Pejabat Mufti Wilayah Persekutuan
Jabatan Perdana Menteri

Dasar Keselamatan ICT

Versi 1.0

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
09 FEBRUARI 2021	1	JPICT PMWP BIL. 1/2021	19 APRIL 2021

GLOSARI

Bandwidth	Lebar Jalur. Ukuran atau jumlah data yang boleh dipindah melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	Ketua Pegawai Maklumat (*Chief Information Officer)*
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).
ICTSO	Pegawai Keselamatan ICT (*ICT Security Officer)*
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*.
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.
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.

1.0 PENGENALAN

Dasar Keselamatan ICT mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) Pejabat Mufti Wilayah Persekutuan (PMWP). Dasar ini juga menerangkan kepada semua pengguna di PMWP mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT PMWP.

2.0 OBJEKTIF

Dasar Keselamatan ICT PMWP diwujudkan dengan tujuan memastikan tahap keselamatan ICT PMWP terurus serta menjamin kesinambungan urusan perkhidmatan yang disediakan oleh PMWP kepada orang awam, beroperasi dengan baik selain dapat meminimumkan kes insiden keselamatan ICT.

3.0 SKOP

Dasar ini meliputi semua sumber atau aset ICT yang digunakan seperti perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar ini adalah terpakai oleh semua pengguna di PMWP termasuk pegawai, kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT PMWP.

4.0 PRINSIP-PRINSIP

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

a. Capaian atas dasar perlu mengetahui

Capaian terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk capaian adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

b. Hak capaian minimum

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

c. Akauntabiliti

Semua pengguna adalah bertanggungjawab ke atas semua tindakannya terhadap aset ICT PMWP;

d. Pengasingan

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

e. Pengauditan

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

f. Pematuhan

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

g. Pemulihan

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

h. Saling Bergantungan

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

PERKARA 01 : PEMBANGUNAN DAN PENYELENGGARAAN DASAR	
0101 Dasar Keselamatan ICT	
Objektif : Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan PMWP dan perundangan yang berkaitan.	
Program / Aktiviti	**Tanggungjawab**
010101 Pelaksanaan Dasar	Ketua Jabatan
Pelaksanaan dasar ini akan dijalankan oleh Mufti Wilayah Persekutuan selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT) PMWP. Ahli JPICT ini terdiri daripada CIO, ICTSO dan Ketua Bahagian/Unit.	
010102 Penyebaran Dasar	ICTSO
Dasar ini bertujuan memastikan hala tuju pengurusan organisasi untuk melindungi aset ICT selaras dengan keperluan perundangan. Dasar ini perlu disebarkan kepada semua pengguna PMWP (termasuk pegawai, kakitangan, pembekal, pakar runding yang berurusan dengan pihak PMWP).	
010103 Penyenggaraan Dasar	ICTSO
Dasar Keselamatan ICT Kerajaan adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Prosedur Penyelenggaraan Dasar Keselamatan ICT PMWP adalah seperti berikut :- a. Mengkaji semula dasar ini sekurang-kurangnya sekali setahun bagi mengenal pasti dan menentukan perubahan yang diperlukan; b. Mengemukakan cadangan pindaan dan/atau perubahan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT); dan	

c. Memaklumkan sebarang perubahan dasar yang telah dipersetujui dalam mesyuarat JPICT kepada semua pengguna PMWP.	
010104 Pemakaian Dasar	Semua
Dasar Keselamatan ICT PMWP adalah terpakai kepada semua pengguna ICT PMWP dan tiada pengecualian diberikan.	
PERKARA 02 : ORGANISASI KESELAMATAN	
0201 Infrastruktur Organisasi Keselamatan	
Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.	
Program / Aktiviti	**Tanggungjawab**
020101 Ketua Jabatan PMWP	Ketua Jabatan
Peranan dan tanggungjawab Ketua Jabatan adalah seperti berikut :- a. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT PMWP; b. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT PMWP; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT PMWP.	
020102 Struktur Dalaman Organisasi	Semua
Struktur formal dalam PMWP diwujudkan untuk mengurus keselamatan ICT organisasi yang mana perkara berikut adalah dipatuhi :-	

a. Komitmen pengurusan ke atas keselamatan ICT dilaksanakan dengan aktif dan telus; b. Aktiviti pengurusan keselamatan ICT diselaraskan oleh wakil atau urus setia tertentu yang diwujudkan dari semua peringkat PMWP berdasarkan peranan masing-masing; c. Wakil yang diberikan peranan perlu bertanggungjawab di atas setiap tugasan keselamatan ICT yang diamanahkan; d. Keperluan pengurusan kerahsian maklumat dikenal pasti, dilaksana dan dikaji secara berkala; e. Memastikan perhubungan atau komunikasi dengan pihak yang berkaitan dipelihara; dan f. Memastikan kajian semula ke atas keselamatan maklumat dijalankan mengikut peraturan yang ditetapkan.	
020103 Ketua Pegawai Maklumat (CIO)	CIO
Timbalan Mufti adalah merupakan Ketua Pegawai Maklumat (CIO). Peranan dan tanggungjawab beliau adalah seperti berikut :- a. Membantu Ketua Jabatan dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Menentukan keperluan keselamatan ICT; dan c. Membangun dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT.	
020104 Pegawai Keselamatan ICT (ICTSO)	ICTSO
Pegawai Keselamatan ICT (ICTSO) PMWP adalah Ketua Unit ICT, Bahagian Khidmat Sokongan. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut : - a. Mengurus keseluruhan program-program keselamatan ICT PMWP; b. Menguatkuasakan Dasar Keselamatan ICT PMWP;	

c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT PMWP kepada semua pengguna; d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT PMWP; e. Menyedia dan melaksanakan program kesedaran mengenai keselamatan ICT; f. Menjalankan pengurusan risiko; g. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; h. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; i. Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (CERT) NACSA dan memaklumkannya kepada CIO; j. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan k. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT PMWP.	
020105 Pengurus Komputer	Pengurus Komputer
Peranan dan tanggungjawab Pengurus Komputer adalah seperti berikut : - a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT PMWP; b. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan PMWP; c. Menentukan kawalan capaian semua pengguna terhadap aset ICT PMWP;	

d. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan e. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT PMWP.	
020106 Pentadbir Sistem ICT	Pentadbir Sistem ICT
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 ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT PMWP; c. Memantau aktiviti capaian harian pengguna; d. Mengenal pasti 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; dan f. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala.	
020107 Pentadbir Rangkaian	Pentadbir Rangkaian
Pentadbir Rangkaian berperanan dan bertanggungjawab 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 ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT PMWP; c. Memantau aktiviti capaian rangkaian harian pengguna; d. Mengenal pasti 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; dan f. Menyediakan laporan capaian pengguna terhadap rangkaian secara berkala.	
020108 Pentadbir Laman Web (*Webmaster*)	Pentadbir Laman Web
Peranan dan tanggungjawab Pentadbir Laman Web adalah seperti berikut: a. Menerima kandungan laman web yang telah disahkan kesahihan dan terkini daripada sumber yang sah; b. Memantau prestasi capaian dan menjalankan penalaan prestasi untuk memastikan akses yang lancar; c. Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai antara muka laman web; d. Menghadkan capaian Pentadbir Laman Web bahagian ke web server; e. Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet ke laman web PMWP; f. Memastikan hanya maklumat yang bersifat terbuka dipaparkan di laman web; g. Memastikan reka bentuk laman web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; dan	

h. Melaksanakan perkemasan keselamatan terhadap sistem pengoperasian dan perisian-perisian lain di web server;	
020109 Pentadbir E-mel	Pentadbir E-mel
Peranan dan tanggungjawab Pentadbir E-mel adalah seperti berikut: a. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan. Pembatalan akaun (pengguna yang berhenti, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat; b. Pentadbir E-mel boleh membekukan akaun pengguna jika perlu semasa pengguna bercuti panjang, berkursus atau menghadapi tindakan tatatertib; c. Memastikan pengguna e-mel PMWP berkemahiran menggunakan e-mel melalui penyediaan dokumen tatacara penggunaan e-mel dan Internet serta pelaksanaan Kursus Pembudayaan ICT (Penggunaan E-mel dan Internet) secara berterusan. d. Memastikan kemudahan membuat capaian e-mel melalui pelbagai peralatan ICT dan alat komunikasi; dan e. Mengesah dan memaklumkan kepada ICTSO sekiranya mengalami insiden keselamatan melalui saluran rasmi.	
020110 Pengguna ICT	Semua
Peranan dan tanggungjawab pengguna adalah seperti berikut :- a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT PMWP; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat PMWP;	

d. Menghadiri program-program kesedaran mengenai keselamatan ICT; e. Melaksanakan langkah-langkah perlindungan seperti berikut :- i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi piawai, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran,penyampaian, pertukaran dan pemusnahan; vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; dan viii. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera. f. Menandatangani surat akuan pematuhan DKICT PMWP seperti di **Lampiran 1**.	
020111 Jawatankuasa Pemandu ICT (JPICT) PMWP	Ketua Jabatan
Keanggotaan JPICT adalah seperti berikut :- Pengerusi: Ketua Jabatan, Mufti Wilayah Persekutuan Ahli: a. Timbalan Mufti (CIO); b. Ketua Penolong Mufti; c. Ketua Bahagian/Unit;	

d. Penolong Pegawai Teknologi Maklumat Kanan dan e. Juruteknik Komputer. Urusetia: Unit ICT, Bahagian Khidmat Sokongan. Bidang kuasa: a. Menetapkan arah tuju dan strategi ICT untuk pelaksanaan ICT PMWP; b. Merancang, menyelaras dan memantau pelaksanaan program atau projek ICT PMWP; c. Menyelaras dan menyeragamkan pelaksanaan ICT agar selari dengan Pelan Strategik Teknologi Maklumat (PSTM) Sektor Awam; d. Meluluskan projek-projek ICT; e. Mengikuti dan memantau perkembangan program ICT serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pelaksanaan ICT; f. Merancang dan menentukan langkah-langkah keselamatan ICT; g. Mengemukakan perolehan ICT yang telah diluluskan di peringkat JPICT PMWP kepada Jawatankuasa Teknikal ICT (JTICT) MAMPU untuk kelulusan; h. Mengemukakan laporan kemajuan projek ICT yang diluluskan kepada JTICT MAMPU; i. Menetapkan dasar dan prosedur pengurusan laman web PMWP; j. Menyelenggara dokumen DKICT PMWP; k. Memantau tahap pematuhan DKICT PMWP; dan l. Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam jabatan yang mematuhi keperluan DKICT PMWP;	

020112 Pasukan Pengendali Insiden (CERT) PMWP	
Keanggotaan PMWP CERT adalah seperti berikut :- Pengarah CERT: Ketua Penolong Mufti Pengurus ICT: Ketua Unit ICT, Bahagian Khidmat Sokongan Ahli : a. Penolong Mufti, Bahagian Khidmat Sokongan dan b. Juruteknik Komputer, Unit ICT, Bahagian Khidmat Sokongan. Urusetia: Unit ICT, Bahagian Khidmat Sokongan Peranan dan tanggungjawab PMWP CERT adalah seperti berikut :- a. Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; b. Merekod dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d. Menghubungi dan melaporkan insiden yang berlaku kepada ICTSO dan pihak NACSA sama ada sebagai input atau untuk tindakan seterusnya; e. Merujuk agensi-agensi di bawah kawalannya untuk mengambil tindakan pemulihan dan pengukuhan; f. Menyebarkan makluman berkaitan insiden kepada agensi di bawah kawalannya; dan g. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	Pengarah CERT dan ICTSO

Apabila berlaku insiden, Pengarah CERT agensi perlu menggerakkan ahli CERT agensi untuk mengambil tindakan berikut :- a. Mengurus dan mengambil tindakan ke atas insiden yang berlaku sehingga keadaan pulih; b. Mengaktifkan Pelan Pemulihan Perkhidmatan (BCP) jika perlu; dan c. Menentukan sama ada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang/ keselamatan.	
0202 Pihak Luar/Ketiga	
Objektif : Menjamin Keselamatan semua aset ICT yang digunakan oleh pihak luar/ketiga.	
Program / Aktiviti	**Tanggungjawab**
020201 Keperluan Keselamatan Kontrak Dengan Pihak Luar/Ketiga	CIO, ICTSO, Pengurus Komputer, Pentadbir Sistem ICT, Pentadbir Rangkaian dan Pihak Ketiga
Pihak PMWP mesti memastikan keselamatan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar/ketiga. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Mengenal pasti risiko keselamatan maklumat dan kemudahan proses maklumat dan laksanakan kawalan yang sesuai sebelum memberikan capaian kepada pihak luar/ketiga; b. Capaian kepada aset ICT PMWP perlu berlandaskan kepada perjanjian kontrak; dan c. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeteraikan. i. Dasar Keselamatan ICT PMWP; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; iv. Hak Harta Intelek.	

PERKARA 03 : KAWALAN DAN PENGELASAN ASET	
0301 Akauntabiliti Inventori Aset	
Objektif : Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT PMWP.	
Program / Aktiviti	**Tanggungjawab**
030101 Inventori Aset	Semua
Memastikan semua aset ICT Kerajaan diberikan perlindungan yang bersesuaian oleh pemilik atau pemegang amanah masing-masing; Perkara yang perlu dipatuhi adalah seperti berikut :- a. Memastikan semua aset dikenal pasti dan maklumat aset direkodkan ke dalam borang daftar harta modal dan inventori dan sentiasa dikemaskini; b. Memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; dan c. Peraturan bagi penggunaan aset hendaklah dikenal pasti, didokumen dan dilaksanakan.	
0302 Pengkelasan dan Pengendalian Maklumat	
Objektif : Memastikan setiap maklumat dan aset ICT diberikan tahap perlindungan yang bertepatan.	
Program / Aktiviti	**Tanggungjawab**
030201 Pengelasan Maklumat	Semua
Memastikan setiap maklumat diberikan perlindungan yang bersesuaian berdasarkan tahap sensitiviti masing-masing;	

Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut :- a. Rahsia Besar b. Rahsia; c. Sulit; atau d. Terhad.	
030202 Pengendalian Maklumat	Semua
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut :- a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.	

PERKARA 04 : KESELAMATAN SUMBER MANUSIA	
0401 Keselamatan ICT Dalam Tugas Harian	
Objektif : Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT PMWP.	
Program / Aktiviti	**Tanggungjawab**
040101 Tanggungjawab Keselamatan	Semua
Peranan dan tanggungjawab pengguna terhadap keselamatan ICT mestilah lengkap, jelas, direkod, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.	
040102 Perakuan Akta Rasmi	Semua
Warga PMWP yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan **Akta Rahsia Rasmi 1972**.	
040103 Terma dan Syarat Perkhidmatan	Semua
Semua warga PMWP yang dilantik hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	
040103 - 1 Sebelum Berkhidmat	Semua
Pekara yang perlu dipatuhi adalah seperti berikut :- a. Peranan dan tanggungjawab penjawat awam, kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan dengan aset ICT Kerajaan perlu dinyatakan dengan jelas dan terperinci sebelum, semasa dan selepas perkhidmatan;	

a. Penyaringan dan pengesahan latar belakang calon untuk penjawat awam, kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan hendaklah dilakukan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan a. Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	
040103 - 2 Dalam Perkhidmatan	Semua
Pekara yang perlu dipatuhi adalah seperti berikut :- a. Memastikan semua pengguna PMWP menguruskan keselamatan berdasarkan perundangan dan peraturan yang ditetapkan oleh PMWP; b. Memastikan latihan kesedaran yang berkaitan mengenai pengurusan keselamatan ICT diberi kepada semua pengguna PMWP dan sekiranya perlu diberikan kepada kontraktor, pihak ketiga dan lain-lain pihak yang berkepentingan dari semasa ke semasa; dan c. Memastikan adanya proses tindakan disiplin ke atas semua pengguna PMWP, sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan PMWP.	
040103 - 3 Tamat Perkhidmatan/Bersara atau Bertukar	Semua
Memastikan semua pengguna PMWP diuruskan dengan teratur apabila tamat perkhidmatan atau bertukar dari PMWP. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Memastikan semua aset ICT Kerajaan dikembalikan kepada PMWP mengikut peraturan yang ditetapkan PMWP dan/atau terma perkhidmatan yang ditetapkan; dan	

b. Membatalkan atau meminda semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan.	
0402 Pendidikan	
Objektif : Meningkatkan pengetahuan dan kesedaran mengenai kepentingan keselamatan ICT.	
Program / Aktiviti	**Tanggungjawab**
040201 Program Kesedaran Keselamatan ICT	Semua
Setiap pengguna di PMWP perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah proaktif yang boleh mengurangkan ancaman keselamatan ICT PMWP.	
0403 Tindakan Tatatertib	
Objektif : Meningkat kesedaran dan pematuhan ke atas Dasar Keselamatan ICT PMWP.	
Program / Aktiviti	**Tanggungjawab**
040301 Penyalahgunaan dan Pelanggaran Dasar	Semua
Pelanggaran Dasar Keselamatan ICT PMWP akan dikenakan tindakan tatatertib.	

PERKARA 05 : KESELAMATAN FIZIKAL DAN PERSEKITARAN	
0501 Keselamatan Kawasan	
Objektif : Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada ruang pejabat dan maklumat.	
Program / Aktiviti	**Tanggungjawab**
050101 Perimeter Keselamatan Fizikal	Pejabat Ketua Pegawai Keselamatan Kerajaan, CIO dan ICTSO
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut : - a. Kawasan keselamatan fizikal hendaklah di kenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; c. Memperkukuhkan dinding dan siling; d. Memasang alat penggera atau kamera (CCTV); e. Menghadkan jalan keluar masuk; f. Mewujudkan sistem kad keselamatan keluar-masuk; g. Mempamerkan papan tanda 'Kawasan Larangan'; h. Menyediakan tempat atau bilik khas untuk pelawat; dan i. Mewujudkan perkhidmatan kawalan keselamatan.	
050102 Kawalan Masuk Fizikal	Semua
Kawalan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar-masuk kawasan premis PMWP.	

a. Setiap pengguna PMWP hendaklah memakai atau mengenakan kad/pas keselamatan sepanjang waktu bertugas; b. Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; c. Semua pas keselamatan hendaklah diserahkan balik kepada jabatan apabila pengguna berhenti atau bersara; d. Setiap pelawat hendaklah mendaftar di pintu utama Keluar - Masuk Jabatan ; e. Kehilangan pas mestilah dilaporkan dengan segera; dan f. Pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT PMWP.	
050103 Kawasan Larangan	Semua
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di PMWP adalah bilik Mufti, bilik Timbalan Mufti, bilik Ketua Penolong Mufti, bilik Ketua Bahagian/Unit, bilik fail dan bilik server. Kemasukan ke bilik-bilik tersebut hanyalah kepada pegawai-pegawai yang diberi kuasa sahaja :- a. Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu; b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; dan Semua penggunaan peralatan yang melibatkan penghantaran, kemaskini dan penghapusan maklumat rahsia rasmi hendaklah	

dikawal dan mendapat kebenaran daripada Ketua Bahagian/Unit bagi setiap Bahagian/Unit.	
0502 Keselamatan Peralatan ICT	
Objektif : Melindung peralatan dan maklumat.	
Program / Aktiviti	**Tanggungjawab**
050201 Peralatan ICT	Semua
Secara umumnya peralatan ICT hendaklah dijaga dan dikawal dengan baik supaya boleh digunakan bila perlu :- a. Setiap pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Semua peralatan hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; c. Setiap pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; dan d. Sebarang bentuk penyelewengan atau salah guna peralatan hendaklah dilaporkan kepada ICTSO.	
050202 Media Storan	Semua
Keselamatan media storan perlu diberi perhatian khusus kerana ianya berupaya menyimpan maklumat yang besar. Langkah-langkah pencegahan seperti berikut hendaklah di ambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang di simpan dalam media storan adalah terjamin dan selamat :- a. Penyediaan ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;	

b. Kebenaran untuk memasuki kawasan penyimpanan media hendaklah terhad kepada mereka atau pengguna yang dibenarkan sahaja; c. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu; dan d. Pergerakan media storan hendaklah direkodkan.	
050203 Media Tandatangan Digital	Semua
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a. Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b. Media ini tidak boleh dipindah milik atau dipinjamkan; dan c. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	
050204 Media Perisian dan Aplikasi	Semua
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan PMWP; b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada *CD-rom, disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d. Source code sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	

050205 Penyenggaraan Peralatan ICT	Pegawai Aset dan Unit ICT
Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti. a. Semua peralatan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b. Peralatan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; c. Semua peralatan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; dan d. Semua penyelenggaraan mestilah mendapat kebenaran daripada Ketua Bahagian/Unit berkenaan.	
050206 Peminjaman Peralatan Untuk Kegunaan Di Luar Pejabat	Semua
Peralatan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan peralatan :- a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat mestilah mendapat kelulusan pegawai atasan dan tertakluk kepada tujuan yang dibenarkan; dan b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan.	
050207 Peralatan di Luar Ruang Pejabat /Bangunan	Semua
Bagi peralatan yang dibawa keluar dari premis PMWP, langkah-langkah keselamatan hendaklah diadakan dengan mengambil kira risiko yang wujud di luar kawalan PMWP :- a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	

050208 Pelupusan	Pegawai Aset dan Unit ICT
Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan PMWP :- a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding degauzing* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan; dan c. Maklumat lanjut pelupusan bolehlah merujuk kepada Pekeliling Perbendaharaan Bil. 5 Tahun 2007- "Tatacara Pengurusan Aset Alih Kerajaan".	
0503 Keselamatan Persekitaran	
Objektif : Melindungi aset ICT PMWP dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
Program / Aktiviti	**Tanggungjawab**
050301 Kawalan Persekitaran	Semua
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah di rujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil :- a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan	

keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h. Akses kepada saluran riser hendaklah sentiasa dikunci.	
050302 Bekalan Kuasa	ICTSO dan Unit ICT
a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT. b. Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	

050303 Kabel	ICTSO dan Unit ICT
Kabel komputer hendaklah dilindungi kerana boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut :- a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindung laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui trunking bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	
050304 Prosedur Kecemasan	Semua dan Pegawai Keselamatan Jabatan
a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MAMPU 2004; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik.	
0504 Keselamatan Dokumen	
Objektif : Melindungi maklumat PMWP dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
Program / Aktiviti	**Tanggungjawab**
050401 Dokumen	

Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi: a. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b. Hendaklah difail dan dilabelkan mengikut klasifikasi seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; c. Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik; dan d. Memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak.	Semua
PERKARA 06 : PENGURUSAN OPERASI DAN KOMUNIKASI	
0601 Pengurusan Prosedur Operasi	
Objektif :Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat.	
Program / Aktiviti	**Tanggungjawab**
060101 Pengendalian Prosedur	Semua
a. Semua prosedur keselamatan ICT yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	

060102 Kawalan Perubahan	Semua
a. Pengubahsuaian yang melibatkan peralatan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pengurus ICT, pegawai atasan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
060103 Prosedur Pengurusan Insiden	ICTSO, Pentadbir Sistem ICT, Pentadbir Rangkaian dan Unit ICT.
Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan, prosedur pengurusan insiden mestilah mengambil kira kawalan berikut :- a. Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan; c. Menyimpan jejak audit dan memelihara bahan bukti; dan d. Menyediakan tindakan pemulihan segera.	

060104 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	Pihak Ketiga
Memastikan pelaksanaan dan penyenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dilaksanakan dan diselenggarakan oleh pihak ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak dan diaudit dari semasa ke semasa; dan c. Pengurusan kepada perubahan penyediaan perkhidmatan termasuk meyelenggarakan dan menambahbaik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	
0602 Perancangan dan Penerimaan Sistem	
Objektif : Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
Program / Aktiviti	**Tanggungjawab**
060201 Perancangan Kapasiti	Pentadbir Sistem ICT
Kapasiti sesuatu kompenan atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang; dan	

Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan kepada perkhidmatan dan kerugian akibat pengubahsuaian yang dirancang.	
060202 Penerimaan Sistem	ICTSO dan Pentadbir Sistem ICT
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	
0603 Perisian Berbahaya	
Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan	
Program / Aktiviti	**Tanggungjawab**
060301 Perlindungan dari Perisian Berbahaya	Semua
a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus dan *Intrusion Detection System* (IDS) dan *Intrusion* Prevention System *(IPS)* mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah Akta Hakcipta (Pindaan) Tahun 1997; c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d. Mengemas kini *pattern* antivirus setiap minggu; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;	

g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
060302 Perlindungan dari *Mobile Code*	Semua
Penggunaan mobile code yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	
0604 *Housekeeping*	
Objektif : Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.	
Program / Aktiviti	**Tanggungjawab**
060401 Penduaan	Semua
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan penduaan seperti yang dibutirkan hendaklah dilakukan setiap kali konfigurasi berubah. Salinan penduaan hendaklah direkodkan dan di simpan di *off site,* diantaranya adalah :- a. Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan operasi; c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan	

berkesan apabila digunakan khususnya pada waktu kecemasan; dan d. *backup* dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat dan hendaklah disimpan sekurang-kurangnya tiga (3) generasi.	
060402 Sistem Log	Unit ICT
a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	
0605 Pengurusan Rangkaian	
Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
Program / Aktiviti	**Tanggungjawab**
060501 Kawalan Infrastruktur Rangkaian	Unit ICT
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan :- a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;	

b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e. *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh Pentadbir Sistem ICT; f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan PMWP; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. Memasang perisian *Intrusion Detection System* (IDS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat PMWP; i. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan"; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan PMWP hendaklah mendapat kebenaran ICTSO; k. Semua pengguna hanya dibenarkan menggunakan rangkaian PMWP sahaja. Penggunaan modem atau melakukan penyambungan ke rangkaian lain atau yang seumpamanya, adalah dilarang sama sekali;	

l. Kemudahan bagi *wireless Local Area Network* (LAN) PMWP dengan pelaksanaan kawalan keselamatan; dan m. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	
0606 Pengurusan Media	
Objektif : Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.	
Program / Aktiviti	**Tanggungjawab**
060601 Penghantaran dan Pemindahan	Semua
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	
060602 Prosedur Pengendalian Media	Pentadbir Sistem ICT dan Semua
a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c. Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat.	

060603 Keselamatan Sistem Dokumentasi	ICTSO dan Pentadbir Sistem ICT
a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	

0607 Keselamatan Komunikasi	
Objektif : Melindungi aset ICT melalui sistem komunikasi yang selamat.	
Program / Aktiviti	**Tanggungjawab**
060701 Internet	Semua
a. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan; b. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan baik, rujukan sumber Internet hendaklah dinyatakan; c. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan sebelum dimuat naik ke Internet; d. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; e. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh PMWP; f. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan	

perbincangan awam ini hendaklah mendapat kelulusan daripada Ketua Jabatan terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; dan g. Maklumat lanjut mengenai keselamatan Internet bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".	
060702 Mel Elektronik	Semua
a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh PMWP sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh PMWP; 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 e-mel penerima adalah betul; e. Menggunakan kaedah inovatif dalam penghantaran fail bersaiz besar seperti menggunakan kaedah muat turun fail dengan memaklumkan lokasi *Universal Resource Location* (URL) atau kaedah pemampatan untuk mengurangkan saiz fail dengan memastikan ciri-ciri keselamatan dilaksanakan; f. penghantaran lampiran dalam format atau *extension*" *.exe, *.bat " dan " *.com" tidak dibenarkan; g. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui; h. menggunakan enkripsi bagi dokumen terperingkat yang dihantar secara elektronik;	

i. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; j. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; k. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; l. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; dan m. Maklumat lanjut mengenai keselamatan e-mel bolehlah merujuk kepada Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".	
060703 Perkhidmatan E-Dagang (*Electronic Commerce Services*)	Semua
Memastikan keselamatan perkhidmatan E-Dagang dan penggunaannya. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Maklumat yang terlibat dalam E-Dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b. Maklumat yang terlibat dalam transaksi dalam talian (*online*) perlu dilindungi bagi mengelakkan penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan masej yang tidak benar atau bersesuaian; dan c. Integriti maklumat yang disediakan dalam sistem untuk kegunaan awam perlu dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	

060704 Paparan Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat umum adalah seperti berikut :- a. Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; b. Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web; dan c. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian.	Semua
0608 Pengurusan Penyampaian Perkhidmatan Pembekal, Pakar Runding dan Pihak-Pihak Lain Yang Terlibat	
Objektif : Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
Program / Aktiviti	**Tanggungjawab**
Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pembekal, pakar runding dan pihak-pihak lain yang terlibat. Perkara-perkara yang mesti dipatuhi termasuk yang berikut :- a. Memasukkan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan disenggarakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pembekal, pakar runding dan pihak-pihak lain yang terlibat perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan	Pengurus ICT dan Pentadbir Sistem ICT

c. Pengurusan ke atas perubahan penyediaan perkhidmatan termasuk menyelenggara dan menambah baik polisi keselamatan, prosedur dan kawalan maklumat sedia ada, perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	
0609 Pemantauan	
Objektif : Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
Program / Aktiviti	**Tanggungjawab**
060901 Pengauditan dan Forensik ICT	ICTSO
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut :- a. Sebarang percubaan pencerobohan kepada sistem ICT PMWP; b. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), spam, pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); c. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f. Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; g. Aktiviti penyalahgunaan akaun e-mel; dan	

h. Aktiviti penukaran alamat IP (*IP address*) selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT.	
060902 Jejak Audit	Pentadbir Sistem ICT dan Pentadbir Rangkaian
Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi : - a. Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan c. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan; Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubah suaian yang tidak dibenarkan.	
060903 Sistem Log	Pentadbir Sistem ICT
Fail log hendaklah disimpan untuk tempoh sekurang-kurangnya enam (6) bulan. Jenis fail log bagi server dan aplikasi yang perlu diaktifkan adalah seperti berikut :- i. Fail log sistem pengoperasian; ii. Fail log servis (contoh: web, e-mel);	

iii. Fail log aplikasi (*audit trail*); dan iv. Fail log rangkaian (contoh : *switch, firewall, IPS*) Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut :- a. mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO.	
060904 Pemantauan Log	Pentadbir Sistem ICT dan Unit ICT
Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d. Aktiviti pentadbiran dan operator sistem perlu direkodkan; e. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; dan f. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam PMWP atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	

PERKARA 07 : KAWALAN CAPAIAN	
0701 Kawalan Capaian	
Objektif : Memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat PMWP.	
Program / Aktiviti	**Tanggungjawab**
070101 Dasar Kawalan Capaian	Semua
Peraturan kawalan hendaklah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan pengurusan PMWP dan keselamatan. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna; b. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c. Kawalan ke atas kemudahan pemprosesan maklumat; dan d. Keselamatan maklumat yang dicapai menggunakan kemudahan peralatan mudah alih.	
0702 Pengurusan Capaian Pengguna	
Objektif : Mengawal capaian pengguna ke atas aset ICT PMWP dengan memastikan bahawa sistem maklumat yang dicapai oleh pengguna yang sah dan menghalang capaian dari pihak pengguna yang tidak sah. Prosedur pendaftaran dan pembatalan kebenaran capaian pengguna perlu diwujudkan dan didokumenkan.	
Program / Aktiviti	**Tanggungjawab**
070201 Akaun Pengguna	

Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-langkah berikut hendaklah dipatuhi :- a. Akaun yang diperuntukkan oleh jabatan sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna yang di wujud pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut :- i. Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	Pentadbir Sistem ICT dan Semua
070202 Hak Capaian	Pentadbir Sistem ICT
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	

Keperluan capaian hendaklah sentiasa dipantau dan dikemas kini bagi memastikan hak capaian ini diberikan kepada pegawai dan kakitangan yang dibenarkan sahaja.	
070203 Pengurusan Kata Laluan	Pentadbir Sistem ICT dan Semua
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh PMWP seperti berikut :- a. dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; c. panjang kata laluan mestilah sekurang-kurangnya dua belas (12) aksara dengan gabungan antara aksara, angka dan aksara khas; d. kekerapan penukaran dan penggunaan kata laluan adalah mengikut ketetapan polisi pengurusan kata laluan yang berkuatkuasa; e. kata laluan windows dan screen saver hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama; f. kata laluan hendaklah diingat dan tidak boleh dicatat, disimpan atau didedahkan dengan apa cara sekalipun; g. kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;	

h. kuatkuasakan pertukaran kata laluan semasa login kali pertama atau selepas login kali pertama atau selepas kata laluan diset semula; i. kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; j. had kemasukan katalaluan bagi capaian kepada sistem aplikasi adalah maksimum tiga (3) kali sahaja. Setelah mencapai tahap maksimum, capaian kepada sistem akan disekat sehingga id capaian diaktifkan semula; k. kata laluan hendaklah disimpan dalam bentuk yang telah dienkripkan; dan l. sistem yang dibangunkan mestilah mempunyai kemudahan menukar kata laluan oleh pengguna.	
070204 *Clear Desk* dan *Clear Screen*	Semua
Prosedur *Clear Desk* dan *Clear Screen* perlu dipatuhi supaya maklumat dalam apa jua bentuk media disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. Perkara-perkara yang mesti dipatuhi termasuk yang berikut :- a. menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer; b. menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c. memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	

0703 Kawalan Capaian Rangkaian	
Objektif : Menghalang capaian yang tidak sah dan tanpa kebenaran serta boleh mewujudkan kerosakan.	
Program / Aktiviti	**Tanggungjawab**
070301 Tanggungjawab Pengguna	Semua
Memastikan pengguna melaksanakan langkah berkesan ke atas kawalan capaian untuk menghalang penyalahgunaan, kecurian maklumat dan kemudahan proses maklumat. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Mematuhi amalan terbaik pemilihan dan penggunaan kata laluan; b. Memastikan kemudahan dan peralatan yang tidak digunakan mendapat perlindungan sewajarnya; dan c. Mematuhi amalan *clear desk/clear screen policy*.	
070302 Capaian Sistem Pengoperasian	Pentadbir Sistem ICT
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi :- a. mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan b. merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut :- a. mengesahkan pengguna yang dibenarkan; b. mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan	

c. menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi termasuk berikut :- a. mengawal capaian ke atas sistem operasi menggunakan prosedur *log on* yang terjamin; b. menghadkan dan mengawal penggunaan program; dan c. mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
070303 Sijil Digital Token /Kad Pintar Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a. penggunaan sijil digital token/kad pintar hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b. token/kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c. perkongsian penggunaan token/kad pintar adalah tidak dibenarkan sama sekali. Token/kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan d. sebarang kehilangan, kerosakan perlu dimaklumkan kepada Meja Bantuan.	Semua
070304 Kawalan Capaian Rangkaian Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan :- a. Menempatkan atau memasang antara muka yang menepati kesesuaian penggunaannya di antara rangkaian PMWP, rangkaian agensi lain dan rangkaian awam; b. Mewujud dan menguatkuasakan makanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya.	ICTSO dan Pentadbir Sistem ICT

Perkara yang perlu dipatuhi adalah seperti berikut :- a. Memastikan pengguna membuat capaian pada sistem yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian PMWP; b. Kaedah C*ontent Filtering* mestilah digunakan bagi mengawal akses internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing, video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; d. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya; e. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/ pegawai yang diberi kuasa; f. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; g. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian/Unit sebelum dimuat naik ke Internet; h. Pengguna hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; i. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh PMWP; j. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan	Pentadbir Rangkaian, Pengurus ICT dan Semua

perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; k. Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan l. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut :- i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian Internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah.	
070305 Kawalan Capaian Aplikasi dan Maklumat	ICTSO dan Pentadbir Sistem ICT
Bertujuan menghalang capaian yang tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi. Capaian sistem dan aplikasi di PMWP adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi :- a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini;	

c. Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja. f. Maklumat tarikh login terakhir hendaklah dipamerkan; dan g. *Session timeout* hendaklah dilaksanakan.	
0704 Peralatan Komputer Mudah Alih dan Kerja Jarak Jauh	
Objektif : Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh	
Program / Aktiviti	**Tanggungjawab**
070401 Peralatan Komputer Mudah Alih dan Kerja Jarak Jauh a. Merekodkan aktiviti keluar masuk penggunaan peralatan mudah alih bagi mengesan kehilangan atau pun kerosakan; b. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan c. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Pegawai Aset dan Semua

PERKARA 8 : PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM	
0801 Keselamatan Dalam Membangunkan Sistem Aplikasi	
Objektif : Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
Program / Aktiviti	**Tanggungjawab**
080101 Keperluan keselamatan	Pemilik Sistem, Pentadbir Sistem ICT dan ICTSO
a. Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan sistem output untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	
080102 Pengesahan *Data Input*	Pemilik Sistem dan Pentadbir Sistem ICT
Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	

080103 Kawalan Prosesan	Pemilik Sistem dan Pentadbir Sistem ICT
Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	
080104 Pengesahan *Data Output*	Pemilik Sistem dan Pentadbir Sistem ICT
Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	
0802 Kawalan Kriptografi	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat.	
Program / Aktiviti	**Tanggungjawab**
080201 Enkripsi	Semua
Pengguna hendaklah membuat enkripsi ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	
080202 Tandatangan Digital	Semua
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik	
080203 Pengurusan Infrastruktur Kunci Awam (PKI)	Semua
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	

0803 Fail Sistem	
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
Program / Aktiviti	**Tanggungjawab**
080301 Kawalan Fail Sistem Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat. a. Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan; dan e. Data ujian perlu dipilih sewajarnya, dikawal penggunaannya serta dilindungi.	Pemilik Sistem dan Pentadbir Sistem ICT
0804 Proses Pembangunan dan Sokongan	
Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
Program / Aktiviti	**Tanggungjawab**
O80401 Prosedur Kawalan Perubahan	

Perkara-perkara yang perlu dipatuhi adalah seperti berikut :- a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b. Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh vendor; c. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; d. Akses kepada kod sumber (source code) aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan e. Menghalang sebarang peluang untuk membocorkan maklumat.	Pemilik Sistem dan Pentadbir Sistem ICT
080402 Pembangunan Secara *Outsources*	Pemilik Sistem, Pengurus ICT dan Pentadbir Sistem ICT
Pembangunan perisian aplikasi secara *outsource* hendaklah mematuhi perkara-perkara berikut :- a. setiap projek perlu dipantau oleh Pengurus ICT; b. kontrak perbekalan hendaklah memasukkan klausa kod sumber menjadi hak milik PMWP; c. kod sumber yang diserahkan kepada PMWP mesti bebas daripada sebarang ralat dan kerentanan; d. mengutamakan kepakaran teknologi tempatan; e. pembangunan aplikasi hendaklah dijalankan dalam persekitaran pengkomputeran PMWP; f. penggunaan *data masking* semasa pengujian;	

g. data ujian hendaklah dilupuskan secara kekal (*secured delete*) selepas projek disiapkan/tamat kontrak; dan h. aktiviti sandaran hendaklah berjaya dilakukan sebelum projek tamat.	
080403 Kawalan Teknikal Keterdedahan (*Vulnerability*)	Pentadbir Sistem ICT
Kawalan teknikal keterdedahan perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut :- a. memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b. menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c. mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	
PERKARA 09 : PENGURUSAN INSIDEN KESELAMATAN ICT	
0901 Pengurusan Insiden Keselamatan ICT	
Objektif : Memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan serta meminimumkan kesan insiden keselamatan ICT.	
Program / Aktiviti	**Tanggungjawab**
090101 Mekanisme Pelaporan Insiden Keselamatan ICT	Semua
a. Pelaporan Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan PMWP CERT untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan.	

b. PMWP CERT

Pasukan PMWP CERT akan bertindak dan menghubungi NACSA sebagai makluman atau bagi mendapatkan bantuan.

c. Tanggungjawab Pengguna

Semua pengguna perlu segera melaporkan sebarang kejadian insiden keselamatan ICT bagi mengelakkan kerosakan bahan bukti tanpa melaksanakan tindakan secara sendirian.

d. Tindakan Dalam Keadaan Berisiko Tinggi

Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak.

e. Sekiranya berlaku sesuatu keadaan yang mencurigakan seperti di bawah, insiden keselamatan ICT hendaklah dilaporkan kepada ICTSO dan PMWP CERT dengan kadar segera :-

i. maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa;

ii. sistem maklumat digunakan tanpa kebenaran atau yang disyaki sedemikian;

iii. kata laluan atau mekanisme kawalan akses yang hilang, dicuri, didedahkan atau yang disyaki sedemikian;

iv. berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal berfungsi atau dicapai, dan komunikasi tersalah hantar; dan

v. berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka yang boleh menjejaskan keselamatan ICT.

f. ICTSO melaporkan kepada NACSA apabila berlaku sebarang insiden keselamatan ICT sekiranya perlu. g. Tanggungjawab Pentadbir Sistem ICT Pentadbir Sistem ICT yang terlibat diingatkan perlu melaporkan sebarang kejadian yang melibatkan keselamatan ICT kepada PMWP CERT dan ICTSO PMWP.	
090102 Prosedur Pengurusan dan Pengendalian Insiden Keselamatan ICT	ICTSO dan PMWP CERT
Pasukan Pengendali Insiden (CERT) PMWP perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur pengurusan pelaporan dan pengendalian insiden keselamatan ICT PMWP di **Lampiran 2**. PMWP CERT menerima aduan atau laporan daripada pengguna, laporan yang dikesan dari pihak MAMPU atau laporan dari sumber lain. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden kemudiannya dimaklumkan kepada pihak NACSA. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguatkuasa undang-undang. PMWP CERT yang diketuai oleh Pengarah CERT akan menjalankan tindakan pengendalian secara capaian jauh (*remote*) atau *on-site*. Sekiranya laporan tersebut memerlukan bantuan pihak NACSA, permohonan akan dihantar bagi mendapatkan maklum balas pihak NACSA.	

Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan akan dihantar melalui pihak NACSA dan khidmat nasihat akan disalurkan. PMWP CERT seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya PKP perlu diaktifkan atau sebaliknya. Pengesahan akan dihantar kepada CIO bagi mengaktifkan PKP. Laporan insiden yang tidak memerlukan PKP akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan. Prosedur pengurusan insiden perlu diwujudkan dan didokumenkan. Pengendalian insiden keselamatan ICT perlu diuruskan dengan cepat, teratur dan berkesan. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Mengenal pasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. Menyediakan pelan kotigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c. Menyimpan jejak audit dan memelihara bahan bukti; d. Menyediakan pelan tindakan pemulihan segera; e. Menyediakan tindakan pencegahan supaya insiden serupa tidak berulang; dan f. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	

PERKARA 10 : PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	
1001 Dasar Kesinambungan Perkhidmatan	
Objektif Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
Program / Aktiviti	**Tanggungjawab**
100101 Pelan Kesinambungan Perkhidmatan	ICTSO
Pelan kesinambungan perkhidmatan hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT dan perkara-perkara berikut perlu diberi perhatian :- a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; c. Mendokumentasikan proses dan prosedur yang telah dipersetujui; d. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; e. Membuat penduaan; dan f. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.	

PERKARA 11 : PEMATUHAN	
1101 Pematuhan dan Keperluan Perundangan	
Objektif : Meningkatkan tahap keselamatan ICT bagi mengelak berlakunya pelanggaran kepada Dasar Keselamatan ICT PMWP.	
Program / Aktiviti	**Tanggungjawab**
110101 Pematuhan Dasar	Semua
Setiap pengguna di PMWP hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT PMWP dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT di PMWP termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan.	
110102 Keperluan Perundangan	Semua
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di PMWP :- a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 - "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"; c. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002; d. Pekeliling Am Bilangan 1 Tahun 2001 - "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)";	

e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; f. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; g. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; h. Surat Arahan Ketua Setiausaha Negara - Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006; i. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007; j. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007; k. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK); l. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender; m. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan; n. Akta Tandatangan Digital 1997; o. Akta Rahsia Rasmi 1972; p. Akta Jenayah Komputer 1997; q. Akta Hak Cipta (Pindaan) Tahun 1997;	

r. Akta Komunikasi dan Multimedia 1998; s. Perintah-Perintah Am; t. Arahan Perbendaharaan; u. Arahan Teknologi Maklumat 2007; v. Garis Panduan Keselamatan MAMPU 2004; w. Standard Operating Procedure (SOP) ICT PMWP; x. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009; dan y. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.	
110103 Pematuhan Kepada Dasar, Piawaian dan Teknikal Keselamatan	Semua
Dasar ini bertujuan memastikan keselamatan maklumat disemak secara berkala supaya penggunanya patuh dan selaras dengan dasar dan piawaian keselamatan PMWP. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Pegawai penyelia hendaklah memastikan bahawa semua peraturan keselamatan di bawah kawal selia masing-masing dipatuhi selaras dengan perundangan, peraturan dan lain-lain keperluan keselamatan; dan b. Sistem maklumat hendaklah disemak dan diuji secara berkala untuk memastikan ia memenuhi pelaksanaan piawaian keselamatan yang ditetapkan.	

LAMPIRAN 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT (DKICT)
PEJABAT MUFTI WILAYAH PERSEKUTUAN

Nama (Huruf Besar) : ……
No. Kad Pengenalan : ……
Jawatan : ……
Bahagian/Unit (PMWP) : ……
Organisasi (selain warga PMWP) : ……
No. Kontrak (jika berkaitan) : ……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

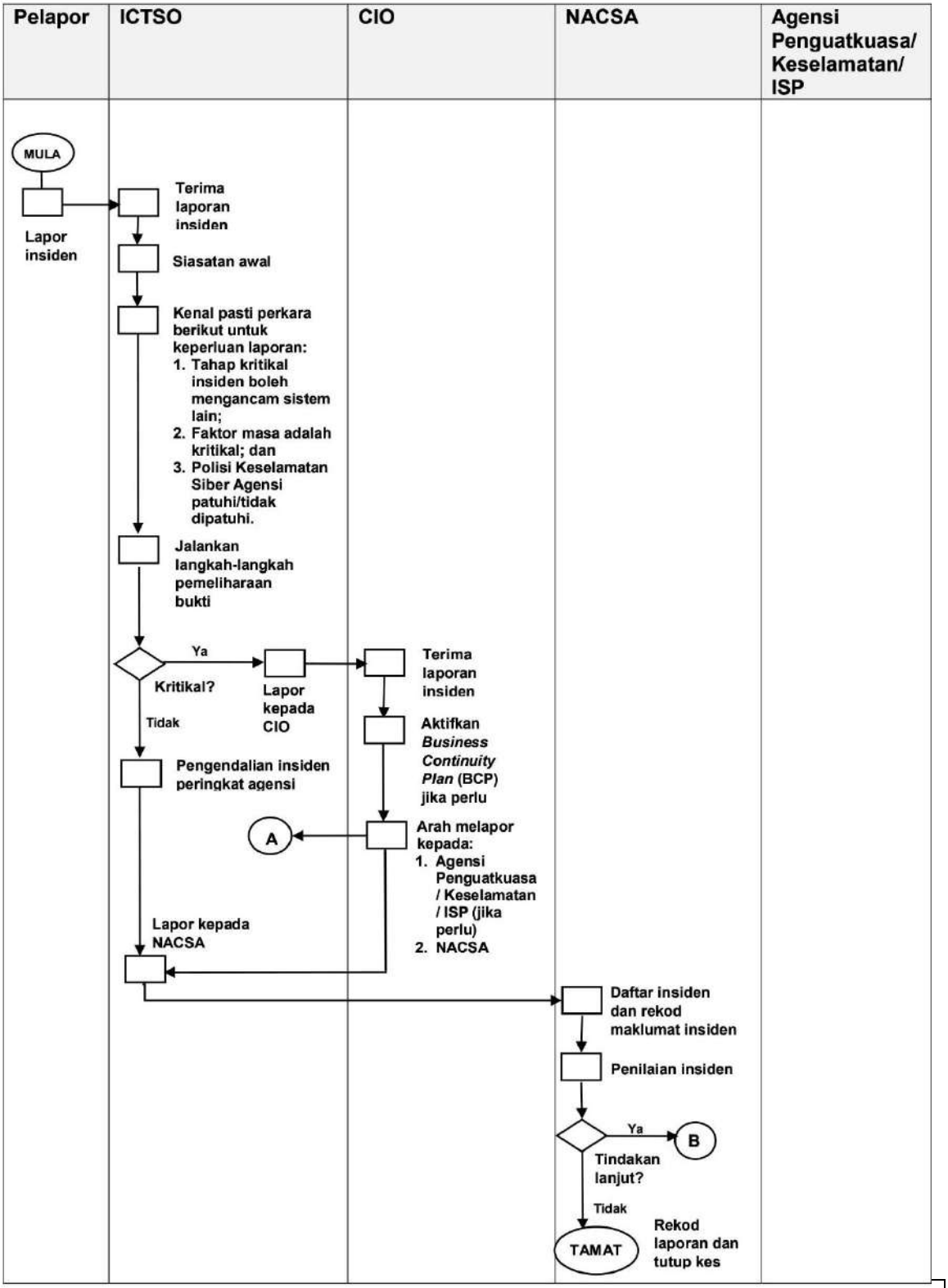
……..

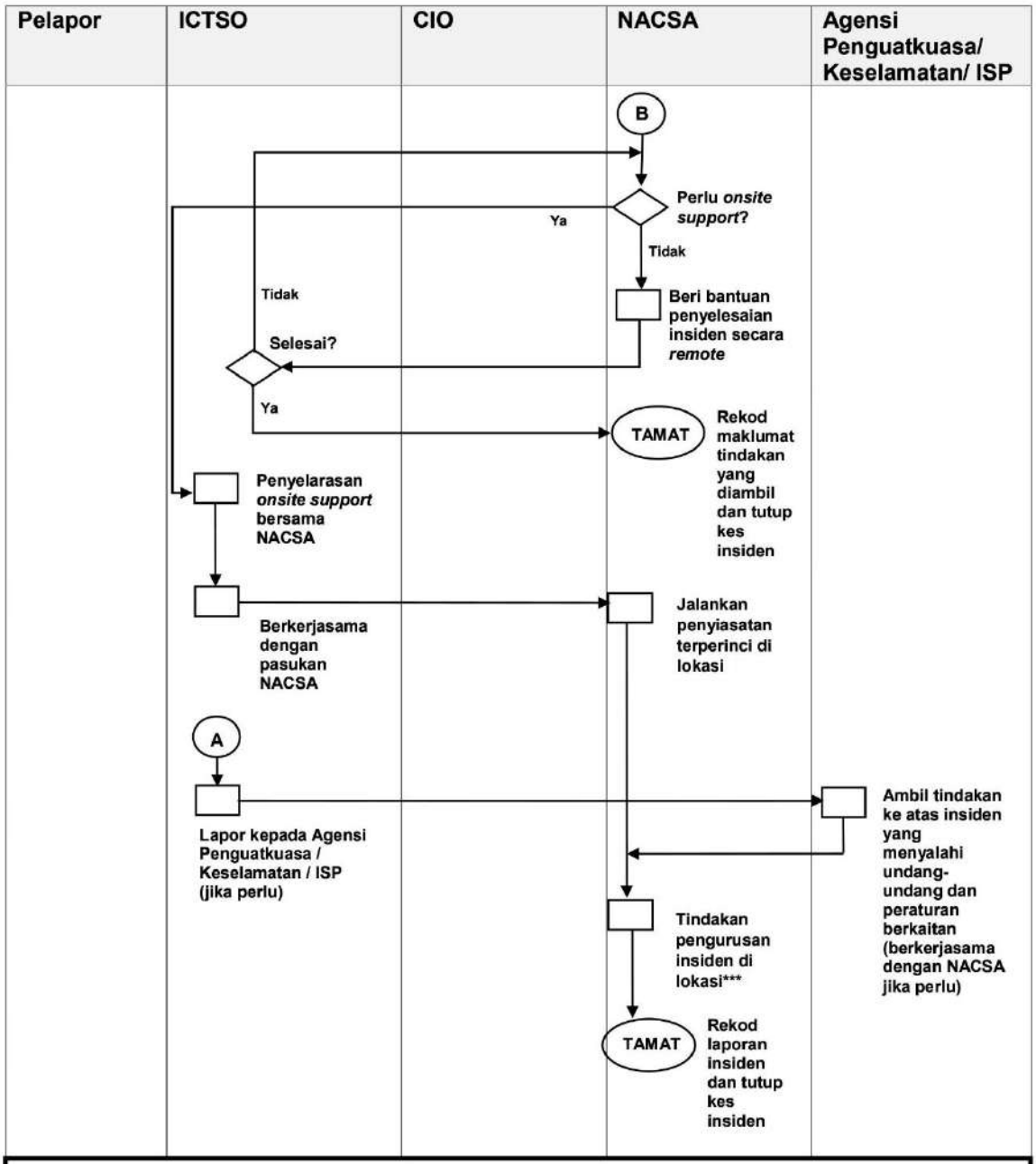
(Nama Pegawai Keselamatan ICT)
b.p Mufti Wilayah Persekutuan

Tarikh: ……

LAMPIRAN 2

CARTA ALIR PENGENDALIAN INSIDEN KESELAMATAN ICT





***** Tindakan pengurusan insiden di lokasi:**

1. Kawal kerosakan;
2. Baik pulih minima dengan segera;
3. Siasat insiden dengan terperinci;
4. Analisis impak (Business Impact Analysis);
5. Hasilkan laporan insiden;
6. Bentang dan kemukakan laporan kepada agensi; dan
7. Selaraskan tindakan di antara agensi dan Agensi Penguatkuasa/Keselamatan/ISP (jika berkenaan).