DASAR KESELAMATAN ICT

Versi 2.0

KEMENTERIAN PEMBANGUNAN WANITA, KELUARGA DAN MASYARAKAT

SERTA

AGENSI DI BAWAHNYA

31 MAC 2011

PERUTUSAN

KETUA SETIAUSAHA

KEMENTERIAN PEMBANGUNAN WANITA,

KELUARGA DAN MASYARAKAT (KPWKM)

DASAR KESELAMATAN ICT (DKICT) VERSI 2

Assalamualaikum wrt wbt dan Salam Sejahtera,

Setinggi-tinggi kesyukuran dipanjatkan ke hadrat Allah S.W.T kerana dengan limpah kurnia dan izinNya, Dasar Keselamatan ICT Kementerian Pembangunan Wanita, Keluarga dan Masyarakat (KPWKM) versi 2 telah berjaya dibangunkan. Sekalung penghargaan dan tahniah juga dirakamkan kepada Bahagian Pengurusan Maklumat (BPM) Kementerian, agensi-agensi di bawah KPWKM dan Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) di atas usaha, tenaga, idea dan komitmen yang dicurahkan dalam melaksanakan kajian semula dokumen Dasar Keselamatan ini.

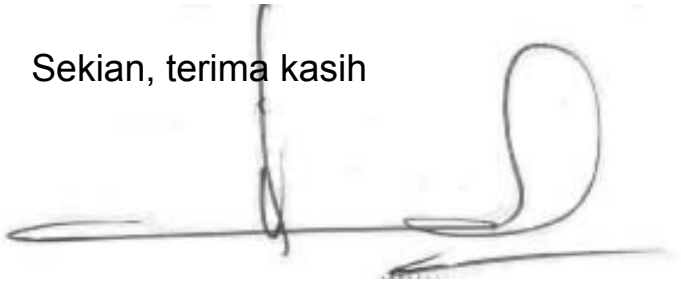
Dasar Keselamatan ICT (DKICT) KPWKM telah diwujudkan buat julung kalinya pada 26 Julai 2007 sebagai panduan dan rujukan kepada warga KPWKM dalam memenuhi keperluan penguatkuasaan, kawalan dan langkah-langkah menyeluruh untuk melindungi aset ICT Kerajaan dan seterusnya menjamin kesinambungan urusan Kerajaan.

Dalam pada itu, ledakan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial yang begitu dinamik dalam dunia

ICT sama ada di peringkat domestik mahu pun global menuntut kepada pelaksanaan kajian semula ke atas DKICT KPWKM bagi memastikan ia sentiasa relevan dan menepati peredaran zaman. Hasilnya, DKICT KPWKM versi 2 telah dihasilkan yang mana kandungannya adalah bersesuaian dengan kehendak dan keperluan semasa berhubung isu-isu perlindungan dan keselamatan ICT KPWKM, seterusnya menjamin operasi ICT di Kementerian ini sentiasa berterusan tanpa sebarang gangguan dan risiko ancaman keselamatan.

Akhir kata, besar harapan saya agar DKICT KPWKM versi 2 turut dijadikan sebagai wadah oleh semua warga KPWKM untuk meningkatkan rasa tanggungjawab dalam penggunaan aset ICT Kerajaan khususnya di Kementerian ini bagi memastikan aspek keselamatan ICT di Kementerian ini berada pada tahap yang tinggi.

Sekian, terima kasih



.....

(DATO' DR. NOORUL AINUR MOHD. NUR)

21 APRIL 2011

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
02 April 2007	1.0	Ketua Setiausaha	26 Julai 2007
22 Oktober 2010	2.0	Ketua Setiausaha	31 Mac 2011

ISI KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT (DKICT) ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) di KPWKM dan Agensi. Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT. Dasar ini adalah digunapakai oleh semua kakitangan KPWKM dan Agensi. Oleh itu istilah Jabatan digunakan di dalam dasar ini bagi merujuk kepada KPWKM dan Agensi.

Agensi di bawah KPWKM adalah seperti berikut:

(a) JKM - Jabatan Kebajikan Masyarakat

(b) JPW - Jabatan Pembangunan Wanita

(c) ISM - Institut Sosial Malaysia

(d) NIEW - NAM Institute for the Empowerment of Women Malaysia

(e) LPPKN - Lembaga Penduduk dan Pembangunan Keluarga Negara

OBJEKTIF

Dasar Keselamatan ICT diwujudkan untuk menjamin kesinambungan urusan Jabatan dengan meminimumkan kesan insiden keselamatan ICT.

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi Jabatan. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT ialah seperti berikut:

(a) Memastikan kelancaran operasi Jabatan dan meminimumkan kerosakan atau kemusnahan;

(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

(c) 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 suatu 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:

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;
(b) Menjamin setiap maklumat adalah tepat dan sempurna;
(c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan
(d) Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar Keselamatan ICT merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(a) Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

(b) Integriti - Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan;

(c) Tidak Boleh Disangkal - Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

(d) Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan

(e) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT; 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 Jabatan terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT menetapkan keperluan-keperluan asas berikut:

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

(b) Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan ketepatan maklumat serta untuk melindungi kepentingan kerajaan, perkhidmatan dan masyarakat.

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

(a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan jabatan. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem

pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada Jabatan;

(c) Perkhidmatan

Perkhidmatan atau sistem yang menyokong aset lain untuk melaksanakan fungsi-fungsinya. Contoh:

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;

ii. Sistem halangan akses seperti sistem kad akses; dan

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

(d) Data atau Maklumat

Koleksi fakta-fakta dalam bentuk kertas atau mesej elektronik, yang mengandungi maklumat-maklumat untuk digunakan bagi mencapai misi dan objektif Jabatan. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod Jabatan, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

(e) Manusia

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

(f) Premis Komputer Dan Komunikasi

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

Setiap perkara di atas perlu diberi perlindungan rapi. Sebarang kebocoran rahsia atau kelemahan perlindungan adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

PRINSIP-PRINSIP

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

(a) Akses atas dasar perlu mengetahui

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

(b) Hak akses minimum

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

(c) Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

ii. Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

iii. Menentukan maklumat sedia untuk digunakan;

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

Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

(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 di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

(e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan.

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

(f) 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

(g) 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

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

Jabatan 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 Jabatan 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.

Jabatan 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.

Jabatan 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-pihak lain yang berkepentingan.

BIDANG 01
DASAR KESELAMATAN ICT

0101 Dasar Keselamatan ICT

Objektif:

Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan Jabatan serta tertakluk kepada perundangan yang berkaitan.

010101 Pelaksanaan Dasar

Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha (KSU) KPWKM selaku Pengerusi Jawatankuasa Pemandu ICT (JPICT) KPWKM.	KSU KPWKM

010102 Penyebaran Dasar

Dasar ini perlu disebarkan kepada semua warga Jabatan (termasuk kakitangan, pembekal, pakar runding dan lain-lain).	ICTSO Jabatan

010103 Penyelenggaraan Dasar

Dasar Keselamatan ICT ini adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT: (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemuka cadangan pindaan secara bertulis kepada ICTSO	ICTSO Jabatan

Jabatan untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT) Jabatan; Maklum kepada semua pengguna perubahan yang telah dipersetujui oleh JPICT Jabatan; dan (c) Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	
010104 Pengecualian Dasar	
Dasar Keselamatan ICT adalah terpakai kepada semua pengguna di Jabatan termasuk pihak ketiga yang memberi perkhidmatan ICT dan tiada pengecualian diberikan.	Semua

BIDANG 02
ORGANISASI KESELAMATAN

0201 Infrastruktur Organisasi Dalaman

Objektif:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT.

020101 Ketua Setiausaha KPWKM / Ketua Jabatan

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

020102 Ketua Pegawai Maklumat (CIO)

Ketua Pegawai Maklumat (CIO) adalah seperti berikut: KPWKM – Timbalan Ketua Setiausaha (Pengurusan) KPWKM,	CIO

JKMM – Timbalan Ketua Pengarah (Operasi) JPW – Timbalan Ketua Pengarah LPPKN – Timbalan Ketua Pengarah (Pengurusan) ISM – Timbalan Pengarah NIEW – Ketua Penolong Pengarah (3) Peranan dan tanggungjawab CIO adalah seperti berikut: (a) Membantu Ketua Jabatan 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 serta pengurusan risiko dan pengauditan; dan (d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT.	
020103 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Keselamatan ICT (ICTSO) bagi KPWKM ialah Ketua Unit Operasi dan Rangkaian, Bahagian Pengurusan Maklumat (BPM) manakala ICTSO bagi Agensi di bawahnya ialah Pegawai Teknologi Maklumat yang dilantik. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: (a) Mengurus keseluruhan program-program keselamatan ICT; (b) Menguatkuasakan pelaksanaan Dasar Keselamatan ICT; (c) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT kepada semua kakitangan;	ICTSO

(d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT; (e) Menjalankan pengurusan risiko; (f) Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan 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 CIO dan Pasukan Tindak Balas Insiden Keselamatan ICT Agensi (CERT); (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; dan (k) Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
020104 Pengurus ICT	
Pengurus ICT adaalah seperti berikut: KPWKM – Pengurus Bahagian Pengurusan Maklumat; JKMM – Pengurus IT Cawangan Teknologi Maklumat; JPW – Pengarah Bahagian Khidmat Pengurusan;	Pengurus ICT

LPPKN – Pengarah Bahagian Teknologi Maklumat; ISM – Ketua Unit Teknologi Maklumat;dan NIEW – Ketua Unit Teknologi Maklumat. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT; (b) Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan Jabatan; (c) Menentukan kawalan akses pengguna terhadap aset ICT Jabatan; (d) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; (e) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KPWKM dan Jabatan; 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.	
020105 Pentadbir Sistem ICT	
Pentadbir Sistem ICT ialah Pegawai ICT yang dilantik. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT; (b) Menjaga kerahsiaan kata laluan; (c) Menjaga konfigurasi aset ICT (d) Mengambil tindakan yang bersesuaian dengan segera apabila	Pentadbir Sistem ICT

dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (e) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai pengguna luar dan pihak ketiga yang berhenti atau tamat projek; (f) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT; (g) Memantau aktiviti capaian harian sistem aplikasi pengguna; (h) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (i) Menganalisis dan menyimpan rekod jejak audit; (j) Menyediakan laporan mengenai aktiviti capaian secara berkala; dan (k) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik.	
020106 Pemilik Sistem	
Sesuatu Sistem perlu dimiliki oleh sesuatu Unit/Bahagian di Jabatan yang mempunyai kepentingan terhadap sistem yang dibangunkan. Pemilik Sistem adalah terdiri daripada Ketua Jabatan atau Ketua Unit/Bahagian yang terlibat dengan sistem yang dibangunkan. Peranan dan tanggungjawab Pemilik Sistem adalah seperti berikut:	Pemilik Sistem ICT

(a) Mempromosikan pelaksanaan sistem kepada pengguna sasaran (b) Menentukan pengguna dan kategori atau tahap capaian pengguna sistem (c) Menguruskan senarai pengguna yang telibat di dalam Latihan Pengguna. (d) Menguatkuasakan penggunaan sistem di kalangan pengguna (e) Memantau perlaksaan dan keberkesanan sistem sistem secara berterusan. (f) Memaklumkan sebarang masalah dan keperluan peningkatan sistem kepada pembangun sistem Pemilik sistem hendaklah melantik seorang pegawai sebagai Pentadbir Sistem untuk tujuan penyelenggaraan sistem tersebut.	
020107 Pentadbir Rangkaian ICT	
Pentadbir Rangkaian ICT adalah Pegawai ICT yang dilantik. Peranan dan tanggungjawab Pentadbir Rangkaian ICT adalah seperti berikut: (a) Mentadbir akaun pengguna; (b) Merangka, melaksana dan menguatkuasa polisi keselamatan seperti perlindungan dan perkongsian data; (c) Merancang dan melaksana polisi ancaman keselamatan, memantau keadaan rangkaian dan mengawal penggunaan sumber; (d) Menyelia dan membuat proses backup server; dan (e) Memberi bantuan dalam menyelesaikan masalah-masalah yang dilaporkan oleh pengguna ICT.	Pentadbir Rangkaian ICT

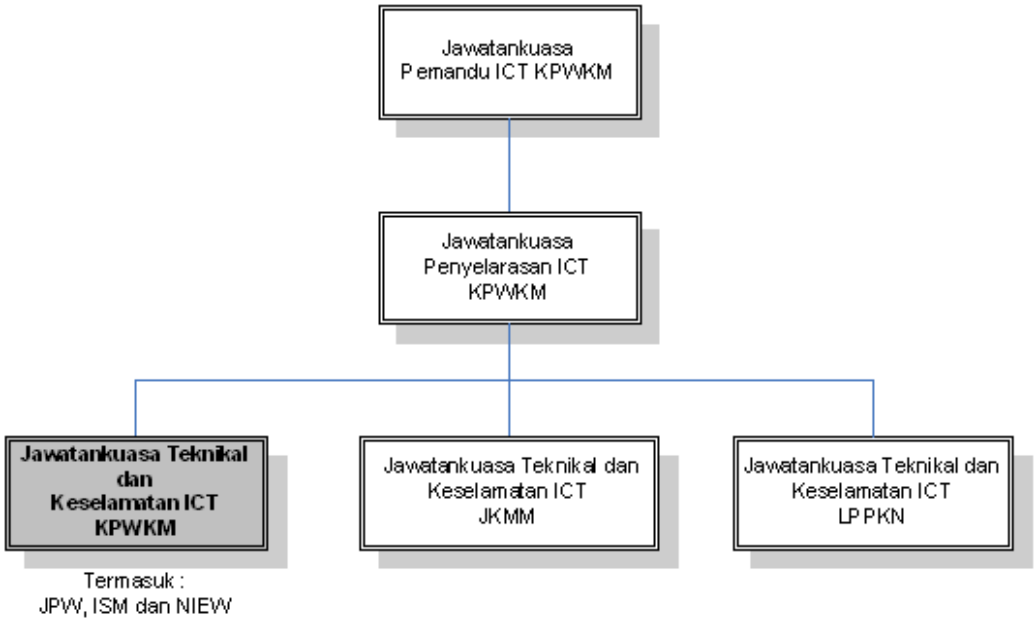
020108 Pengguna

Pengguna adalah warga Jabatan yang menggunakan perkhidmatan ICT dan mempunyai peranan seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT; (b) Menjaga kerahsiaan maklumat Kerajaan yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan;Menjaga kerahsiaan kata laluan; (c) Memastikan maklumat berkaitan adalah tepat dan lengkap dari semasa ke semasa; (d) Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum; (e) Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; (f) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat; (g) Melaksanakan prinsip-prisip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat; (h) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; (i) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan (j) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT sebagaimana **Lampiran 1**.	Pengguna

020109 Tadbir Urus Pengurusan Keselamatan ICT KPWKM

JPICT

Struktur Tadbir Urus Pengurusan Keselamatan ICT adalah seperti carta di bawah:



Bidang kuasa:

(a) Memperakukan/meluluskan dokumen Dasar Keselamatan ICT;

(b) Memantau tahap pematuhan keselamatan ICT;

(c) Memperaku garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam Jabatan yang mematuhi keperluan DKICT;

(d) Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT;

(e) Memastikan DKICT selaras dengan dasar-dasar ICT kerajaan semasa;

(f) Menerima laporan dan membincangkan hal-hal keselamatan ICT semasa;

(g) Membincang tindakan yang melibatkan pelanggaran DKICT; dan (h) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	
020110 Pasukan Tindak Balas Insiden Keselamatan ICT (CERT) KPWKM	
Keanggotaan CERT adalah seperti berikut: **Pengarah** : Pengurus BPM, KPWKM **Pengurus** : ICTSO KPWKM **Ahli** : 1. Semua Ketua Unit BPM, KPWKM; 2. Pegawai Teknologi Maklumat Agensi yang dilantik; dan 3. Penolong Pegawai Teknologi Maklumat Agensi yang dilantik. Peranan dan tanggungjawab CERT adalah seperti berikut: (a) Menerima dan mengesan aduan keselamatan ICT serta 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) Menasihati Jabatan mengambil tindakan pemulihan dan pengukuhan; (e) Menyebarkan maklumat berkaitan pengukuhan keselamatan ICT kepada Jabatan	CERT KPWKM

0202 Pihak Ketiga

Objektif:

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

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga

Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT; (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 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; ii. Tapisan Keselamatan iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. (f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT sebagaimana **Lampiran 1**.	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem ICT dan Pihak Ketiga

BIDANG 03
PENGURUSAN ASET

0301 Akauntabiliti Aset

Objektif:

Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT.

030101 Inventori Aset ICT

Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini;' (b) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemas kini; (c) Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (d) Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di Jabatan; (e) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, di dokumen dan dilaksanakan; dan (f) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya.	Pentadbir Sistem dan Semua

0302 Pengelasan dan Pengendalian Maklumat

Objektif:

Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.

030201 Pengelasan Maklumat

Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan. 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	Semua

030202 Pengendalian Maklumat

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;	Semua

(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.

BIDANG 04
KESELAMATAN SUMBER MANUSIA

0401 Keselamatan Sumber Manusia Dalam Tugas Harian

Objektif:

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

040101 Sebelum Perkhidmatan

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

040102 Dalam Perkhidmatan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan kakitangan Jabatan dan pihak ketiga yang berkepentingan mengurus keselamatan ICT berdasarkan	Semua

perundangan dan peraturan yang ditetapkan; (b) Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; (c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas kakitangan Jabatan dan pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan; dan (d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Pengurusan Sumber Manusia Jabatan masing-masing.	
040103 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada Jabatan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan (b) Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh Jabatan dan/atau terma perkhidmatan.	Semua

BIDANG 05
KESELAMATAN FIZIKAL DAN PERSEKITARAN

0501 Keselamatan Kawasan

Objektif:

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

050101 Kawalan Kawasan

Ini bertujuan untuk menghalang akses tanpa kebenaran, kerosakan dan gangguan secara fizikal terhadap premis, aset ICT dan maklumat Jabatan. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada 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 litar tertutup; (d) Menghadkan laluan 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	Ketua Jabatan, Pegawai Keselamatan Jabatan

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.	
050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Setiap kakitangan Jabatan hendaklah memakai atau mengenakan kad pengenalan Jabatan sepanjang waktu bertugas; (b) Semua kad pengenalan Jabatan hendaklah diserahkan balik kepada Bahagian Khidmat Pengurusan Jabatan apabila kakitangan Jabatan berhenti atau bersara; (c) Setiap pelawat hendaklah mendapatkan Pas Pelawat di pintu kawalan utama premis Jabatan. Amalan ini juga perlu dipatuhi oleh semua cawangan-cawangan Jabatan di peringkat negeri. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; (d) Kehilangan pas mestilah dilaporkan dengan segera.	Semua
050103 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan	Pentadbir

kepada pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset dan maklumat ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di Jabatan adalah Pusat Data, Bilik Server, Ruang Kerja ICT, Bilik Fail dan Stor Peralatan ICT. (a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; dan (b) Pihak ketiga adalah dilarang untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai.	Sistem

0502 Keselamatan Peralatan

Objektif:

Melindungi peralatan ICT Jabatan dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

050201 Peralatan ICT

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) kakitangan Jabatan hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) kakitangan Jabatan bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; (c) kakitangan Jabatan dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT;	Semua

(d) kakitangan Jabatan dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pengurus ICT;

(e) kakitangan Jabatan adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

(f) kakitangan Jabatan mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan;

(g) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;

(h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran;

(i) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS);

(j) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches*, *hub*, *router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci;

(k) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai;

(l) Peralatan ICT yang hendak dibawa keluar dari premis Jabatan, perlulah mendapat kelulusan ICTSO dan Pegawai Aset serta direkodkan bagi tujuan pemantauan;

(m) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset dengan segera;

(n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk

kepada peraturan semasa yang berkuat kuasa; (o) kakitangan Jabatan tidak dibenarkan mengubah kedudukan komputer dari tempat asal ia ditempatkan tanpa kebenaran ICTSO dan Pegawai Aset ; (p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada ICTSO dan Pegawai Aset untuk dibaik pulih; (q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (r) kakitangan Jabatan dilarang menggunakan kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT; (s) kakitangan Jabatan bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; dan (t) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.	
050202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, *thumb drive, external hard disk* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (g) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat;	Semua

(h) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada kakitangan Jabatan yang dibenarkan sahaja; (i) Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; (j) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan daripada dipecahkan, api, air dan medan magnet; (k) Akses dan pergerakan media storan hendaklah direkodkan; (l) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; (m) Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; (n) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan (o) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	
050203 Media Tandatangan Digital	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) kakitangan Jabatan hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;	Semua

(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	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan Jabatan; (b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; (c) Perolehan lesen dan sijil perisian mestilah didaftarkan atas nama Jabatan dan menjadi hak milik Jabatan; (d) 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 (e) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua
050205 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pegawai Aset dan Bahagian/Unit ICT Jabatan

(a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan kakitangan Jabatan sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	
050206 Peralatan di Luar Premis	
Perkakasan yang dibawa keluar dari premis Jabatan adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan perlu dilindungi dan dikawal sepanjang masa; dan (b) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Semua
050207 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak	Semua,

boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh Jabatan dan ditempatkan di Jabatan dan semua cawangan di peringkat negeri. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan Jabatan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; (b) Sekiranya maklumat perlu disimpan, maka kakitangan Jabatan bolehlah membuat penduaan; (c) Peralatan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; (d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (e) Peralatan yang hendak dilupus hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (f) Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset (SPA); (g) Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan (h) Kakitangan Jabatan adalah **DILARANG** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak	Pegawai Aset , Bahagian/Unit ICT KPWKM

dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hard disk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti *Audio Video Recorder (AVR)*, *speaker* dan peralatan yang berkaitan ke mana-mana bahagian di Jabatan; iii. Memindah keluar dari Jabatan mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab Unit Pengurusan Aset Jabatan; dan v. Bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
0503 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT Jabatan dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Pelan perlindungan fizikal perlulah disedia, dibentuk dan dilaksanakan bagi menjamin keselamatan persekitaran daripada ancaman bencana seperti kebakaran, banjir, gempa bumi, letupan, kejadian di luar jangka dan lain-lain	Semua

secara semulajadi atau buatan manusia *(man-made).* Perkara-perkara berikut bolehlah dipertimbangkan bagi menjamin keselamatan persekitaran: (a) Bahan mudah terbakar, meletup atau bahan cecair hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; (b) Peralatan alternatif dan media *backup* perlulah diletakkan berasingan di tempat yang selamat untuk mengelakkan bencana yang terjadi di premis utama; (c) 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; (d) Peralatan perlindungan seperti alat pemadam api hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; (e) Akses kepada saluran *riser* hendaklah sentiasa dikunci; (f) Semua peralatan perlindungan hendaklah disemak dan dipantau dari semasa ke semasa; dan (g) Pengujian peralatan perlindungan perlulah dijalankan sekurang-kurangnya satu (1) kali dalam setahun.	
050302 Bekalan Utiliti	
Bekalan utiliti merupakan semua kemudahan utiliti seperti bekalan elektrik, bekalan air, alat penghawa dingin, saluran kumbahan dan lain-lain yang perlu dilindungi dari kegagalan fungsi atau gangguan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Bahagian/Unit ICT, Jabatan / Bahagian Khidmat Pengurusan

(a) Semua peralatan ICT hendaklah dilindungi daripada kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; (b) Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal supaya mendapatkan bekalan kuasa berterusan; (c) Suis kecemasan perlu ditempatkan berhampiran laluan kecemasan. Lampu kecemasan perlu disediakan dan berfungsi sekiranya berlaku gangguan bekalan kuasa; (d) Bekalan air perlu mencukupi bagi memastikan sistem penghawa dingin berfungsi dengan baik; dan (e) Semua peralatan sokongan bekalan utiliti perlu disemak dan diuji secara berjadual.	dan ICTSO
050303 Kabel	
Kabel bekalan kuasa dan telekomunikasi hendaklah dilindungi dari gangguan dan kerosakan. 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) Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Bahagian/Unit ICT Jabatan/ Bahagian Khidmat Pengurusan dan ICTSO

050304 Prosedur Kecemasan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap kakitangan Jabatan hendaklah membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan oleh pegawai keselamatan Jabatan; (b) Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada Pegawai Keselamatan Jabatan; (c) Mengadakan, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa; dan (d) Mengadakan latihan *fire drill* mengikut jadual.	Semua dan Pegawai Keselamatan Jabatan
0504 Keselamatan Dokumen	
Objektif: Melindungi maklumat Jabatan dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050401 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan	Semua

semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan (e) Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	

BIDANG 06
PENGURUSAN OPERASI DAN KOMUNIKASI

0601 Pengurusan Prosedur Operasi

Objektif:

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

060101 Pengendalian Prosedur

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur pengurusan operasi yang diwujud, dikenal pasti dan diguna pakai hendaklah didokumen, 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.	Semua

060102 Kawalan Perubahan

Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai atasan atau pemilik aset ICT terlebih dahulu;	Semua

(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 di rekod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
060103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi; dan (c) Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pengurus ICT dan ICTSO

0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif: Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
060201 Perkhidmatan Penyampaian	
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; (b) Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan (c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Bahagian/Unit ICT Jabatan
0603 Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang.	entadbir Sistem ICT dan ICTSO

Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	
060302 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Penggunaan peralatan dan sistem mestilah dipantau, ditala (*tuned*) dan perancangan perlu dibuat bagi memenuhi keperluan kapasiti akan datang untuk memastikan prestasi sistem di tahap optima; dan b) Kriteria penerimaan untuk peralatan dan sistem baru, peningkatan dan versi baru perlu ditetapkan dan ujian yang sesuai ke atasnya perlu dibuat semasa pembangunan dan sebelum penerimaan sistem.	Pentadbir Sistem ICT dan Pengurus ICT
0604 Perisian Berbahaya	
Objektif: Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *trojan* dan sebagainya.	
060401 Perlindungan dari Perisian Berbahaya	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti Antivirus, *Intrusion Detection System*	Pentadbir Sistem ICT dan

(IDS), *Intrusion Prevention System* (IPS), *firewall,* serta mengikut prosedur penggunaan yang betul dan selamat; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; (c) Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; (d) Mengemas kini anti virus dengan *pattern* antivirus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; (g) Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; (h) Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan (i) Memberi makluman dan panduan mengenai ancaman keselamatan ICT seperti serangan virus.	ICTSO
060402 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Kawalan pencegahan, pengesahan dan pemulihan untuk melindungi daripada *malicious code*; dan	Semua

b) Dalam keadaan di mana *mobile code* dibenarkan, konfigurasinya hendaklah memastikan bahawa ia beroperasi berdasarkan kepada dasar keselamatan yang jelas.	
0605 Housekeeping (*Back-up)*	
Objektif: Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
060501 *Information Back-up*	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. (a) Perkara-perkara yang perlu dipatuhi adalah seperti berikut:Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; (c) Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; (d) Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan (e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Pentadbir Sistem/ ICTSO

0606 Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
060601 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; (b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; (e) *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Rangkaian ICT; (f) Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan Jabatan; (g) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; (h) Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan menceroboh dan aktiviti-aktiviti lain	Pentadbir Rangkaian ICT dan ICTSO

yang boleh mengancam sistem dan maklumat Jabatan; (i) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; (j) Sebarang penyambungan rangkaian adalah di bawah kawalan Jabatan; (k) Kakitangan Jabatan hanya dibenarkan menggunakan rangkaian Jabatan sahaja dan penggunaan modem atau *mobile broadband* adalah tertakluk kepada peraturan semasa Jabatan; dan (l) Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.	
0607 Pengurusan Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060701 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pemilik terlebih dahulu.	Semua
060702 Prosedur Pengendalian Media	
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut: (a) Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; (b) Menghadkan dan menentukan capaian media kepada pengguna	Semua

yang dibenarkan sahaja; (c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan (e) Menyimpan semua media di tempat yang selamat.	
060703 Pelupusan Media	
Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul dan selamat.	Semua
060704 Keselamatan Sistem Dokumentasi	
Sistem dokumentasi perlu dilindungi daripada capaian yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Semua

0608 Pengurusan Pertukaran Maklumat

Objektif:

Memastikan keselamatan pertukaran maklumat dan perisian antara Jabatan dan entiti luar terjamin.

060801 Pertukaran Maklumat

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

060802 Pengurusan Mel Elektronik

Penggunaan mel elektronik (e-mel) di Jabatan hendaklah dipantau secara berterusan oleh Pentadbir Sistem E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "*Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan*" dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian e-mel adalah seperti berikut: (a) Akaun atau alamat e-mel yang disediakan oleh Jabatan sahaja boleh digunakan. Penggunaan akaun milik orang lain atau	Semua

akaun yang dikongsi bersama adalah dilarang;

(b) Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh Jabatan;

(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) Pengguna dinasihatkan menggunakan fail kepilan, 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 mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

(h) E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

(i) kakitangan Jabatan hendaklah menentukan tarikh dan masa sistem komputer adalah tepat bagi memastikan kesahihan masa penghantaran dan penerimaan;

(j) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera;

(k) kakitangan Jabatan hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak digunakan untuk tujuan rasmi; dan

(l) kakitangan Jabatan hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	
0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)	
Objektif: Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
060901 E-Dagang	
Bagi menggalakkan pertumbuhan e-dagang serta sebagai menyokong hasrat kerajaan mempopularkan penyampaian perkhidmatan melalui elektronik, pengguna boleh menggunakan kemudahan Internet. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan (c) Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Semua
060902 Transaksi *Online*	
Maklumat yang melibatkan transaksi *online* perlu dilindungi bagi mengelakkan	Semua

transmisi yang tidak lengkap, *mis-routing,* pendedahan, pertindihan dan perubahan yang tidak dibenarkan.	
060903 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut: (a) Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; (b) Memastikan sistem yang boleh diakses oleh orang awam diuji terlebih dahulu; dan (c) Memastikan segala maklumat yang hendak dipaparkan telah disah dan diluluskan sebelum dimuat naik ke laman web.	Semua
0610 Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
061001 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi; (b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti,	Pentadbir Sistem ICT

rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan (d) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. (e) Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. (f) Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
061002 Sistem Log	
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO dan CIO; (d) Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu	Pentadbir Sistem ICT

siasatan dan memantau kawalan capaian; (e) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; (f) Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; (g) Aktiviti pentadbiran sistem perlu direkodkan; (h) Log kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan, dianalisis dan diambil tindakan sewajarnya.	
061003 *Clock Syncronization*	
Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam Jabatan atau domain keselamatan perlu diselaraskan dengan *Malaysian Standard Time* (MST) yang ditetapkan oleh sumber yang sah.	Pentadbir Sistem ICT

BIDANG 07
KAWALAN CAPAIAN

0701 Dasar Kawalan Capaian

Objektif:

Mengawal capaian ke atas maklumat.

070101 Keperluan Kawalan Capaian

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

0702 Pengurusan Capaian Pengguna

Objektif:

Mengawal capaian pengguna ke atas aset ICT

070201 Akaun Pengguna

Setiap pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh Jabatan sahaja boleh digunakan; (b) Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; (c) Tahap capaian adalah berdasarkan kepada keperluan skop tugasan yang ditetapkan. 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 yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau	Semua dan Pentadbir Sistem ICT

v. Ditamatkan perkhidmatan.	
070202 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT
070203 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh Jabatan seperti berikut: (a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) kakitangan Jabatan hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; (d) Kata laluan TIDAK BOLEH 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 *login.* (g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas kata laluan diset semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna;	Semua dan Pentadbir Sistem ICT

(i) Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa yang bersesuaian; dan (j) Tidak dibenarkan penggunaan semula tiga (3) kata laluan yang terakhir digunakan.	
070204 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Semua
0703 Kawalan Capaian Rangkaian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	

070301 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian Jabatan, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	Pentadbir Rangkaian ICT dan ICTSO
070302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di Jabatan hendaklah dipantau secara berterusan oleh Pentadbir Rangkaian ICT bagi memastikan penggunaanya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code*, virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian Jabatan; (b) Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (c) Penggunaan teknologi *bandwidth management* untuk mengawal aktiviti seperti *video conferencing, video streaming, chat, downloading* adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; (d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja.	Pentadbir Rangkaian ICT

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 Pengurus ICT;

(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) Kakitangan Jabatan 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 Jabatan;

(j) Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan;

(k) P enggunaan modem / *mobile broadband* untuk tujuan sambungan ke Internet tidak dibenarkan kecuali setelah mendapat kebenaran daripada Pengurus ICT; 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 dan 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.	

0704 Kawalan Capaian Sistem Pengoperasian

Objektif:

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

070401 Capaian Sistem Pengoperasian

Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: (a) Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; dan (b) Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (a) Mengesahkan kakitangan Jabatan yang dibenarkan; (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* dan (c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin;	Pentadbir Sistem ICT dan ICTSO

(b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap kakitangan Jabatan dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Menghadkan dan mengawal penggunaan program; dan (d) Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
070402 Kad Pintar	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; (b) Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; (c) Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan (d) Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Bahagian / Unit Kewangan, Jabatan	Semua
0705 Kawalan Capaian Aplikasi dan Maklumat	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi	

070501 Capaian Aplikasi dan Maklumat	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: (a) kakitangan Jabatan hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); (c) 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.	Pentadbir Sistem ICT dan ICTSO
0706 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif: Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh	
070601 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut:	Semua

(a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan (b) Mewujudkan peraturan dan garis panduan keselamatan yang bersesuaian untuk melindungi daripada risiko penggunaan peralatan mudah alih dan kemudahan komunikasi.	
070602 Kerja Jarak Jauh	
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan; dan (b) Mewujudkan peraturan dan garis panduan untuk memastikan persekitaran kerja jarak jauh adalah sesuai dan selamat.	Semua

BIDANG 08
PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

Objektif:

Memastikan sistem yang dibangunkan secara dalaman *(inhouse)* atau pihak ketiga *(outsource)* mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

080101 Keperluan Keselamatan Sistem Maklumat

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

080102 Pengesahan Data Input dan Output	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Data *input* bagi aplikasi perlu disemak dan disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; (b) Data *output* daripada aplikasi perlu disemak dan disahkan bagi memastikan maklumat yang dihasilkan adalah tepat; dan (c) Tindakan pembetulan dan pengukuhan perlu diambil bagi sebarang ralat input dan output yang tidak sah bagi memastikan pemprosesan yang tepat.	Pemilik Sistem dan Pentadbir Sistem
0802 Kawalan Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 Enkripsi	
Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Semua
080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua

080203 Pengurusan Infrastruktur Kunci Awam (*PKI*)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. Sebarang perubahan kepada pemilik / pemegang kunci hendaklah dilaporkan kepada Pentadbir Sistem.	Semua / Pentadbir Sistem
0803 Keselamatan Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
080301 Kawalan Fail Sistem	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; (c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan (e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem dan Pentadbir Sistem

0804 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif:

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

080401 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 perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi; (c) Pegawai yang telah dipertanggungjawabkan dan ditetapkan perlu memantau penambahbaikan, pembetulan atau perubahan yang dilakukan oleh pihak ketiga; (d) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (e) Akses kepada kod sumber (*source code)* aplikasi perlu dihadkan kepada pengguna yang dibenarkan; dan (f) Menghalang sebarang peluang untuk membocor dan memanipulasi maklumat.	Pemilik Sistem dan Pentadbir Sistem

080402 Pembangunan Perisian Secara *Outsource*

(a) Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pemilik sistem/pentadbir sistem; (b) Kod sumber (*source code)* bagi semua aplikasi dan perisian	Pemilik Sistem dan Pentadbir Sistem

adalah menjadi hak milik Kerajaan; (c) Kod sumber *(source code)* yang diserahkan kepada Kerajaan mesti bebas daripada sebarang ralat; dan (d) Maklumat, prosidur, dokumen yang digunakan semasa pembangunan secara *outsource* adalah menjadi rahsia Kerajaan yang tidak boleh disebar dan didedahkan.	
0805 Kawalan Teknikal Keterdedahan (*Vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080501 Kawalan dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem

BIDANG 09
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.

090101 Mekanisme Pelaporan

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

Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di Jabatan sepertimana **Lampiran 2**. Prosedur pelaporan insiden keselamatan ICT berdasarkan: 1. Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan 2. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
0902 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada Jabatan. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: 1. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; 2. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan;	ICTSO

3. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; 4. Menyediakan tindakan pemulihan segera; dan 5. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	

BIDANG 10
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan

Objektif:

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

100101 Pelan Kesinambungan Perkhidmatan

CIO dan ICTSO Jabatan

Pelan Kesinambungan Perkhidmatan (*Business Continuity Management - BCM*) hendaklah dibangunkan untuk menentukan pendekatan menyeluruh yang diambil bagi mengekalkan kesinambungan perkhidmatan.

Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT KPWKM. Perkara-perkara berikut perlu diberi perhatian:

(a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan;

(b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap perkhidmatan Jabatan serta kemungkinan dan impak gangguan tersebut terhadap keselamatan ICT;

(c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan;

(d) Mendokumentasikan proses dan prosedur yang telah dipersetujui;

(e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan;

(f) Membuat *backup*; dan

(g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali.

Pelan BCM perlu dibangunkan, didokumentasikan dan hendaklah mengandungi perkara-perkara berikut:

(a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

(b) Senarai personel utama Jabatan, pembekal perkhidmatan dan pihak ketiga berserta nombor yang boleh dihubungi (faksimili, telefon, sistem pesanan ringkas, dan e-mel). Senarai personel kedua juga hendaklah disediakan sebagai menggantikan personel utama yang tidak dapat hadir untuk menangani insiden;

(c) Senarai lengkap maklumat yang memerlukan backup dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;

(d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan

(e) Perjanjian dengan pembekal perkhidmatan dan pihak ketiga untuk mendapatkan keutamaan penyambungan semula perkhidmatan di mana boleh.

Salinan dokumentasi pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan BCM hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan.

Ujian pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

Jabatan hendaklah memastikan salinan dokumentasi pelan BCM sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	

BIDANG 11
PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT.

110101 Pematuhan Dasar

Setiap pengguna di Jabatan hendaklah membaca, memahami dan mematuhi Dasar Keselamatan ICT dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. Semua aset ICT Kerajaan di Jabatan dan pembekal perkhidmatan termasuk maklumat dan sistem yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Pengarah/pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT Kerajaan di Jabatan dan pembekal perkhidmatan selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber Jabatan.	Semua

110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

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

110103 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan .	Semua
110104 Keperluan Perundangan	
Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua pengguna di Jabatan adalah seperti di Lampiran 3.	Semua
110105 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT boleh dikenakan tindakan tatatertib tertakluk mengikut perundangan dan peraturan.	Semua

GLOSARI	
Ancaman	Bermaksud kemungkina yang boleh menyebabkan bahaya, kerosakan dan kerugian
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Bermaksud semua yang mempunyai nilai kepada jabatan merangkumi perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Clear Desk	Tidak meninggalkan sebarang dokumen yang sensitif di atas meja.
Clear Screen	Tidak memaparkan sebarang maklumat sensitif apabila komputer berkenaan ditinggalkan.
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. Teks biasa (*plaintext)* akan ditukar kepada kod yang tidak difahami dan kod yang tidak difahami ini akan menjadi versi teks *cipher*. Bagi mendapatkan semula teks biasa tersebut, proses penyahsulitan digunakan.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam

GLOSARI	
	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*).
CERT	*Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Jabatan. 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	Sistem Pengesan Pencerobohan

GLOSARI	
System (IDS)	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.
Kriptografi	Satu sains penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak yang tertentu sahaja.
Insiden Keselamatan	Musibah (*adverse event*) yang berlaku ke atas sistem maklumat.
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
Mobile Code	Kod perisian yang dipindahkan dari satu komputer kepada komputer lain dan melaksanakan secara automatik fungsi – fungsi tertentu dengan sedikit atau tanpa interaksi dari pengguna.
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan

GLOSARI	
	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.
Penilaian Risiko	Penilaian ke atas kemungkina berlakunya bahaya atau kerosakan atau kehilangan aset.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Risiko	Kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian.
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

GLOSARI	
	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.
Vulnerability (Kerentanan)	Sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

Lampiran 1

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT KPWKM DAN AGENSI

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Bahagian/Jabatan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :-

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT; dan

2. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tanda tangan : .....

Tarikh : .....

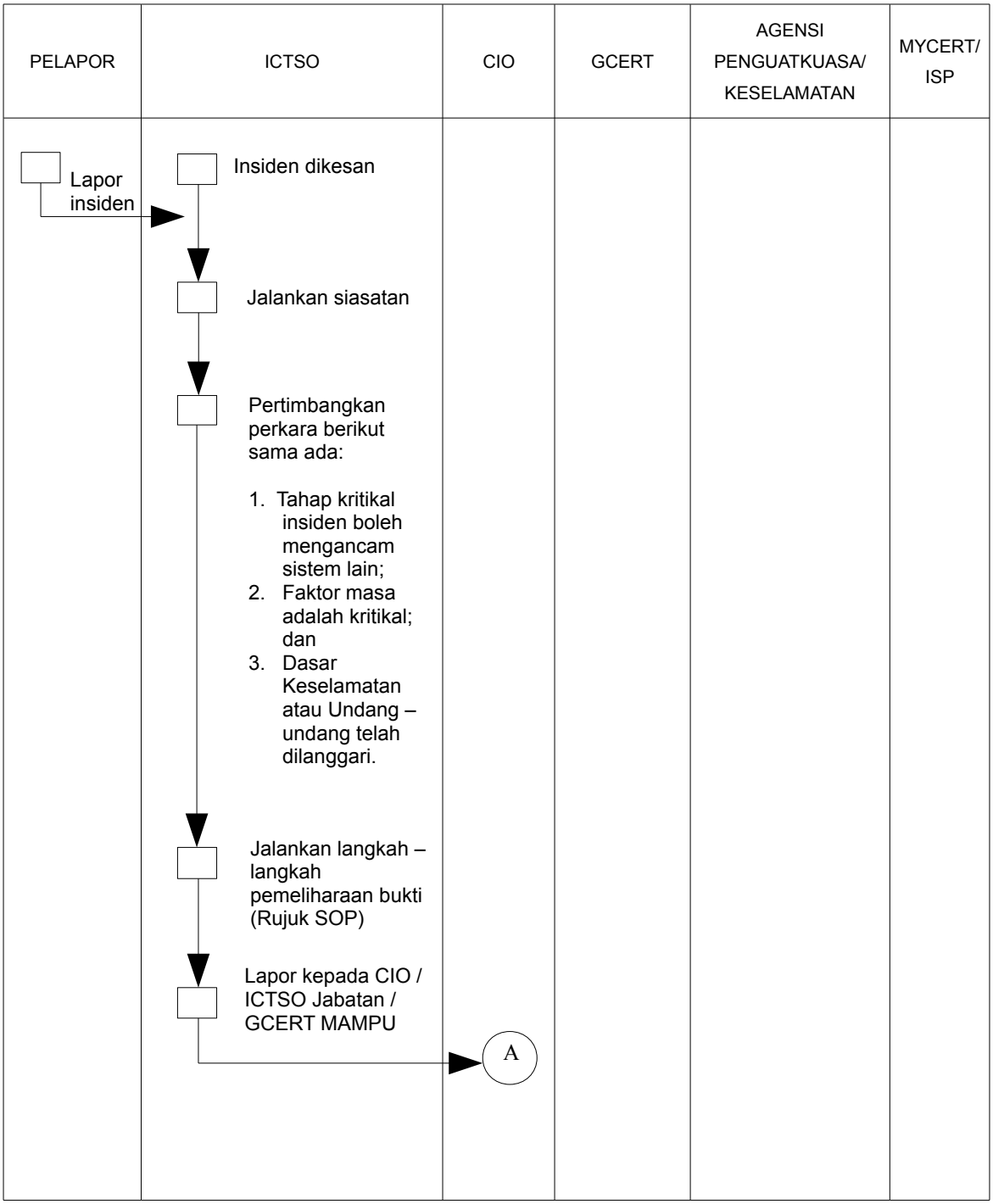
Pengesahan Pegawai Keselamatan ICT

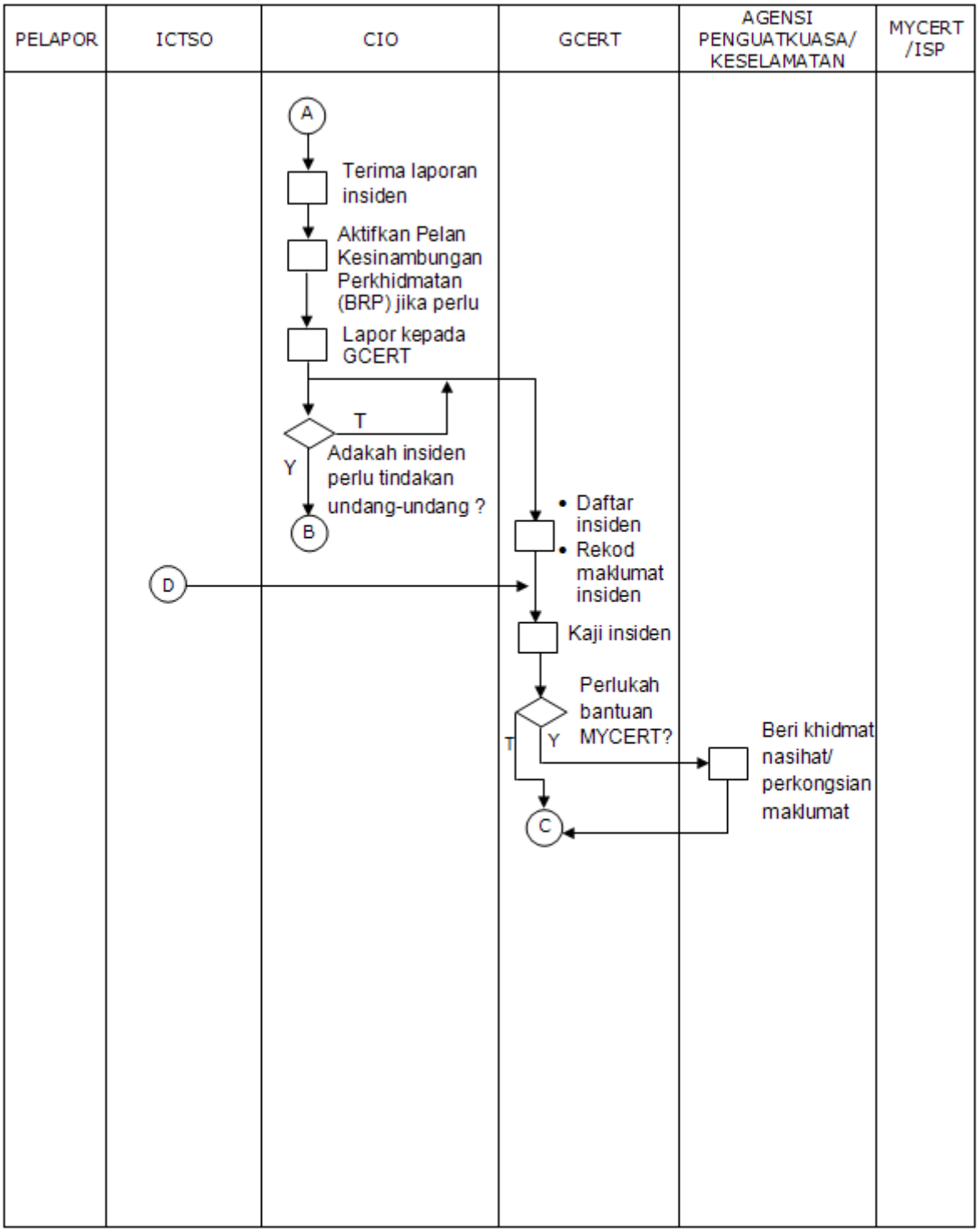
.....
(Nama Pegawai Keselamatan ICT)
b.p. Ketua Setiausaha KPWKM

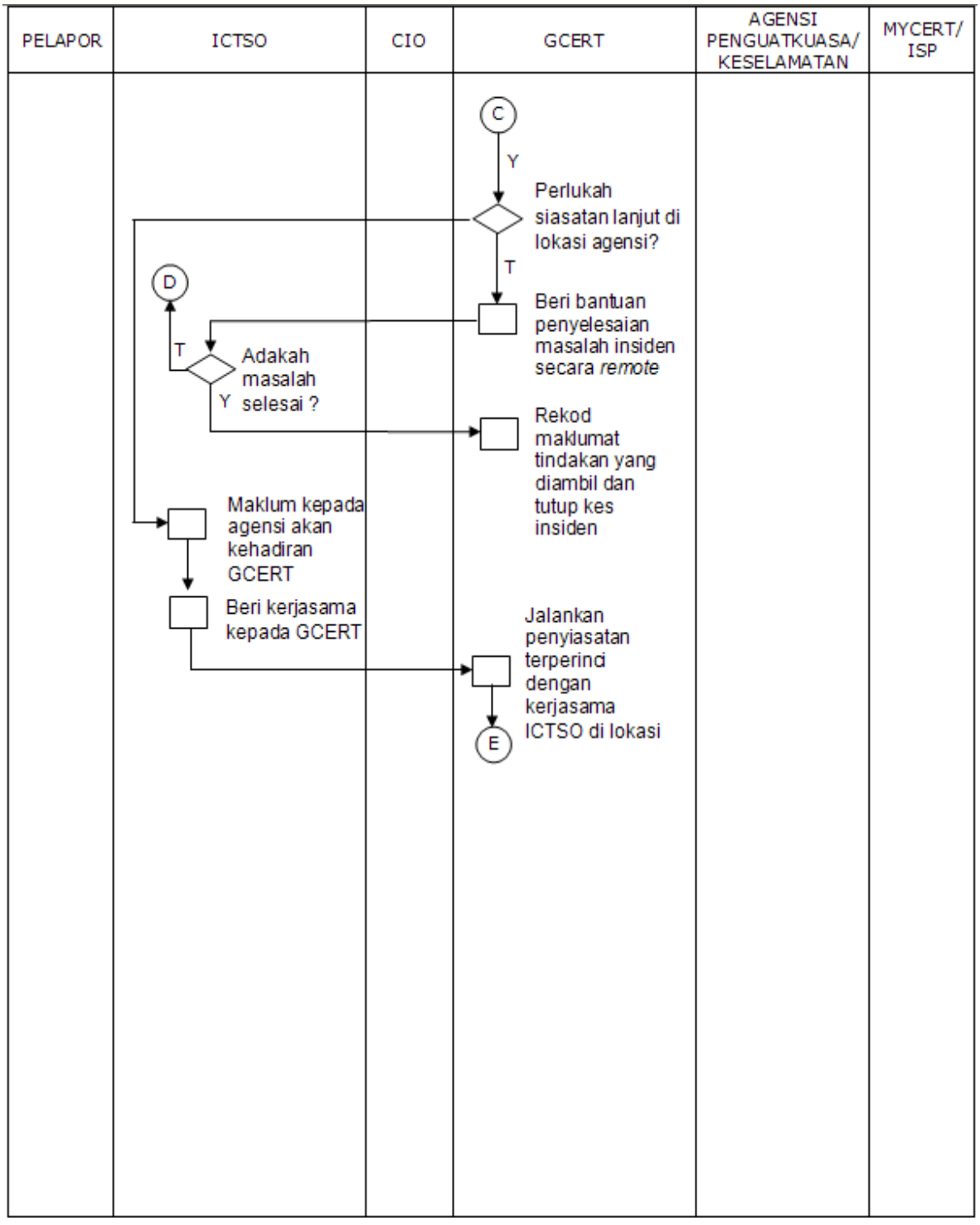
Tarikh: .....

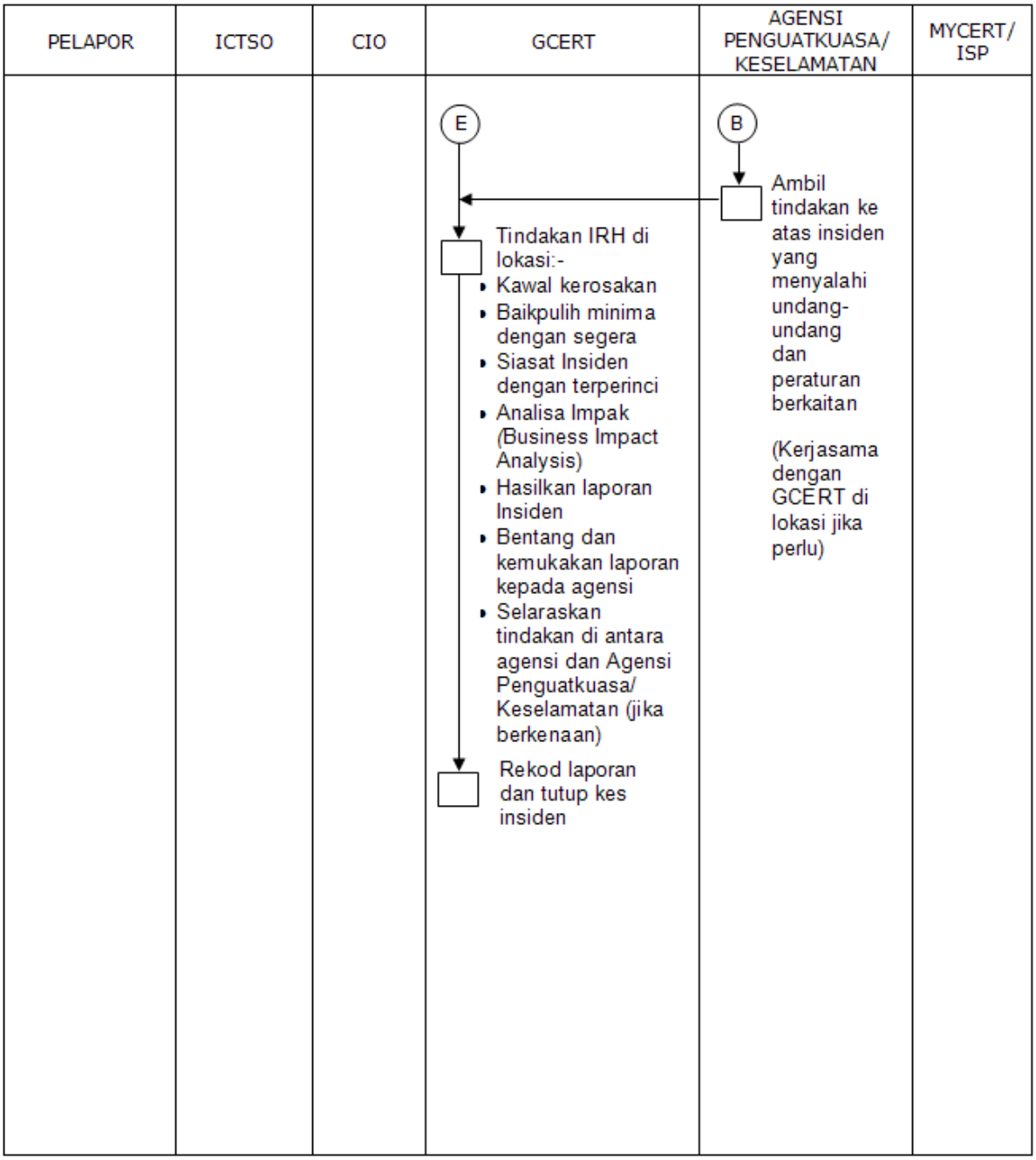
Lampiran 2

Rajah1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT Jabatan




PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT /ISP
A
Terima laporan insiden
Aktifkan Pelan Kesinambungan Perkhidmatan (BRP) jika perlu
Lapor kepada GCERT
T
Y
Adakah insiden perlu tindakan undang-undang ?
B
D
• Daftar insiden
• Rekod maklumat insiden
Kaji insiden
Perlukah bantuan MYCERT?
T
Y
Beri khidmat nasihat/ perkongsian maklumat
C


PELAPOR
ICTSO
CIO
GCERT
AGENSI PENGUATKUASA/ KESELAMATAN
MYCERT/ ISP
C
Y
Perlukah siasatan lanjut di lokasi agensi?
T
Beri bantuan penyelesaian masalah insiden secara *remote*
D
T
Adakah masalah
Y selesai ?
Rekod maklumat tindakan yang diambil dan tutup kes insiden
Maklum kepada agensi akan kehadiran GCERT
Beri kerjasama kepada GCERT
Jalankan penyiasatan terperinci dengan kerjasama ICTSO di lokasi
E



Penunjuk :

SOP - *Standard Operating Procedure*

Lampiran 3

SENARAI PERUNDANGAN DAN PERATURAN

(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 MAMPU;

(x) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;

(y) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.