ke atas sistem yang hendak dilaksanakan melalui kajian keperluan pengguna (*user requirement study – URS);* (b) Mendokumentasi dan mengesahkan URS sebelum dilaksanakan; (c) Mengkaji impak operasi dan keselamatan maklumat bagi setiap perubahan yang dicadangkan; (d) Melaksanakan perubahan sistem pada pelayan pembangunan untuk menguji keberkesanan operasi; (e) Setiap permohonan perubahan/penambahbaikan sistem hendaklah menggunakan *Change Request Form(CRF) (Lampiran*	Pemilik Sistem dan Pentadbir Sistem ICT

CRF) untuk memantau perubahan/penambahbaikan yang dilaksanakan oleh pengaturcara; dan (f) Kawalan perlu dibuat ke atas sebarang perubahan atau pindaan ke atas sistem bagi memastikan ianya terhad mengikut keperluan sahaja.	
10.2.3 Kajian Teknikal Sistem Maklumat Selepas Perubahan Platform Operasi	
Perubahan platform operasi sama ada sistem pengoperasian atau rangka kerja (*framework*) hendaklah dikaji dan diuji bagi memastikan tiada sebarang masalah yang timbul terhadap operasi atau keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan perubahan platform operasi ini dilaksanakan dalam persekitaran pengujian; (b) Kawalan aplikasi dan prosedur integrity disemak untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform operasi; (c) Perubahan platform dimaklumkan dari semasa ke semasa bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan; dan (d) Memastikan perubahan yang sesuai diselaraskan kepada pelan kesinambungan perkhidmatan.	Pemilik Sistem dan Pentadbir Sistem ICT
10.2.4 Kawalan Keselamatan Perubahan Pakej Perisian (*Software Packages*)	
Perubahan kepada pakej perisian adalah tidak digalakkan tetapi terhad kepada perubahan yang diperlukan dan semua perubahan hendaklah dikawal. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan perubahan pakej perisian ini mengambilkira aspek keselamatan maklumat; (b) Perubahan pakej perisian ini hanya dilaksanakan oleh pihak yang dibenarkan sahaja; (c) Melaksanakan pengujian ke atas pakej perisian yang terkini sebelum dimaklumkan kepada semua pengguna mengenai perubahan versi pakej perisian; dan (d) Memastikan perubahan pakej perisian ini tidak menjejaskan perkhidmatan operasi sistem maklumat.	Pemilik Sistem dan Pentadbir Sistem ICT

10.2.5 Prinsip Kejuruteraan Keselamatan Sistem	
Prinsip kejuruteraan yang selamat bagi pembangunan sistem maklumat hendaklah diwujudkan, didokumentasi, diselenggara dan digunapakai dalam pelaksanaan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan keselamatan seperti ancaman daripada bencana alam dan manusia diambil kira; dan (b) Perlindungan maklumat dalam pembangunan sistem semasa pemprosesan, perpindahan dan penyimpanan; (c) Mengambil kira kriteria di bawah dalam prinsip kejuruteraan pembangunan sistem. i. *Business Layer* – berdasarkan tahap pengesahan pengguna; hanya pengguna tertentu boleh melihat data peribadi; ii. *Data Layer* – hanya log masuk dengan kata laluan pangkalan data yang selamat untuk aktiviti penyelenggaraan pangkalan data dibenarkan; iii. *Application Layer* – penggunaan enkripsi untuk penghantaran maklumat; dan iv. *Technology Layer* – penggunaan perisian sumber terbuka dan infrastruktur rangkaian.	Pemilik Sistem dan Pentadbir Sistem ICT
10.2.6 Keselamatan Persekitaran Pembangunan Sistem	
Persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran hayat pembangunan sistem (*development lifecycle*). Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan persekitaraan pembangunan diasingkan dan dikawal oleh peralatan keselamatan rangkaian; (b) Capaian ke persekitaraan pembangunan ini hanya kepada pengguna yang dibenarkan sahaja; dan (c) Memastikan pengaturaca menggunakan mekanisma yang selamat dalam perpindahan data atau maklumat.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

10.2.7 Pembangunan Sistem oleh Pihak Ketiga (*Outsourced*)	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pembangunan sistem oleh pihak ketiga perlu diselia dan dipantau oleh pemilik sistem; (b) Memastikan perpindahan teknologi oleh pihak ketiga kepada KWP dilaksanakan; dan (c) Kod sumber (*source code*) bagi semua sistem dan aplikasi yang dibangunkan menjadi hak milik KWP.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO
10.2.8 Pengujian Keselamatan Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengujian fungsi keselamatan sistem hendaklah dilaksanakan semasa fasa pembangunan; (b) Semua sistem baru atau penambahbaikan sistem hendaklah menjalani ujian *Security Posture Assessment* (SPA); (c) Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; (d) Mengenalpasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data; dan (e) Menjalankan proses semakan ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan.	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO
10.2.9 Pengujian Penerimaan Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan proses kerja sistem memenuhi keperluan pengguna; (b) Melaksanakan ujian fungsi ke atas sistem menggunakan data sampah (*dummy input*); (c) Semakan ke atas sistem jika memenuhi keperluan perniagaan organisasi dan kebolehgunaan sistem; (d) Melaksanakan integrasi dan pengujian dengan sistem yang lain sekiranya berkaitan; (e) Merangkumi ujian alfa (*alpha testing*) dan ujian beta (*beta testing*); dan (f) Melibatkan ujian prestasi (*performance test*) dan ujian tekanan (*stress test*).	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO

10.3 DATA UJIAN	
Objektif : Memastikan keselamatan data semasa pengujian	
10.3.1 Kawalan Data Ujian	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Data ujian hendak digunakan perlu dipilih, dilindungi dan dikawal; (b) Pengunaan data ujian hendaklah dilaksanakan ke atas kod aturcara yang terkini; (c) Mengaktifkan audit log bagi merekodkan semua aktiviti pengujian; dan (d) Data ujian hanya boleh digunakan oleh pengguna yang dibenarkan sahaja.	Pemilik Sistem dan Pentadbir Sistem ICT

PERKARA 11: PERHUBUNGAN DENGAN PEMBEKAL

11.1 KESELAMATAN MAKLUMAT PERHUBUNGAN DENGAN PEMBEKAL	
Objektif: Memastikan kawalan keselamatan ke atas aset KWP yang boleh dicapai oleh pembekal.	
11.1.1 Dasar Keselamatan Maklumat Untuk Pembekal	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan perjanjian disediakan dan didokumentaskan dengan pembekal yang mempunyai capaian ke atas aset KWP; (b) Mengenal pasti tahap capaian mengikut kategori pembekal; (c) Merekod dan memantau semua capaian pembekal; (d) Memastikan pembekal diberikan taklimat keselamatan dan menandatangi surat akuan pematuhan dasar keselamatan KWP; dan (e) Memastikan setiap pembekal melaksanakan tapisan keselamatan menerusi mekanisma yang masih berkuatkuasa.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
11.1.2 Menangani Aspek Keselamatan Dalam Perjanjian Pembekal	
Keperluan keselamatan maklumat hendaklah diwujudkan dan dipersetujui dengan pembekal yang akan mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur di KWP. Perkara-perkara yang perlu diambil kira seperti berikut: (a) Mengadakan sesi taklimat keselamatan; (b) Mengklasifikasikan maklumat; (c) Keperluan undang-undang dan peraturan yang berkuatkuasa; (d) Obligasi setiap pihak bagi kawalan akses, pemantauan, pelaporan dan pengauditan; (e) Tapisan keselamatan pembekal; dan (f) Tindakan undang-undang.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
11.1.3 Rantaian Bekalan atau Perkhidmatan Teknologi Maklumat dan Komunikasi	
Perjanjian dengan pembekal hendaklah mengambil kira keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan rantaian bekalan atau perkhidmatan teknologi maklumat dan komunikasi. Perkara-perkara yang perlu diambil kira seperti berikut:	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

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

11.2 PENGURUSAN PENYAMPAIAN PERKHIDMATAN PEMBEKAL

Objektif : Mengekalkan tahap yang dipersetujui dalam keselamatan maklumat dan penyampaian perkhidmatan selaras dengan perjanjian pembekal.

11.2.1 Pemantauan dan Kajian Perkhidmatan Pembekal

Perkara-perkara yang perlu diambil kira seperti berikut: (a) Melaksanakan pemantauan, kajian semula dan pengauditan perkhidmatan pembekal mengikut keperluan; (b) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian tahap perkhidmatan (*service level agreement*); dan (c) Mengkaji semula laporan perkhidmatan yang dikemukakan oleh pembekal berdasarkan kepada status kemajuan.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

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

PERKARA 12: PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

12.1 MEKANISME PELAPORAN INSIDEN KESELAMATAN	
Objektif: Memastikan pendekatan yang konsisten dan berkesan untuk pengurusan insiden keselamatan maklumat termasuk mengenal pasti ancaman dan kelemahan.	
12.1.1 Prosedur dan Tanggungjawab	
Perkara-perkara yang perlu diambil kira seperti berikut: (a) Menubuhkan prosedur dan pasukan yang mengendalikan serta menguruskan insiden keselamatan maklumat; (b) Memastikan tindakan pengukuhan serta maklum balas yang cepat, efektif dan teratur bagi setiap insiden keselamatan maklumat; dan (c) Pemakluman kepada pihak berkuasa atau agensi yang bertangungjawab dalam menangani insiden keselamatan.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
12.1.2 Mekanisme Pelaporan Insiden Keselamatan	
Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO. Tindakan oleh CERT, KWP untuk melaporkan kepada GCERT MAMPU dengan kadar segera. Prosedur pelaporan insiden keselamatan ICT adalah berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
12.1.3 Pelaporan Kelemahan Keselamatan ICT	
Kakitangan dan pembekal yang menggunakan sistem dan perkhidmatan ICT KWP dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT. Perkara-perkara yang perlu dilaporkan adalah seperti berikut: (a) Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak- pihak yang tidak diberi kuasa;	Semua

(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.	
12.1.4 Penilaian dan Analisa Aktiviti Keselamatan Maklumat	
Aktiviti keselamatan maklumat hendaklah dinilai dan dianalisa sama ada akan diklasifikasikan sebagai insiden keselamatan maklumat. Perkara-perkara yang perlu diambil kira adalah seperti berikut: (a) Merekod dan menyimpan semua aktiviti keselamatan maklumat secara berpusat atau pada peralatan ICT; dan (b) Menganalisa setiap aktiviti keselamatan maklumat secara berkala bagi memastikan pihak yang berkaitan dapat mengklasifikasikan aktiviti tersebut.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
12.1.5 Tindakan Pada Insiden Keselamatan Maklumat	
Perkara-perkara yang perlu diambil kira adalah seperti berikut: (a) Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; (b) Menjalankan kajian dan analisa; (c) Menghubungi pihak berkuasa atau agensi yang berkenaan dengan secepat mungkin; (d) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; (e) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; dan (f) Menangani insiden keselamatan maklumat mengikut Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

12.1.6 Pengalaman dari Insiden Keselamatan Maklumat	
Pengalaman serta pengetahuan yang diperolehi melalui proses menganalisis dan penyelesaian insiden keselamatan maklumat yang telah berlaku boleh digunakan untuk mengurangkan kebarangkalian (*likelihood*) atau kesan insiden pada masa akan datang. Perkara-perkara yang perlu diambil kira adalah seperti berikut: (a) Menyimpan dan merekodkan tindakan pengukuhan yang telah dilaksanakan semasa berlaku insiden keselamatan; dan (b) Menganalisa impak ke atas tindakan yang dilaksanakan.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
12.1.7 Pengumpulan Bahan Bukti	
Perkara-perkara yang perlu diambil kira adalah seperti berikut: (a) Prosedur untuk mengenal pasti, mengumpul, mendapatkan dan menyimpan bahan bukti hendaklah dibangunkan bagi memastikan bahan bukti dilindungi dan tersedia; dan (b) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti.	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

PERKARA 13: ASPEK KESELAMATAN DALAM PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

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

(e) Menjalankan analisis impak organisasi; (f) Melaksanakan prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (g) Mendokumentasikan proses dan prosedur yang telah ditetapkan; (h) Mengadakan program latihan secara berkala kepada warga KWP mengenai prosedur kecemasan; (i) Membuat *backup* mengikut prosedur yang ditetapkan; dan (j) Menguji, menyelenggara dan mengemaskini pelan keselamatan ICT setahun sekali atau mengikut keperluan.	
13.1.3 Pengesahan Kajian dan Penilaian Keselamatan Maklumat dalam Kesinambungan Perkhidmatan	
KWP hendaklah memeriksan serta mengesahkan secara berkala Pelan Pengurusan Kesinambungan Perkhidmatan yang dibangunkan dan kawalan keselamatan maklumat yang akan dilaksanakan bagi memastikan keberkesanan kawalan ini semasa berlaku bencana atau ancaman. Perkara-perkara yang perlu diambil kira adalah seperti berikut: (a) Menyenaraikan senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel KWP dan pembekal berserta nombor yang boleh dihubungi (faskimile, 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) Menetapkan arahan pemulihan maklumat dan kemudahan yang berkaitan; (e) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; (f) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh;	Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

(g) Salinan pelan pengurusan kesinambungan perkhidmatan perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama; (h) Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan; dan (i) Pelan pengurusan kesinambungan perkhidmatan hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan; (j) Ujian pelan hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan; dan (k) KWP hendaklah memastikan salinan pelan sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

13.2 *REDUNDANCY*

Objektif: Memastikan ketersediaan perkhidmatan dan kemudahan pemperosesan atau sistem maklumat.

13.2.1 Ketersediaan Perkhidmatan dan Kemudahan Pemprosesan Maklumat

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

PERKARA 14: PEMATUHAN

14.1 PEMATUHAN KEPADA KEPERLUAN PERUNDANGAN DAN KONTRAK	
Objektif: Mencegah pelanggaran obligasi perundangan, undang-undang, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat dan apa-apa keperluan keselamatan.	
14.1.1 Mengenalpasti Keperluan Perundangan dan Perjanjian Kontrak	
Semua keperluan undang-undang berkanun, peraturan dan kontrak perjanjian yang berkaitan dengan KWP perlu ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat. Senarai perundangan dan peraturan yang wajib dipatuhi oleh semua pengguna adalah seperti **Lampiran 2**.	Semua
14.1.2 Hak Harta Intelek (*Intellectual Property Rights*-IPR)	
Prosedur berkaitan perlu dibangunkan bagi memastikan pematuhan terhadap keperluan perundangan, peraturan dan perjanjian kontrak yang berkaitan hak harta intelek serta pemilik perisian yang sah. Pengguna perlu mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Keperluan hak cipta yang berkaitan dengan bahan proprietari, perisian, dan rekabentuk yang diperoleh melalui KWP; (b) Keperluan pelesenan menghadkan penggunaan produk, perisian, rekabentuk dan bahan-bahan lain yang diperolehi oleh KWP; (c) Pematuhan yang berterusan dengan sekatan hakcipta produk dan keperluan perlesenan; dan (d) Perisian atau sistem maklumat yang dibangunkan oleh KWP adalah menjadi harta intelek KWP.	Semua
14.1.3 Perlindungan Rekod	
Rekod-rekod yang penting (fizikal atau media) hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, pelepasan yang tidak dibenarkan mengikut undang-undang, peraturan, kontrak, dan keperluan perniagaan.Perkara-perkara yang perlu dipatuhi adalah	Semua

seperti berikut: (a) Pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat; (b) Jadual penyimpanan rekod perlu dikenal pasti; dan (c) Inventori rekod.	
14.1.4 Privasi dan Perlindungan Maklumat Peribadi	
KWP perlu mengenal pasti privasi dan melindungi maklumat peribadi penguna adalah terjamin seperti yang ditakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkenaan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Tidak mendedahkan maklumat peribadi pengguna pada mana-mana pihak yang tidak berkaitan; (b) Memastikan kawalan penyimpan rekod maklumat peribadi pengguna ditempat yang selamat; dan (c) Maklumat peribadi pengguna hanya boleh digunakan untuk tujuan rasmi dan dengan kebenaran.	Semua
14.1.5 Peraturan Kawalan Kriptografi	
KWP perlu memastikan kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang, dan peraturan-peraturan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Sekatan ke atas pengimport / pengeksport perkakasan dan perisian komputer yang melaksanakan fungsi-fungsi kriptografi tanpa kelulusan pihak berkuasa; (b) Sekatan ke atas pengimport/pengeksport perkakasan dan perisian yang ditambah direka untuk mempunyai fungsi kriptografi tanpa kelulusan pihak berkuasa; (c) Sekatan penggunaan enkripsi yang tidak dibenarkan; dan (d) Mematuhi kaedah akses oleh pihak berkuasa Malaysia bagi maklumat enkripsi perkakasan dan perisian.	Semua

14.2 KAJIAN KESELAMATAN MAKLUMAT	
Objektif: Memastikan keselamatan maklumat dilaksanakan dan beroperasi selaras dengan polisi atau prosedur KWP.	
14.2.1 Kajian Keselamatan Maklumat oleh Pihak Ketiga atau Badan Bebas	
KWP perlu memastikan kaedah pengurusan keselamatan maklumat serta pelaksanaannya seperti objektif kawalan, kawalan, polisi dan prosedur perlu dikaji secara bebas secara berkala atau sekiranya berlaku perubahan yang besar.	CIO, Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
14.2.2 Pematuhan Kepada Dasar Keselamatan dan Standard	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pentadbir Sistem ICT perlu memastikan kajian ke atas pematuhan dan prosedur pemprosesan maklumat di dalam bidang tanggungjawab mereka selaras dengan dasar keselamatan maklumat atau lain-lain keperluan keselamatan; (b) Mengenal pasti punca-punca ketidakpatuhan; (c) Menilai keperluan tindakan untuk mencapai pematuhan; (d) Melaksanakan tindakan pembetulan yang sewajarnya; dan (e) Mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti apa-apa kekurangan dan kelemahan; dan (f) 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**.	CIO, Pentadbir Sistem ICT, Pengurus ICT dan ICTSO
14.2.3 Pematuhan Kajian Teknikal	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Sistem maklumat hendaklah dikaji sekurang-kurangnya setahun atau mengikut keperluan supaya selaras dengan pematuhan dasar dan standard; dan (b) Keselamatan sistem maklumat hendaklah dikaji sekurang-kurangnya sekali setahun atau mengikut keperluan.	CIO, Pentadbir Sistem ICT, Pengurus ICT dan ICTSO

PERKARA 15: KAWALAN MEMBAWA PERANTI ANDA SENDIRI (BYOD)

15.1 KEPERLUAN KESELAMATAN	
Objektif: Memberi kebenaran kepada pegawai dan kakitangan untuk menggunakan telefon pintar, tablet serta kompter riba di tempat kerja berdasarkan kepada peraturan yang yang digariskan di bawah.	
15.1.1 Pengenalan	
Peraturan ini bertujuan melindungi keselamatan, integriti data dan infrastruktur di KWP. Pegawai serta kakitangan hendaklah bersetuju dengan terma dan syarat yang ditetapkan dalam dasar ini kebenaran akses ke rangkaian KWP dapat diberikan.	Semua
15.1.2 Polisi	
Perkara-perkara berikut perlu dipatuhi: (a) KWP mendefinisikan sebarang penggunaan peranti peribadi adalah bertujuan sama ada secara langsung atau tidak langsung, yang menyokong tugasan harian di KWP. (b) KWP mendefinisikan sebarang penggunaan peranti peribadi sepanjang waktu bekerja sebagai alat komunikasi atau rekreasi peribadi yang munasabah dan terhad, seperti membaca atau melayari internet. (c) Pegawai dan kakitangan dihalang daripada mengakses laman web tertentu semasa waktu kerja atau semasa disambungkan ke rangkaian KWP. Walaubagaimanapun, kebenaran akses akan diberikan setelah mendapat kebenaran daripada Pengurus ICT atau ICTSO. (d) Peranti peribadi tidak boleh digunakan pada bila-bila masa untuk menyimpan atau menghantar bahan yang dilarang, menyimpan atau menghantar maklumat yang tidak dibenarkan, mengganggu orang lain, menyebarkan maklumat terperingkat KWP, terlibat dalam aktiviti perniagaan luar tugas rasmi dan lain-lain perkara yang bertentangan dengan dasar Kerajaan. (e) Pegawai dan kakitangan dibenarkan menggunakan peranti peribadi untuk mengakses sumber atau aplikasi KWP seperti e-mel, kalendar, dokumen, dan lain-lain akses yang dibenarkan.	Semua

(f) Sambungan ke rangkaian KWP perlu diluluskan oleh Pengurus ICT atau ICTSO. (g) KWP tidak bertanggungjawab ke atas sebarang kerosakan peranti peribadi atau sistem operasi atau isu berkaitan perkakasan. (h) Peranti mesti dikemukakan kepada BPM untuk konfigurasi aplikasi yang sesuai dan perisian keselamatan (*anti-virus software*), sebelum mereka dapat mengakses rangkaian. (i) KWP berhak untuk mengambil tindakan tatatertib yang sesuai seperti penamatan akses sekiranya didapati tidak mematuhi peraturan dalam dasar ini.	
15.1.3 Pengguna Tiada Hak Privasi	
KWP akan menghormati privasi peranti peribadi semua pegawai serta kakitangan, dan mengambil langkah pencegahan yang terbaik untuk memastikan keselamatan maklumat privasi. KWP mempunyai hak untuk menjejaki dan meminta akses kepada peranti peribadi untuk melaksanakan fungsi teknikal serta melaksanakan kawalan keselamatan seperti yang digariskan dalam dasar ini. Pegawai serta kakitangan tidak mempunyai hak dan tidak seharusnya mempertikaikan hak privasi sepanjang menggunakan peralatan BYOD di premis KWP.	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.
Peralatan 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.
BYOD	BYOD adalah singkatan dari ayat "*Bring Your Own Device*" iaitu di dalam bahasa malaysia adalah "membawa peranti anda sendiri". BYOD merupakan suatu konsep atan dasar dimana ia membenarkan pekerja untuk membawa peranti mudah alih sendiri iaitu telefon pintar, tablet dan komputer riba yang boleh digunakan di tempat kerja mereka dan menggunakan peranti-peranti tersebut untuk mengakses maklumat khas dan aplikasi dalam kerja seharian
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.
***Intrusion Prevention System* (IPS)**	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya: Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Log Keluar	Log Keluar komputer Keluar daripada sesuatu input atau aplikasi komputer.
Log Masuk	Log Masuk Komputer Masuk ke sesuatu input 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.
Peralatan Mudah Alih	Merujuk kepada iPad, *laptop* dan *smartphone*.
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.
Escrow	Perjanjian kontrak di mana pihak ketiga diterima atau dokumen bagi pihak-pihak transaksi utama, dengan pengeluaran yang bergantung kepada syarat yang dipersetujui oleh pihak-pihak yang berurus niaga.

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT KWP
VERSI 5.0

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 : ……..

……

(Nama Pegawai Keselamatan ICT)
Kementerian Wilayah Persekutuan (KWP)

LAMPIRAN 2

SENARAI UNDANG-UNDANG, DASAR DAN PERATURAN

(1) Arahan Keselamatan;

(2) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)

(3) Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar KeselamatanTeknologi Maklumat dan Komunikasi Kerajaan;

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

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

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

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

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

(9) 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;

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

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

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

(13) Surat Pekeliling Perbendaharaan Bil 2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;

(14) Surat Pekeliling Perbendaharaan Bil 3/1995 – Peraturan Perolehan Perkhidmatan Perundingan;

(15) Akta Tandatangan Digital 1997;

(16) Akta Rahsia Rasmi 1972;

(17) Akta Jenayah Komputer 1997;

(18) Akta Hak Cipta (Pindaan) Tahun 1997;

(19) Akta Komunikasi dan Multimedia 1998;

(20) Perintah-perintah Am;

(21) Arahan Perbendaharaan;

(22) Arahan Teknologi Maklumat 2007;

(23) Garis Panduan Keselamatan MAMPU 2004;

(24) Standard *Operating Procedure* (SOP) ICT MAMPU.