DASAR KESELAMATAN ICT

KEMENTERIAN SUMBER MANUSIA

Versi 4.0

A. INFORMASI DOKUMEN

VERSI	KELULUSAN	TARIKH KUATKUASA
Versi 1.0	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KSM	30 Mac 2007
Versi 2.0	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KSM Bil. 4 Tahun 2010	30 Disember 2010
Versi 3.0	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KSM Bil. 2 Tahun 2012	18 Mei 2012
Versi 3.1	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KSM Bil. 2 Tahun 2013	23 Mei 2013
Versi 3.2	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KSM Bil. 3 Tahun 2014	25 Ogos 2014
Versi 4.0	Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KSM Bil. 2 Tahun 2015	22 Mei 2015

B. REKOD PINDAAN

Tarikh	VERSI	PINDAAN
15 April 2015	Versi 4.0	Pindaan keseluruhan Bidang Keselamatan dengan merujuk kepada Standard ISO/IEC 27001:2013 Information Security Management System (ISMS).

KANDUNGAN

1.0 PENGENALAN

Dasar Keselamatan ICT (DKICT) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) Kementerian Sumber Manusia (KSM). Dasar ini juga menerangkan kepada semua pengguna di KSM mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KSM.

2.0 OBJEKTIF

Objektif utama Dasar Keselamatan ICT di KSM adalah seperti berikut:

a. Memastikan kelancaran operasi KSM dengan mencegah serta meminimumkan kerosakan atau kemusnahan aset ICT KSM;
b. Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integri kebolehsediaan, kesahihan maklumat dan komunikasi;
c. Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan;
d. Meningkatkan tahap kesedaran keselamatan ICT kepada pengguna, pakar runding dan pembekal;
e. Memperkemaskan pengurusan risiko;
f. Mencegah penyalahgunaan atau kecurian aset ICT KSM; dan
g. Melindungi aset ICT daripada penyelewengan oleh pengguna, pakar runding dan pembekal

3.0 PERNYATAAN DASAR KESELAMATAN ICT KSM

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. 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 bagi segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan. Terdapat empat (4) komponen asas keselamatan ICT iaitu:

a. Melindungi maklumat rahsia rasmi dan maklumat rasmi di KSM 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 hanya kepada pengguna yang sah atau penerimaan maklumat dari sumber-sumber yang sah.

DKICT KSM merangkumi perlindungan ke atas semua bentuk maklumat elektronik bertujuan untuk menjamin keselamatan 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 akses tanpa kebenaran;
b. Integriti – data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;
c. Tidak boleh disangkal – punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh di sangkal;

d. Kesahihan – data dan maklumat hendaklah dijamin kesahihannya; dan
e. Kebolehsediaan – data dan maklumat hendaklah boleh diakses pada bila-bila masa.

Selain itu, langkah-langkah ke arah keselamatan ICT hendaklah bersandarkan kepada penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semulajadi aset ICT, risiko yang mungkin timbul dan langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

4.0 SKOP

Sistem ICT KSM terdiri daripada organisasi, manusia, perisian, perkakasan, telekomunikasi, kemudahan ICT dan data. KSM telah menetapkan keperluan-keperluan asas keselamatan seperti berikut:

a. Data dan Maklumat hendaklah boleh diakses secara berterusan dengan cepat, tepat, mudah dan dengan cara yang boleh dipercayai. Ini adalah amat perlu bagi membolehkan keputusan dan penyampaian perkhidmatan dilakukan dengan berkesan dan berkualiti.
b. Semua data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan kesempurnaan dan melindungi kepentingan KSM.

Bagi menentukan sistem ICT ini terjamin keselamatannya sepanjang masa, DKICT KSM ini merangkumi perlindungan ke atas semua bentuk maklumat ICT Kerajaan yang dimasuki, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar dan dibuat salinan. Ini akan dilakukan melalui penubuhan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

a. Data dan maklumat – semua data dan maklumat yang disimpan atau digunakan di pelbagai media atau peralatan ICT;

b. Peralatan ICT – semua peralatan komputer dan periferal seperti komputer peribadi, stesen kerja, kerangka utama dan alat-alat prasarana seperti *Uninterrupted Power Supply* (UPS), punca kuasa dan pendingin hawa;

c. Media Storan – semua media storan dan peralatan yang berkaitan seperti disket, *thumbdrive,* CD ROM, pita, cakera, pemacu cakera, kad memori dan *external hard disk*;

d. Komunikasi dan peralatan rangkaian – semua peralatan berkaitan komunikasi seperti pelayan rangkaian, *gateway*, *bridge*, *router* dan peralatan PABX;

e. Perisian – semua perisian yang digunakan untuk mengendali, memproses, menyimpan, menjana dan mengirim maklumat. Ini meliputi semua perisian sistem, perisian utiliti, perisian rangkaian, program aplikasi, pangkalan data, fail program dan fail data;

f. Dokumentasi – semua dokumentasi yang mengandungi maklumat berkaitan dengan penggunaan dan pemasangan peralatan dan perisian. Ia juga meliputi data dalam semua bentuk media seperti salinan kekal, salinan elektronik, *transparencies*, risalah dan slaid-slaid;

g. Manusia – semua pengguna yang dibenarkan termasuk pentadbir dan pengurus serta mereka yang bertanggungjawab terhadap keselamatan ICT; dan

h. Premis komputer dan komunikasi – semua kemudahan serta premis yang digunakan untuk menempatkan perkara (i) hingga (vii) di atas.

Dasar ini terpakai kepada semua Pengguna ICT di KSM yang mencapai, mengurus, menyelenggara, memproses, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT KSM.

5.0 PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT KSM 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, mengemaskini, 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 KSM hendaklah 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

vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

d. Pengasingan

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

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

g. Pemulihan

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

h. Saling Bergantungan

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

6.0 PENILAIAN RISIKO KESELAMATAN ICT

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

KSM 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 bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat KSM 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.

KSM 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. KSM 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**	
0101 Pengurusan Keselamatan Maklumat ICT	
Objektif: Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan KSM dan perundangan yang berkaitan.	
010101 Dasar Keselamatan Maklumat	
Satu set dasar untuk keselamatan maklumat perlu ditakrifkan, diluluskan, diterbitkan dan dikomunikasikan oleh pihak pengurusan KSM kepada pegawai/staf dan pihak-pihak luar yang relevan. (A.5.1.1 Policies for Information Security) Ketua Setiausaha KSM adalah bertanggungjawab terhadap pelaksanaan dasar ini dengan dibantu oleh Jawatankuasa Pemandu ICT (JPICT) KSM yang terdiri daripada Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO), Setiausaha Bahagian Pengurusani Maklumat, Timbalan Setiausaha Bahagian (Kewangan) semua Ketua Jabatan, dan pegawai-pegawai yang diturunkan kuasa. Dasar Keselamatan Maklumat perlu menangani keperluan: a. Strategik KSM b. Peraturan, undang-undang dan kontrak c. Ancaman persekitaran keselamatan maklumat semasa dan unjuran Polisi keselamatan maklumat hendaklah mengandungi kenyataan yang membabitkan: a. Definisi keselamatan maklumat, objektif dan prinsip kepada semua aktiviti yang berhubung dengan keselamatan maklumat b. Tanggungjawab am dan khusus bagi pengurusan keselamatan maklumat c. Proses ketidakpatuhan pengendalian dan pengecualian keselamatan maklumat.	Ketua Setiausaha (KSU) / Pegawai yang diturunkan kuasa
010102 Kajian Semula Dasar Keselamatan Maklumat	
Dasar Keselamatan Maklumat KSM perlu dikaji semula pada jangka masa yang dirancang atau apabila perubahan ketara untuk memastikan kesesuaian kesinambungan, kecukupan dan keberkesanan dasar. (A.5.1.2 *Review of policies for information security*) Setiap dasar keselamatan maklumat harus mempunyai pemilik yang telah diluluskan tanggungjawab pengurusan untuk pembangunan, penilaian dan kajian.	(Kekerapan : 1/ tahun)

Kajian semula dasar keselamatan KSM perlu menilai peluang untuk penambahbaikan dasar sebagai tindak balas kepada perubahan persekitaran organisasi, keadaan perniagaan dan keadaan undang-undang.	

BIDANG 02 **KESELAMATAN ORGANISASI**	
0201 Struktur Organisasi Keselamatan	
Objektif: Menerangkan peranan dan tanggungjawab pengguna yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif organisasi.	
020101 Ketua Jabatan	
Peranan dan tanggungjawab Ketua Setiausaha adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT ; b. Merangka, mengkaji semula pelaksanaan dan keberkesanan Dasar Keselamatan ICT mengikut keperluan; c. Memberi arahan dan hala tuju yang jelas serta sokongan pengurusan yang mantap; d. Mewujudkan dan mengetuai Jawatankuasa Pemandu Keselamatan ICT KSM; e. Meluluskan pelantikan mana-mana pegawai yang diberi peranan dan tanggungjawab terhadap keselamatan maklumat ICT dalam organisasi; f. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT KSM; g. Memastikan semua pengguna mematuhi Dasar Keselamatan ICT KSM; h. Memastikan semua keperluan keselamatan ICT jabatan (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; i. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT KSM; dan j. Menandatangani “Surat Akuan Pematuhan” bagi mematuhi Dasar Keselamatan ICT. Sila rujuk **Lampiran 1**.	Ketua Setiausaha
020102 Ketua Pegawai Maklumat (CIO)	
Peranan dan tanggungjawab CIO yang dilantik adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT; b. Bertanggungjawab kepada Ketua Setiausahadalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; c. Memastikan kawalan keselamatan maklumat dalam organisasi diseragam dan diselaraskan dengan sebaiknya;	CIO

d. Menentukan keperluan keselamatan ICT; e. Memastikan dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; f. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT KSM; g. Memastikan dan melaksanakan program-program kesedaran mengenai keselamatan ICT; h. Menyelia dan memantau perlaksanaan Dasar Keselamatan ICT di peringkat negeri; i. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT KSM; dan j. Menandatangani "Surat Akuan Pematuhan" bagi mematuhi Dasar Keselamatan ICT. Sila rujuk **Lampiran 1**.	
020103 Pengurus ICT	
Setiausaha Bahagian Pengurusan Maklumat merupakan Pengurus ICT KSM. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KSM; b. Memastikan kajian semula dan pelaksanaan kawalan keselamatan ICT selaras dengan keperluan KSM; c. Menentukan kawalan akses semua pengguna terhadap aset ICT KSM; d. Memaklumkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO untuk tindakan; e. Memastikan penyimpanan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KSM dilaksanakan; f. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai Pentadbir Sistem ICT yang tamat perkhidmatan, bertukar, bercuti panjang atau berlaku perubahan dalam bidang tugas; g. Menyebarkan amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta melaksanakan langkah perlindungan yang bersesuaian; h. Memaklumkan insiden keselamatan ICT kepada ICTSO; i. Mengenalpasti punca ancaman atau insiden keselamatan ICT dan melaksanakan langkah-langkah membaik pulih dengan segera;	Pengurus ICT

j. Melaporkan sebarang salahlaku pengguna yang melanggar dasar keselamatan ICT KSM kepada ICTSO; dan k. Menyelaraskan program-program kesedaran mengenai keselamatan ICT.	
020104 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT Kerajaan; b. Menguatkuasakan Dasar Keselamatan ICT KSM; c. Mengurus keseluruhan program-program keselamatan ICT KSM; d. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT KSM kepada semua pengguna; e. Menjalankan penilaian risiko; f. Menyelaraskan program 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 Pasukan Tindakbalas Insiden Keselamatan ICT (GCERT-MAMPU) dan memaklumkannya kepada Ketua Jabatan, CIO dan Pengurus ICT; dan i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera.	
020105 Pentadbir Sistem ICT	
Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KSM; b. Menjaga kerahsiaan kata laluan; c. Menjaga kerahsiaan konfigurasi aset ICT; d. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT KSM;	Pentadbir Sistem ICT: a.Pentadbir Pusat Data; b.Pentadbir Email; c.Pentadbir Rangkaian;

e. Memantau aktiviti capaian harian pengguna; f. Mengenalpasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; g. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; dan h. Menyimpan dan menganalisis rekod jejak audit (audit trail).	Pentadbir Sistem dan Aplikasi
020106 Pengguna KSM	
Peranan dan tanggungjawab pengguna adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KSM; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Menjaga kerahsiaan maklumat Kerajaan yang meliputi maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; d. Menjaga kerahsiaan kata laluan; e. Memastikan maklumat berkaitan adalah tepat dan lengkap dari semasa ke semasa; f. Mengambil bahagian dalam program-program kesedaran mengenai keselamatan ICT (sama ada secara langsung atau tidak langsung); dan g. Menandatangani "Surat Akuan Pematuhan" bagi mematuhi Dasar Keselamatan ICT. Sila rujuk **Lampiran 1**.	Pengguna
020107 Pengguna Luar	
Terdiri daripada pembekal, pakar runding dan pihak-pihak yang berkepentingan. Peranan dan tanggungjawab pengguna luar adalah seperti berikut: a. Membaca, memahami dan mematuhi DKICT KSM; b. Menjaga kerahsiaan kata laluan yang diberikan; c. Menggunakan kemudahan ICT dengan berpandukan garis panduan yang telah ditetapkan; dan d. Menandatangani Surat Akuan Pematuhan DKICT KSM (Lampiran 2), NDA form.	Penguna Luar

020108 Jawatankuasa Pemandu ICT (JPICT) KSM	
Bertanggungjawab memperakui: a. Meluluskan perlaksanaan ISMS; b. Meluluskan perolehan; c. Mengambil maklum status ISMS; d. Mengesahkan status kemajuan ISMS; e. Melantik Jawatankuasa Pengurusan dan Pasukan Pelaksana ISMS; dan f. Meluluskan dan mengesahkan DKICT.	JPICT
020109 Jawatankuasa Pengurusan ISMS KSM	

Bagi memantapkan pengurusan projek Persijilan ISO/IEC 27001: 2013, Jawatankuasa Pemandu ISMS KSM telah dibentuk untuk memantau keseluruhan projek. Jawatankuasa ini bertindak dalam melakukan aktiviti berikut: a. Meluluskan skop dan objektif ISMS; b. Menetap kriteria penerimaan risiko, tahap risiko dan pelan rawatan risiko c. Meluluskan Peniliaian Risiko, RTP, SOA; d. Mengesahkan perancangan serta arah tuju dan strategi pelaksanaan; e. Mengesahkan aktiviti dan jadual pelaksanaan secara terperinci; f. Mengesahkan isu dan masalah pelaksanaan dan cadangan penyelesaian; g. Memantau kemajuan pelaksanaan berdasarkan jadual pelaksanaan yang telah ditetapkan; h. Menyemak deliverables pelaksanaan. i. Memantau dan menyemak semula ISMS. j. Mengesahkan pelan latihan, kompetensi dan kesedaran ISMS.	Jawatankuasa Pengurusan ISMS

020110 Jawatankuasa Pelaksana ISMS KSM	
Projek Persijilan ISO ISO/IEC 27001:2013 dilaksanakan oleh sebuah pasukan projek yang terdiri dari pegawai-pegawai Bahagian Pengurusan Maklumat (BPM). Struktur Organisasi projek ini telah dipersetujui oleh Setiausaha BPM. Pasukan projek ini telah dibahagikan kepada 5 pasukan kecil bagi memudahkan perjalanan projek. a. Menghadiri kursus kesedaran standard ISO/IEC 27001:2013; b. Menyediakan dan mengemukakan dasar ISMS, *Statement of Applicability* (SoA), penilaian risiko, *risk treatment plan* dan prosedur-prosedur; c. Melaksana prosedur dan kawalan dalam ISO/IEC 27001:2013; d. Melaksanakan *risk treatment plan;* e. Menyedia kaedah pengukuran keberkesanan kawalan ISMS; f. Mengukur keberkesanan kawalan ISMS; g. Memantau dan menyemak semula ISMS; h. Menjalankan kerja-kerja pentadbiran ISMS seperti dokumentasi, minit mesyuarat dan logistik; i. Merancang dan menyelaras pensijilan ISMS; dan j. Merancang pelan latihan, kompetensi dan kesedaran ISMS.	Jawatankuasa Pelaksana ISMS
020111 Computer Emergency Response Team KSM (CERT KSM)	
Keanggotaan CERT adalah seperti berikut: Pengerusi : CIO Ahli : ICTSO : (1) Pegawai Teknologi Maklumat (2) Penolong Pegawai Teknologi Maklumat Peranan dan tanggungjawab CERT adalah seperti berikut: a. Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden;	CERT KSM

b. Merekod dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baikpulih minima; d. Menghubungi dan melapor insiden yang berlaku kepada GCERT MAMPU samada sebagai input atau untuk tindakan seterusnya; e. Menjalankan penilaian untuk mempastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
020112 Audit Dalaman/Pihak Ketiga KSM	
a. Menyediakan jadual audit tahunan, jadual pelaksanaan audit dan senarai semak audit; b. Melaksana Audit Dalam berdasarkan kawalan yang diperlukan dalam ISO/IEC 27001:2013; c. Menyediakan Laporan Audit Dalam ISMS; d. Membentang penemuan Audit Dalam ISMS ke Jawatankuasa Pengurusan ISMS; e. Menjalankan audit susulan bagi mengesahkan tindakan pembetulan yang dilaksanakan; dan f. Mengemukakan Laporan Audit Susulan kepada Jawatankuasa Pemandu ISMS.	Pasukan Audit ISMS

BIDANG 03 **KESELAMATAN SUMBER MANUSIA**	
0301 Sebelum Perkhidmatan	
Objektif: Memastikan semua pengguna termasuk pengguna KSM dan pengguna luar memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
030101 Penapisan (*Screening*)	
Perkara yang mesti dipatuhi termasuk yang berikut: Menjalankan tapisan keselamatan untuk pengguna KSM serta pengguna luar yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan. (A.7.1.1 *Screening*).	ICTSO, HR, Pengurus ICT, Pengguna KSM & Pengguna Luar
030102 Terma & Syarat Pekerjaan	
Perkara yang mesti dipatuhi termasuk yang berikut: a. Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pegawai dan kakitangan KSM serta pengguna luar yang terlibat dalam menjamin keselamatan informasi maklumat. (A.7.1.2 *Terms & Conditions of employment*). b. Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	ICTSO, HR, Pengurus ICT, Pengguna KSM & Pengguna Luar
0302 Dalam Perkhidmatan	
030201 Tanggungjawab Pengurusan	
Perkara yang perlu dipatuhi termasuk yang berikut: a. Pengurusan ICT KSM hendaklah memastikan semua pegawai dan kakitangan KSM serta pengguna luar mematuhi dasar keselamatan maklumat KSM. (A.7.2.1 *Management responsibilities*)	ICTSO, HR, Pengurus ICT, Pengguna KSM & Pengguna Luar

b. Memastikan pegawai dan kakitangan KSM serta pengguna luar mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh KSM;	
030202 Latihan kesedaran dan Pendidikan Keselamatan Maklumat	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Melaksanakan latihan kesedaran dan pendidikan berkaitan dengan pengurusan keselamatan ICT kepada pengguna KSM dan pengguna luar (sekiranya perlu) secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. b. KSM perlu menyediakan latihan kesedaran dan pendidikan keselamatan ICT sekurang-kurangnya sekali setahun. (A.7.2.2 *Information security awareness, education and training*) c. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul bagi menjamin kepentingan keselamatan ICT. Sebarang kursus dan latihan teknikal yang diperlukan, pengguna boleh merujuk kepada Bahagian Khidmat Pengurusan dan Sumber Manusia, KSM.	ICTSO, HR, Pengurus ICT, Pengguna KSM & Pengguna Luar
030203 Proses Tatatertib	
Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan KSM serta pengguna luar sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan (A.7.2.3 *Disciplinary process*)	ICTSO, HR, Pengurus ICT, Pengguna KSM & Pengguna Luar
0303 Penamatan atau Perubahan Perkhidmatan	
030301 Penamatan atau Perubahan Tanggungjawab Pekerjaan	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Tanggungjawab keselamatan ICT dan tugasannya harus ditentukan dan dimaklumkan kepada pekerja atau kontraktor selepas penamatan atau perubahan perkerjaan. (A.7.3.1 *Termination or change of employment responsibilities*)	ICTSO, HR, Pengurus ICT, Pengguna KSM & Pengguna Luar

b. Menguruskan urusan keluar, berhenti, pertukaran peranan dan tanggungjawab pengguna KSM serta pengguna luar; c. Tanggungjawab untuk melaksanakan penamatan atau perubahan pekerjaan hendaklah ditakrifkan dengan jelas termasuk; i. Perjanjian Kerahsiaan (NDA) ii. Perubahan dalam terma & syarat penamatan / tanggungjawab iii. Tentukan tempoh akhir pekerjaan iv. Tanggungjawab masih sah selepas penamatan d. Memastikan semua aset ICT dikembalikan kepada KSM mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan e. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh KSM dan/atau terma perkhidmatan.	

BIDANG 04 PENGURUSAN ASET	
0401 Akauntabiliti/Tanggungjawab Aset	
Objektif: Untuk mengenal pasti aset bagi memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KSM	
040101 Inventori Aset	
Ketua Jabatan bertanggungjawab memastikan semua aset ICT KSM diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Tanggungjawab yang perlu dipatuhi adalah termasuk perkara-perkara berikut: (A.8.1.1 *Inventory of assets*) a. Aset yang berkaitan dengan maklumat dan kemudahan pemprosesan maklumat hendaklah dikenal pasti dan maklumat aset direkodkan dalam borang harta modal atau inventori dan sentiasa dikemaskinikan; b. Semua aset ICT KSM hendaklah direkod dan dilabelkan merujuk kepada pekeliling pengurusan asset yang berkuatkuasa; dan c. Semakan inventori ke atas aset ICT dan kemudahan pemprosesan maklumat perlu dilakukan sekurang-kurangnya sekali setahun.	Pengguna KSM & Pengguna Luar, Pegawai Aset dan Pengarah Negeri Pusat Kos
040102 Hakmilik Aset	
KSM perlu memastikan semua aset mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; (A.8.1.2 *Ownership of assets*)	Pengguna KSM & Pengguna Luar, Pegawai Aset dan Pengarah Negeri Pusat Kos
040103 Penerimaan Penggunaan Aset	
KSM perlu memastikan peraturan bagi pengunaan aset dan kemudahan pemprosesan maklumat dikenal pasti, didokumenkan dan dilaksanakan (A.8.1.3 *Acceptable use of assets*). Setiap pengguna bertanggungjawab terhadap semua aset ICT di bawah tanggungjawabnya.	Pengguna KSM & Pengguna Luar, Pegawai Aset dan Pengarah Negeri Pusat Kos
040104 Pemulangan Aset	
Semua pengguna KSM dan pengguna luar hendaklah memulangkan semua aset kepada KSM selepas penamatan pekerjaan, kontrak atau perjanjian. (A.8.1.4 *Return of assets*)	Pengguna KSM & Pengguna Luar,

	Pegawai Aset dan Pengarah Negeri Pusat Kos
0402 Klasifikasi Maklumat	
Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
040201 Pengelasan Maklumat	
Mengelaskan aset mengikut tahap sensitiviti aset berkenaan; (A.8.2.1 *Classification of information*) Maklumat terperingkat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan yang telah ditetapkan di dalam Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	Ketua Pendaftar, CIO dan Pegawai ICT
040202 Pelabelan Maklumat	
Prosedur pelabelan maklumat hendaklah dibangunkan dan dilaksanakan mengikut skim klasifikasi maklumat yang diguna pakai oleh KSM. (A.8.2.2 *Labelling of information*).	Ketua Pendaftar, CIO dan Pegawai ICT
040203 Pengendalian Aset	
Prosedur bagi mengendalikan aset hendaklah dibangunkan dan dilaksanakan mengikut skim klasifikasi maklumat yang diguna pakai oleh KSM. (A.8.2.3 *Handling of assets*). Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;	Ketua Pendaftar, CIO dan Pegawai ICT

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.	
0403 Pengendalian Media	
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
040301 Pengurusan Media Mudah Alih (*Removal* Media)	
Prosedur pengurusan media mudah alih hendaklah dilaksanakan mengikut skim pengelasan yang diguna pakai oleh KSM. (A.8.3.1 *Management of removal 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 yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan e. Menyimpan semua media di tempat yang selamat	CIO, Pegawai ICT dan Pengguna
040302 Pelupusan Media	
Pelupusan media perlu mendapat kelulusan dari pihak pengurusan ICT dan mengikut prosedur KSM yang mana berkenaan. (A.8.3.2 *Disposal of media*) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut prosedur yang betul serta selamat dan dengan kebenaran KSM.	CIO, Pegawai ICT dan Pengguna
040303 Pemindahan Media Fizikal	
KSM hendaklah memastikan media yang mengandungi maklumat dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pengangkutan. (A.8.3.3 *Physical media transfer*)	CIO, Pegawai ICT dan Pengguna

BIDANG 05 **KAWALAN CAPAIAN**	
0501 Keperluan Kawalan Capaian	
Objektif: Menghadkan akses kepada kemudahan pemprosesan data dan maklumat dengan memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas maklumat.	
050101 Dasar Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. (A.9.1.1 *Access control policy*) Peraturan kawalan capaian hendaklah diwujudkan, didokumenkan dan disemak berdasarkan keperluan perkhidmatan dan keselamatan maklumat. Ia perlu dikemas kini setahun sekali atau mengikut keperluan dan menyokong peraturan kawalan capaian pengguna sedia ada. Perkara yang perlu dipatuhi adalah seperti berikut: a. Keperluan keselamatan aplikasi KSM b. Kebenaran untuk menyebarkan maklumat c. Hak akses dan dasar klasifikasi maklumat sistem dan rangkaian d. Undang-undang Malaysia/Persekutuan yang berkaitan dan obligasi kontrak mengenai had akses kepada data atau perkhidmatan e. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; f. Pengasingan peranan kawalan capaian g. Kebenaran rasmi permintaan akses h. Keperluan semakan hak akses berkala i. Pembatalan hak akses j. Arkib semua peristiwa penting yang berkaitan dengan penggunaan dan pengurusan identiti pengguna dan maklumat k. Akses *priveleged*	ICTSO, Pengurus ICT dan Pentadbir ICT
050102 Capaian Kepada Rangkaian Dan Perkhidmatan Rangkaian	
Pengguna hanya boleh dibekalkan dengan capaian ke rangkaian dan perkhidmatan rangkaian setelah mendapat kebenaran dari KSM. (A.9.1.2 *Access to network and network services*) Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang perkakasan ICT yang bersesuaian di antara rangkaian KSM, rangkaian agensi lain dan rangkaian awam;	ICTSO, Pengurus ICT dan Pentadbir Rangkaian

b. Mewujud dan menguatkuasakan mekanisme untuk pengesahan pengguna dan perkakasan ICT yang dihubungkan ke rangkaian; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT.	
0502 Pengurusan Capaian Pengguna	
Objektif: Memastikan kawalan capaian oleh pengguna yang dibenarkan sahaja.	
050201 Pendaftaran Pengguna dan Pembatalan Pengguna	
Proses pendaftaran dan pembatalan pengguna hendaklah dilaksanakan bagi membolehkan capaian dan pembatalan hak capaian (A.9.2.1 *User registration and deregistration*) Perkara –perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh KSM sahaja boleh digunakan; b. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; c. Akaun pengguna luar yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada KSM terlebih dahulu; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan dan arahan KSM. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Bagi memastikan pengendalian Internet dan e-mel Mahkamah beroperasi dengan sempurna dan berkesan, KSM adalah bertanggungjawab: g. Menentukan setiap akaun yang diwujudkan atau dibatalkan telah mendapat kelulusan KSM. Pembatalan akaun (pengguna yang tamat perkhidmatan, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan	Pengguna KSM & Pengguna Luar, Pentadbir ICT, Pengurus ICT dan ICTSO

maklumat. KSM boleh membekukan akaun pengguna, jika perlu, semasa pengguna bercuti panjang, berkursus atau pun menghadapi tindakan tatatertib; h. Menggunakan perisian pemecahan kata laluan yang dibenarkan untuk mengenal pasti kata laluan pengguna yang lemah dan kemudiannya mencadang dan memperakukan ciri-ciri kata laluan yang lebih baik kepada pengguna; dan i. Menghalang kemasukan maklumat dari laman Internet yang berunsur ganas, lucah, permainan elektronik atas talian, judi dan lain-lain aktiviti yang dilarang;	
050202 Semakan Akses Pengguna (*Provisioning*)	
Satu proses semakan akses penguna perlu dilaksanakan untuk mengkaji semula kebenaran dan pembatalan capaian penguna ke atas semua aplikasi dan perkhidmatan (A.9.2.2 *User access provisioning*)	Pentadbir ICT, Pengurus ICT dan ICTSO
050203 Pengurusan *Priviledge Access Rights*	
Peruntukan dan penggunaan *Priviledge Access Rights* perlu dihadkan dan dikawal. (A.9.2.3 *Management of priviledge access rights*) Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir ICT, Pengurus ICT dan ICTSO
050204 Pengurusan Kata Laluan Pengguna	
Peruntukan kata laluan perlu melalui beberapa proses pengurusan formal. (A.9.2.4 *Management of secret authentication information of users*) a. Pengguna perlu menandatangani kenyataan untuk menyimpan kata-laluan dan untuk menjaga authentikasi kerahsiaan kumpulan (iaitu *password* yang dikongsi bersama); kenyataan yang ditandatangani boleh dimasukkan dalam terma-terma dan syarat-syarat pekerjaan b. Pengguna perlu disediakan dengan kata laluan sementara, yang	Pengguna KSM & Pengguna Luar, Pentadbir ICT, Pengurus ICT dan ICTSO

c. Prosedur perlu diwujudkan untuk mengesahkan identiti pengguna sebelum menyediakan kata laluan yang baru, penggantian atau sementara d. kata laluan sementara perlu diedar kepada pengguna dengan selamat dimana katalaluan tidak beleh diedarkan oleh pihak ketiga dan dalam *clear text* e. kata laluan sementara yang dicipta hendaklah unik dan susah dianggar f. pengguna perlu mengesahkan penerimaan kata laluan g. kata laluan vendor *default* perlu diubah selepas pemasangan sistem atau perisian.	
050205 Kajian Semula Hak Capaian Pengguna	
Pemilik aset ICT KSM hendaklah mengkaji semula hak pengguna secara berkala atau sekurang-kurangnya satu (1) kali setahun. (A.9.2.5 *Review of user access rights*)	Pentadbir ICT, Pengurus ICT dan ICTSO
050206 Pembatalan atau Pelarasan Hak Akses	
Hak capaian kakitangan dan pengguna pihak luar untuk kemudahan pemprosesan data dan maklumat hendaklah dikeluarkan/dibatalkan selepas penamatan pekerjaan, kontrak atau perjanjian, atau diselaraskan apabila berlaku perubahan dalam KSM. (A.9.2.6 *Removal or adjustment of access rights*) Pembatalan akaun (pengguna yang tamat perkhidmatan, bertukar dan melanggar dasar dan tatacara jabatan) perlulah dilakukan dengan segera atas tujuan keselamatan maklumat. KSM boleh membekukan akaun pengguna, jika perlu, semasa pengguna bercuti panjang, berkursus atau pun menghadapi tindakan tatatertib.	Pentadbir ICT, Pengurus ICT dan ICTSO
0503 Tanggungjawab pengguna	
Objektif: Untuk memastikan pengguna bertanggungjawab untuk melindungi maklumat yang digunakan untuk pengesahihan identiti mereka	
050301 Penggunaan Kata Laluan	
Pengguna perlu mengikut amalan keselamatan yang baik di dalam pemilihan, penggunaan dan pengurusan kata laluan sebagai melindungi	Pengguna KSM &

maklumat yang digunakan untuk pengesahihan identiti. (A.9.3.1 *Use of secret authentication information*) Pengguna perlu: a. Pastikan kata laluan adalah SULIT. b. Kata laluan hendaklah diingat dan TIDAK BOLEH didedahkan dengan apa cara sekalipun; c. Tukar kata laluan apabila terdapat tanda-tanda kebocoran atau kompromi kata laluan. d. Pilih kata laluan yang berkualiti dengan panjang minimum yang mencukupi. e. Tidak menggunakan kata laluan yang sama untuk sistem yang lain. f. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan digit, abjad dan simbol KECUALI bagi perkakasan atau perisian yang mempunyai pengurusan katalaluan yang terhad; g. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; h. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; i. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; k. Mengelakkan penggunaan kata laluan yang sama bagi urusan rasmi dan tidak rasmi.	Pengguna Luar, dan ICTSO
0504 Kawalan Capaian Sistem dan Aplikasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem dan aplikasi	
050401 Had Kawalan Capaian Maklumat	
Akses kepada fungsi maklumat dan sistem aplikasi hendaklah dihadkan mengikut dasar kawalan capaian. (A.9.4.1 *Information access restriction*)	Pentadbir ICT, ICTSO, Pengurus ICT

050402 Prosedur Log-on	
Capaian kepada sistem dan aplikasi hendaklah dikawal oleh prosedur *log-on* mengikut keperluan. KSM hendaklah mengenal pasti teknik pengesahan *log-on* yang sesuai iaitu: (A.9.4.2 *Secure log-on procedure*). Tidak memaparkan pengenalan sistem atau aplikasi selagi proses *log-on* tidak berjaya. Paparkan suatu notis amaran bahawa komputer hanya boleh diakses oleh pengguna yang sah a. Tidak memberikan bantuan mesej semasa prosedur *log-on*. b. Pengesahan *log-on*. c. Perlindungan terhadap *Brute Force log-on*. d. Log "aktiviti *log on*" yang berjaya dan tidak berjaya e. Mengadakan amaran keselamatan jika ada potensi percubaan atau pencerobohan *log-on* berjaya dikesan f. Memaparkan maklumat berikut setelah selesai *log-on* yang berjaya i. Tarikh dan masa *log-on* sebelumnya ii. Butir-butir percubaan *log-on* yang tidak berjaya g. Tidak memaparkan kata laluan h. Tidak menghantar kata laluan dalam "*clear-text*" melalui rangkaian i. Menamatkan sesi yang tidak aktif selepas tempoh yang tertentu. j. Menghadkan sesi sambungan sekatan untuk aplikasi yang berisiko tinggi.	Pentadbir ICT, ICTSO, Pengurus ICT
050403 Sistem Pengurusan Kata Laluan	
Sistem pengurusan kata laluan mestilah interaktif dan menjamin kata laluan yang berkualiti (A.9.4.3 *Password management system*) a. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan digit, abjad dan simbol KECUALI bagi perkakasan atau perisian yang mempunyai pengurusan katalaluan yang terhad; b. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;	Pengguna, Pentadbir ICT, ICTSO, Pengurus ICT

c. Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; d. Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula KECUALI bagi perkakasan atau perisian yang mempunyai pengurusan katalaluan yang terhad; e. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; f. Mengelakkan penggunaan kata laluan yang sama bagi urusan rasmi dan tidak rasmi.	
050404 Pengunaan Utiliti Sistem	
Penggunaan program utiliti yang mungkin mampu *Over-Riding System* oleh itu kawalan perlu dihadkan dan dikawal ketat. (A.9.4.4 *Use of privileged utility programs*)	Pentadbir ICT
050405 Kawalan Akses Kepada *Source Code Program*	
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh BPM, KSM. (A.9.4.5 *Access control to program source code*) a. Kakitangan sokongan KSM perlu dihadkan akses kepada kod sumber (*source code)* b. Log audit perlu dikekalkan kepada semua akses kepada kod sumber c. Penyelenggaraan dan penyalinan kod sumber hendaklah tertakluk kepada prosedur kawalan perubahan yang ketat d. Kod sumber bagi semua aplikasi dan perisian hendaklah menjadi hak milik KSM.	Pentadbir Sistem, Pengurus ICT

BIDANG 06 **KRIPTOGRAFI**	
0601 Kawalan kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
060101 Kawalan Pengunaan Kriptografi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membangun dan melaksanakan peraturan enkripsi untuk melindungi maklumat sensitif menggunakan kaedah kriptografi yang sesuai pada setiap masa; b. Mengenal pasti tahap perlindungan pengunaan kriptografi dengan mengambil kira jenis, kekuatan dan kualiti algoritma yang diperlukan. (A.10.1.1 *Policy on the use of cryptographic control*)	Pengguna KSM dan Pentadbir ICT
060102 Pengurusan Kunci Kriptografi (Key Management)	
Memastikan kaedah yang selamat dan berkesan untuk pengurusan kunci yang menyokong teknik kriptografi diguna pakai di KSM bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut; dan Setiap urusan transaksi maklumat sensitif secara hendaklah menggunakan tandatangan digital supaya mendapat perlindungan dan pengiktirafan undang-undang. (A.10.1.2 *Key Management*)	Pengguna KSM dan Pentadbir ICT

BIDANG 07
KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 Keselamatan Kawasan

Objektif: Mencegah akses fizikal yang tidak dibenarkan yang boleh mengakibatkan kecurian, kerosakan atau gangguan kepada maklumat and kemudahan pemprosesan maklumat KSM

070101 Kawalan Kawasan

Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. (A.11.1.1 *Physical security parameter*) Perkara yang perlu dipatuhi adalah seperti 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; d. Menghadkan jalan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g. Mewujudkan perkhidmatan kawalan keselamatan; h. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan dan pelawat yang diberi kebenaran sahaja boleh melalui pintu masuk tersebut; i. Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan mengikut Arahan Keselamatan Kerajaan;	Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK), Bahagian Pengurusan, CIO dan ICTSO

j. Merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; k. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya; dan m. Log bagi kad akses ke pintu-pintu kawalan mestilah disemak sekurang-kurangnya setahun sekali.	
070102 Kawalan Masuk Fizikal	
Kawalan masuk fizikal adalah bertujuan untuk mewujudkan kawalan keluar masuk ke premis KSM. (A.11.1.2 *Physical entry controls*) Perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pegawai dan kakitangan KSM hendaklah mempamerkan Pas Keselamatan sepanjang waktu bertugas. Semua pas keselamatan hendaklah dikembalikan kepada KSM apabila bertukar, tamat perkhidmatan atau bersara; b. Setiap pelawat hendaklah mendaftar dan mendapatkan pas keselamatan pelawat di kaunter keselamatan dan hendaklah dikembalikan selepas tamat lawatan; dan c. Hanya pengguna yang diberi kebenaran sahaja boleh menggunakan aset ICT KSM.	Pengguna KSM, Pengguna Luar, Bahagian Pengurusan
070103 Kawalan Pejabat, Bilik dan Tempat Operasi	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Kawasan tempat berkerja, bilik dan tempat operasi ICT perlu dihadkan daripada akses oleh orang luar. b. Penunjuk ke lokasi bilik operasi dan tempat larangan tidak harus menonjol dan hanya memberi petunjuk minimum (A.11.1.3 *Securing offices, rooms and facilities*)	ICTSO, Pejabat KPKK dan Bahagian Pengurusan
070104 Perlindungan Terhadap Ancaman Luaran dan Dalaman	

KSM perlu merekabentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau bilau dan bencana. (11.1.4 *Protecting against external and internal environmental threats*)	ICTSO, Pejabat KPKK dan Bahagian Pengurusan

070105 Kawalan Tempat Larangan (*Working In Secure Area*)	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai yang diberi kebenaran sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. (11.1.5 *Working in secure area*) Kawasan larangan di KSM adalah Bilik Fail, Bilik Stor ICT, Pusat Data (*Data Centre*) dan Pusat Pemulihan Bencana (*Disaster Recovery Centre*). Perkara yang perlu dipatuhi adalah seperti berikut: a. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; Pihak lain adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali dengan kebenaran khas KSM dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; b. kerja tanpa pengawasan oleh kontraktor di kawasan larangan harus dielakkan ; c. Bilik dalam kawasan larangan perlu dikunci pada setiap masa; d. Fotografi, video, audio dan peralatan rakaman lain tidak dibenarkan dibawa masuk melainkan dengan kebenaran; dan e. Pengguna KSM dan pengguna luar yang perlu berurusan di pusat data hendaklah memaklumkan kepada Pentadbir Pusat Data terlebih dahulu dan mengisi buku log keluar masuk Pusat Data.	ICTSO, Pejabat KPKK dan Bahagian Pengurusan
070106 Kawasan Penghantaran dan Pemunggahan	
KSM hendaklah memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya. (11.1.6 *Delivery and loading area*)	ICTSO, Pejabat KPKK dan Bahagian Pengurusan
0702 Keselamatan Peralatan ICT	
Objektif: Melindungi peralatan ICT KSM dari kehilangan, kerosakan, kecurian dan disalahgunakan.	
070201 Peralatan ICT	
Peralatan ICT hendaklah dijaga dan dikawal selia dengan baik. (A.11.2.1 *Equipment sitting and protection*) Perkara yang perlu dipatuhi adalah seperti berikut: a. Memeriksa dan memastikan semua peralatan ICT di bawah kawalan pengguna berfungsi dengan sempurna;	Pengguna KSM, Pengguna Luar dan ICTSO

b. Bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

c. Pengguna dilarang sama sekali menambah, menanggal atau mengganti sebarang peralatan ICT yang telah ditetapkan;

d. Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT;

e. Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

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

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

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

i. 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;

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

k. Peralatan ICT yang hilang hendaklah dilaporkan segera kepada pihak Polis, Ketua Jabatan dan ICTSO;

l. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

m. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada *Help Desk* KSM untuk dibaik pulih;

n. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

o. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal;

p. Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password)* yang telah ditetapkan oleh Pentadbir Sistem ICT;

q. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; dan r. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO.	
070202 Alat Sokongan	
a. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; b. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); c. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; dan d. Semua alat sokongan perlu disemak dan dikemaskinikan dari masa kesemasa (sekurang-kurangnya setahun sekali). (A.11.2.2 *Supporting utilities*)	Pengguna KSM, Pengguna Luar dan ICTSO
070203 Keselamatan Kabel	
Kabel termasuk kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat hendaklah dilindungi. (A.11.2.3 *Cabling security*) 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.	Pentadbir Pusat Data
070204 Penyelenggaraan Peralatan	
Peralatan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. (A.11.2.4 *Equipment maintenance*) Perkara yang perlu dipatuhi adalah seperti berikut:	Semua Pengguna, Pegawai Aset dan Pengurus ICT

a. Semua peralatan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b. Memastikan peralatan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap peralatan bagi penyelenggaraan peralatan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; d. Menyemak dan menguji semua peralatan sebelum dan selepas proses penyelenggaraan; e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	
070205 Peralatan Dibawa Keluar Permis	
a. Peralatan ICT yang hendak dibawa keluar dari premis KSM untuk tujuan rasmi, perlulah mendapat kelulusan Ketua Setiausahaatau pegawai yang diturunkan kuasa dan direkodkan bagi tujuan pemantauan serta tertakluk kepada tujuan yang dibenarkan (A.11.2.5 *Removal of assets*); dan b. Aktiviti peminjaman dan pemulangan perkakasan ICT mestilah direkodkan oleh pegawai yang berkenaan	Semua Pengguna, Pegawai Aset dan Ketua Jabatan
070206 Keselamatan Peralatan di Luar Premis	
Peralatan yang dibawa keluar dari premis KSM adalah terdedah kepada pelbagai risiko. (A.11.2.6 *Security of equipment off-premises*) 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 Pengguna dan Pegawai Aset
070207 Pelupusan Peralatan dan Kitar Semula	

Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh KSM dan ditempatkan di KSM. (A.11.2.7 *Secure disposal or re-use of equipment*) Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KSM. Perkara yang perlu dipatuhi adalah seperti berikut:	Semua Pengguna, Pegawai Aset dan Ketua Jabatan

a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran;

b. Sekiranya maklumat perlu disimpan, maka pengguna bolehlah membuat penduaan;

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 inventori Sistem Pengurusan Aset;

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

h. Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara seperti berikut:

   i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya;

   ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana-mana Bahagian di KSM;

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

   iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab KSM; dan

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

070208 Penjagaan Peralatan Yang Tidak Diguna (*Unattended User Equipment*)	
Pengguna perlu memastikan bahawa peralatan dijaga dan mempunyai perlindungan yang sewajarnya iaitu dengan mematuhi perkara berikut: (A.11.2.8 *Unattended User Equipment*) a. Tamatkan sesi aktif apabila selesai tugas. b. *Log-off* kerangka utama, pelayan dan PC pejabat apabila sesi bertugas selesai. c. PC atau terminal selamat daripada pengguna yang tidak dibenarkan.	Semua Pengguna
070209 Clear Desk dan Clear Screen	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. (A.11.2.9 *Clear Desk and Clear Screen Policy)* *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 yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kemudahan *password screen saver* atau *logout* apabila meninggalkan komputer; b. Menyimpan bahan-bahan sensitif seperti '*electronic storage media'* dan dokumen terperingkat di dalam laci atau kabinet fail yang berkunci; c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat. d. E-mel masuk dan keluar hendaklah dikawal; dan e. Menghalang penggunaan tanpa kebenaran mesin fotokopi dan teknologi penghasilan semula seperti mesin pengimbas dan kamera digital.	Semua Pengguna

BIDANG 08 **PENGURUSAN OPERASI**	
0801 Pengurusan Prosedur Operasi	
Objektif: Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan ke atas kemudahan pemprosesan maklumat	
080101 Pengendalian Prosedur	
Bagi memastikan kemudahan pemprosesan maklumat beroperasi seperti yang telah ditetapkan dan selamat, perkara yang perlu dipatuhi adalah seperti berikut: (A.12.1.1 *Documented operating procedures*) 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.	Pengurus ICT, Pentadbir ICT dan ICTSO
080102 Kawalan Perubahan	
Tanggungjawab dan tugas perlulah diasingkan untuk mengelakkan perubahan yang tidak dibenarkan atau penyalahgunaan aset KSM. (A.12.1.2 *Change management)* Oleh itu, 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; b. Aktiviti-aktiviti seperti memasang, menyelenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Semua Pengguna, Pengurus ICT dan Pentadbir ICT

080103 Perancangan Kapasiti	
a. 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. (A.12.1.3 *Capacity management*); dan b. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Sistem, Pentadbir Emel, Pentadbir Pusat Data dan Pengurus ICT
080104 Pengasingan Kemudahan Pembangunan, Ujian dan Operasi	
a. Perkakasan yang digunakan bagi tugas membangun, mengemaskini, menyelenggara dan menguji aplikasi perlu diasingkan dari perkakasan yang digunakan sebagai pengeluaran (*production*). b. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian. (A.12.1.4 *Separation of development, test and operational facilities*)	Pentadbir Sistem dan Pengurus ICT
0802 Perisian Berbahaya (*Protection from Malware*)	
Objektif: Untuk memastikan bahawa kemudahan pemprosesan maklumat dan maklumat dilindungi daripada *malware*.	
080201 Perlindungan dari Perisian Berbahaya	
Perkara yang perlu dipatuhi adalah seperti berikut: (A.12.2.1 *Controls against malware*) a. Pengguna perlu merujuk kepada garis panduan yang disediakan. b. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; c. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; d. Mengimbas semua perisian atau sistem dengan anti virus sebelum menggunakannya; e. Mengemas kini anti virus dengan *pattern* antivirus yang terkini. Pengemaskinian perlu dilakukan sekurang-kurangnya sekali sehari atau apabila terdapat *pattern* terkni; f. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat;	Semua Pengguna, Pentadbir ICT dan ICTSO

g. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; h. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi perisian berbahaya; i. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan j. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
0803 *Backup*	
Objektif: Memastikan segala data diselenggara agar penyimpanan data diuruskan dengan sempurna.	
080301 Backup Maklumat (*Information Backup*)	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. (A.12.3.1 *Information backup*) Perkara yang perlu dipatuhi adalah seperti berikut: a. Penyediaan *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. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat; e. Membuat salinan pendua ke atas semua data dan maklumat mengikut kesesuaian operasi; dan f. *Backup* hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan *backup* bergantung pada tahap kritikal maklumat.	Pengguna KSM dan Pentadbir ICT

0804 Log dan Pemantauan	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
080401 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit (*audit trail*). Jejak audit merekod aktiviti-aktiviti penguna KSM yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. (A.12.4.1 *Event logging*) a. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: i. Rekod setiap aktiviti transaksi pengguna; ii. Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; iii. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan iv. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. b. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. c. Pentadbir 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.	Pengguna KSM, Pentadbir Sistem, Pentadbir Emel, Pentadbir Rangkaian dan ICTSO
080402 Perlindungan Log	
Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebara*ng capaian yang tidak dibenarkan (A.12.4.2 Protection of log information*)	Pentadbir Pusat Data, Pentadbir Sistem, Pentadbir Rangkaian, Pentadbir Emel dan ICTSO
080403 Log pentadbir dan Operator	
a. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujud dan hasilnya perlu dipantau secara berkala; b. Aktiviti pentadbir dan pengendali sistem perlu direkodkan. Aktiviti log hendaklah dilindungi dan catatan jejak audit disemak dari semasa ke	Pentadbir Pusat Data, Pentadbir Sistem, Pentadbir

semasa dan menyediakan laporan jika perlu. (A.12.4.3 *Administrator and operator log*); c. Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya; d. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; dan e. Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada Pegawai Keselamatan Teknologi Maklumat (ICTSO) dan CIO	Rangkaian, Pentadbir Emel dan ICTSO
080404 *Clock Synchronisation*	
Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KSM atau domain keselamatan perlu diselaraskan dengan satu sumber waktu. (A.12.4.4 *Clock Syncronization*)	Pentadbir Pusat Data
0805 Kawalan Perisian Operasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
080501 Pemasangan Perisian Pada Sistem Operasi	
a. Pengemaskinian perisian operasi, aplikasi dan *program libraries* hanya boleh dilakukan oleh pentadbir terlatih setelah mendapat kelulusan pengurusan. (A.12.5.1 *Installation of software on operational systems*) b. Sistem operasi hanya boleh memegang "*executable code*" dan tidak kod pembangunan atau penyusun. c. Penggunaan aplikasi dan sistem operasi hanya boleh dilaksanakan selepas ujian yang terperinci dan diperakui berjaya. d. Setiap konfigurasi ke atas sistem perlu dikawal dan didokumentasikan melalui satu sistem kawalan konfigurasi. Konfigurasi hanya boleh dilaksanakan selepas mendapat persetujuan dari pihak berkaitan. e. Satu "*rollback*" strategi harus diadakan sebelum perubahan dilaksanakan. f. Versi lama perisian perlu diarkibkan selaras dengan Pengurusan Rekod Elektronik, Jabatan Arkib Negara.	Pentadbir Sistem & Pengurus ICT

0806 Kawalan Teknikal Keterdedahan (*Vulnerability*)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah yang bersesuaian untuk menjamin keberkesanannya.	
080601 Kawalan dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. (A.12.6.1 *Management of technical vulnerabilities*) 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 kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem
080602 Kawalan Pemasangan Perisian	
a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan pengguna di KSM; (A.12.6.2 *Restriction on software installation*) 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.	Penguna KSM, Pentabir Sistem dan ICTSO
0807 Pertimbangan Audit Sistem Maklumat	
Objektif: Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan	
080701 Pematuhan Keperluan Audit/Kawalan Audit Sistem Maklumat	
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. (A.12.7.1 *Information systems audit controls*)	ICTSO & Audit Dalaman

BIDANG 09 PENGURUSAN KOMUNIKASI	
0901 Pengurusan Keselamatan Rangkaian	
Objektif: Memastikan perlindungan pemprosesan maklumat dalam rangkaian.	
090101 Kawalan Infrastruktur Rangkaian	
Sistem dan aplikasi hendaklah dikawal dan diuruskan sebaik mungkin di dalam infrastruktur rangkaian daripada sebarang ancaman. (A.13.1.1 *Network control*) Perkara yang perlu dipatuhi adalah seperti berikut: a. Bertanggungjawab dalam memastikan kerja-kerja operasi rangkaian dilindungi daripada pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah ditempatkan di lokasi yang mempunyai ciri-ciri fizikal yang selamat dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja; d. Semua peralatan rangkaian hendaklah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e. *Firewall* hendaklah dipasang, dikonfigurasi dan diselia oleh Pentadbir Rangkaian; f. Semua trafik keluar dan masuk rangkaian hendaklah melalui *firewall* di bawah kawalan BPM, KSM; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran daripada Pegawai Keselamatan Teknologi Maklumat (ICTSO); h. Memasang perisian *Intrusion Prevention System* (IPS) bagi mencegah sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam data dan maklumat KSM; i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan BPM, KSM adalah tidak dibenarkan; k. Semua pengguna hanya dibenarkan menggunakan rangkaian sedia ada di KSM sahaja dan penggunaan modem adalah dilarang sama sekali; l. Kemudahan bagi *wireless* LAN hendaklah dipantau dan dikawal penggunaannya;	Pengguna, Pentadbir Rangkaian dan ICTSO

m. Semua perjanjian perkhidmatan rangkaian hendaklah mematuhi *Service Level Assurance* (SLA) yang telah ditetapkan. n. Menempatkan atau memasang antara muka (*interfaces*) yang bersesuaian di antara rangkaian KSM, rangkaian agensi lain dan rangkaian awam; o. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; p. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT yang dibenarkan sahaja; q. Mengawal capaian fizikal dan logikal ke atas kemudahan port diagnostik dan konfigurasi jarak jauh; r. Mengawal sambungan ke rangkaian khususnya bagi kemudahan yang dikongsi dan menjangkau sempadan KSM; dan s. Mewujud dan melaksana kawalan pengalihan laluan (*routing control*) bagi memastikan pematuhan terhadap peraturan KSM.	
090102 Keselamatan Perkhidmatan Rangkaian	
Pengurusan bagi semua perkhidmatan rangkaian (*inhouse atau outsource*) yang merangkumi mekanisme keselamatan dan tahap perkhidmatan hendaklah dikenalpasti dan dimasukkan di dalam perjanjian perkhidmatan rangkaian. (A.13.1.2 *Security of network services*)	Pentadbir Rangkaian, Pengurus ICT dan ICTSO
090103 Pengasingan rangkaian	
Pengasingan rangkaian hendaklah dibuat untuk membezakan kumpulan pengguna dan sistem maklumat mengikut segmen rangkaian KSM. (A.13.1.3 *Segregation of network*)	Pentadbir Rangkaian, Pengurus ICT dan ICTSO
0902 Pemindahan Maklumat	
Objektif: Memastikan keselamatan perpindahan/pertukaran maklumat dan perisian antara KSM dan pihak luar terjamin.	
090201 Dasar dan Prosedur Pemindahan Maklumat	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Dasar, prosedur dan kawalan pemindahan maklumat yang formal hendaklah diwujudkan untuk melindungi pemindahan maklumat melalui sebarang jenis kemudahan komunikasi; b. Terma pemindahan maklumat dan perisian di antara KSM dengan pihak luar hendaklah dimasukkan di dalam Perjanjian;	Semua Pengguna, Pentadbir Rangkaian, Pentadbir Emel dan ICTSO

c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan maklumat; dan d. Memastikan maklumat yang terdapat dalam mel elektronik hendaklah dilindungi sebaik-baiknya. (A.13.2.1 *Information transfer policies and procedures)*	
090202 Perjanjian Mengenai Pemindahan Maklumat	
KSM perlu mengambil kira keselamatan maklumat organisasi atau menandatangani perjanjian bertulis apabila berlaku pemindahan maklumat organisasi antara KSM dengan pihak luar. Perkara yang perlu dipertimbangkan adalah: (A.13.2.2 *Agreement on information transfer*) a. Tanggungjawab pengurusan bagi mengawal penghantaran dan penerimaan maklumat organisasi. b. Prosedur bagi pengesanan maklumat organisasi semasa pemindahan maklumat. d.Tanggungjawab dan liabiliti sekiranya berlaku insiden keselamatan maklumat seperti kehilangan data.	CIO dan Pengurus ICT
090203 Pengurusan Mel Elektronik (E-mel)	
Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan Bilangan 1 Tahun 2003 dan mana-mana undang-undang bertulis yang berkuat kuasa. (A.13.2.3 *Electronic messaging*) Perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut: a. Menggunakan akaun atau alamat mel elektronik (e-mel) KSM bagi urusan rasmi. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh KSM; 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;	Semua Pengguna

e. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu, tidak melebihi sepuluh megabait (10Mb) semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan; f. Pengguna dilarang 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. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; k. Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; l. Pengguna hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan m. Pengguna hendaklah bertanggungjawab ke atas penyelenggaraan *mailbox* masing-masing.	
090204 Kerahsiaan dan *Non-Disclosure* Agreement	
Syarat-syarat perjanjian kerahsiaan atau *non-disclosure* perlu mengambil kira keperluan organisasi dan hendaklah disemak dan dokumentasikan dari masa ke semasa. (A.13.2.4 *Confidentiality* and *non-disclosure agreement*)	CIO, BPM dan ICTSO

BIDANG 10 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM	
1001 Keperluan Keselamatan Sistem Maklumat	
Objektif: Memastikan keselamatan maklumat adalah merupakan sebahagian daripada proses pembangunan sistem. Ini merangkumi keperluan keselamatan maklumat apabila menggunakan rangkaian luar.	
100101 Analisis Keperluan dan Spesifikasi Keselamatan Maklumat	
Keperluan keselamatan maklumat bagi pembangunan sistem baru dan penambahbaikan sistem hendaklah mematuhi perkara-perkara berikut: (A.14.1.1 *Information security requirements analysis and spesifications*) a. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah dikaji kesesuaiannya mengikut keperluan pengguna dan selaras dengan Dasar Keselamatan ICT KSM. b. Penyediaan rekabentuk, pengaturcaraan dan pengujian sistem hendaklah mematuhi kawalan keselamatan yang telah ditetapkan; dan c. Ujian keselamatan hendaklah dilakukan di setiap peringkat pembangunan sistem bagi memastikan kesahihan dan integriti data.	Pemilik Sistem dan Pentadbir Sistem
100102 Keselamatan Perkhidmatan Aplikasi di Rangkaian Umum	
Maklumat aplikasi yang melalui rangkaian umum (*public networks*) hendaklah dilindungi daripada aktiviti penipuan dan pendedahan maklumat yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut: (A.14.1.2 *Securing application services on public networks*) a. Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (*authentication*). b. Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi. c. Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaan perkhidmatan ICT. d. Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak. e. Liabiliti yang berkaitan dengan mana-mana kes transaksi *fraud*. f. Keperluan insuran	ICTSO, Pentadbir Rangkaian dan Pentadbir Sistem
100103 Melindungi Perkhidmatan Transaksi Aplikasi	
Maklumat yang terlibat dalam perkhidmatan transaksi hendaklah dilindungi daripada penghantaran yang tidak lengkap, *mis-routing*,	ICTSO, Pentadbir

pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan dan duplikasi mesej. Perkara yang perlu dipertimbangkan adalah seperti berikut: (A.14.1.3 *Protecting application services transactions*) a. Penggunaan tandatangan elektronik oleh setiap pihak yang terlibat dalam transaksi b. Memastikan semua aspek transaksi dipatuhi: i. Maklumat pengesahan pengguna adalah sah digunakan dan telah disahkan ii. Mengekalkan kerahsiaan maklumat iii. Mengekalkan privasi pihak yang terlibat iv. Komunikasi antara semua pihak yang terlibat dirahsiakan v. Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi c. Pihak yang mengeluar dan mengekalkan pensijilan digital atau tandatangan adalah dilantik oleh Kerajaan.	Rangkaian dan Pentadbir Sistem
1002 Keselamatan Dalam Pembangunan Sistem	
Objektif: Memastikan sistem yang dibangunkan mempunyai ciri-ciri keselamatan ICT yang bersesuaian bagi menghalang kesilapan, kehilangan, pindaan yang tidak sah dan penyalahgunaan maklumat dalam aplikasi.	
100201 Dasar Keselamatan Dalam Pembangunan Sistem	
Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan untuk perkembangan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut: (A.14.2.1 *Secure development policy*) a. Keselamatan persekitaran pembangunan b. Panduan keselamatan dalam kitar hayat pembangunan (*development lifecycle*) perisian c. Keselamatan dalam fasa reka bentuk d. Pemeriksaan keselamatan dalam perkembangan projek e. Keselamatan repositori f. Keselamatan dalam kawalan versi g. Keperluan pengetahuan keselamatan dalam pembangunan perisian h. Kebolehan pembekal untuk mengenalpasti kelemahan dan mencadangkan penambahbaikan dalam pembangunan sistem	Pentadbir Sistem dan ICTSO

100202 Prosedur Kawalan Perubahan Sistem	
Perubahan ke atas sistem hendaklah dikawal. Perkara yang perlu dipatuhi adalah seperti berikut: (A.14.2.2 *System change control procedures*) a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, didokumentasi dan disahkan sebelum diguna pakai; b. Setiap perubahan kepada sistem pengoperasian perlu dikaji semula dan diuji untuk memastikan tiada sebarang masalah yang timbul terhadap operasi dan keselamatan agensi. c. *Change Control Board* perlu bertanggungjawab untuk memantau penambahbaikan dan perubahan yang dilakukan oleh pembekal; d. Kawalan perlu dibuat ke atas sebarang perubahan atau pindaan ke atas sistem bagi memastikan ianya terhad mengikut keperluan sahaja.	*Change Control Board* dan Pentadbir Sistem
100203 Kajian Teknikal Selepas Permohonan Perubahan Platform	
Perkara yang perlu dipatuhi adalah seperti berikut: (A.14.2.3 *Technical review of applications after operating platform changes*) a. Kawalan aplikasi dan prosedur integriti disemak untuk memastikan sistem tidak terjejas apabila berlaku perubahan platform. b. Perubahan platform dimaklumkan dari masa ke semasa bagi membolehkan ujian yang bersesuaian dilakukan sebelum pelaksanaan. c. Memastikan perubahan yang sesuai dibuat kepada pelan kesinambungan organisasi.	Pentadbir Sistem dan Pengurus ICT
100204 Sekatan Perubahan Pakej Perisian (*Software Packages*)	
Perubahan kepada pakej perisian adalah tidak digalakkan tetapi terhad kepada perubahan yang diperlukan dan semua perubahan hendaklah dikawal dengan ketat. (A.14.2.4 *Restrictions on changes to software packages*)	Pentadbir Sistem, Pengurus ICT dan ICTSO
100205 Prinsip Kejuruteraan Keselamatan Sistem (S*ecure System Engineering Principles*)	
Prinsip-prinsip kejuruteraan keselamatan sistem hendaklah diwujudkan, didokumentasi, diselenggara dan digunapakai dalam pelaksanaan sistem. (A.14.2.5 *Secure System Engineering Principles*) Keselamatan perlu diambilkira dalam semua peringkat pembangunan sistem.	Pentadbir Sistem dan Pengurus ICT

Prinsip dan prosedur kejuruteraan hendaklah sentiasa dikaji dari masa ke semasa bagi memastikan keberkesanan kepada keselamatan maklumat.	
100206 Keselamatan Persekitaran Pembangunan Sistem	
Persekitaran pembangunan sistem hendaklah selamat bagi melindungi keseluruhan kitaran hayat pembangunan sistem (*development lifecycle*). (A.14.2.6 *Secure development environment*)	Pentadbir Sistem dan Pengurus ICT
100207 Pembangunan Sistem Secara *Outsource*	
Pembangunan sistem secara *outsource* perlu sentiasa dikawalselia dan dipantau (A.14.2.7 *Outsourced development*). Kod sumber (*source code)* bagi semua aplikasi dan perisian hendaklah menjadi hak milik Kerajaan. *Intellectual property rights* (IPR) aplikasi dan perisian yang dibangun oleh pihak ketiga kepada KSM adalah hak milik Kerajaan.	Pentadbir Sistem dan Pengurus ICT
100208 Pengujian Keselamatan Sistem	
a. Pengujian keselamatan sistem hendaklah dijalankan semasa pembangunan. b. Semua sistem baru dan penambahbaikan sistem hendaklah menjalani ujian *Security Posture Assessment* (SPA) termasuk penyediaan jadual terperinci aktiviti, ujian input dan output (*input and output validation*). (A.14.2.8 *System security testing*) c. Menyemak dan mengesahkan input data sebelum dimasukkan ke dalam aplikasi bagi menjamin proses dan ketepatan maklumat; d. Mengenalpasti dan melaksanakan kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi; e. Membuat semakan pengesahan di dalam aplikasi untuk mengenalpasti sebarang pencemaran maklumat sama ada kerana kesilapan atau disengajakan; dan f. Menjalankan proses semak ke atas output data daripada setiap proses aplikasi untuk menjamin ketepatan dan kesesuaian.	Pentadbir Sistem dan ICTSO
100209 Penerimaan Pengujian Sistem	
Penerimaan pengujian semua sistem baru dan penambahbaikan sistem hendaklah memenuhi kriteria yang ditetapkan sebelum sistem digunapakai. (A.14.2.9 *System accepting testing*)	Pentadbir Sistem dan ICTSO

1003 Data Ujian	
100301 Perlindungan Data Ujian	
a. Data dan atur cara yang hendak diuji perlu dipilih, dilindungi dan dikawal. b. Pengujian hendaklah dibuat ke atas atur cara yang terkini. c. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan. (A.14.3.1 *Protection of test data*)	Pemilik Sistem dan Pentadbir Sistem

BIDANG 11 HUBUNGAN DENGAN PEMBEKAL	
1101 Keselamatan Maklumat Dalam Hubungan Dengan Pembekal	
Objektif: Memastikan perlindungan aset KSM yang boleh diakses oleh pembekal	
110101 Dasar Keselamatan Maklumat Untuk Pembekal	
Keperluan keselamatan maklumat hendaklah dipersetujui dan didokumentasikan dengan pembekal bagi mengurangkan risiko kepada aset KSM. Perkara yang perlu dipertimbangkan adalah seperti berikut: (A.15.1.1 *Information security policy for supplier relationships*) a. Mengenal pasti dan mendokumentasi jenis pembekal mengikut kategori b. Proses kitaran hayat (*lifecycle*) yang seragam untuk menguruskan pembekal c. Mengawal dan memantau akses pembekal d. Keperluan minimum keselamatan maklumat bagi setiap pembekal dinyatakan dalam perjanjian e. Jenis-jenis obligasi kepada pembekal f. Pelan kontingensi (*contingency plan*) bagi memastikan ketersediaan kemudahan pemprosesan maklumat g. Latihan Kesedaran Keselamatan untuk KSM dan pembekal	BPM dan Pembekal
110102 Menangani Keselamatan Maklumat Dalam Perjanjian Pembekal	
Semua keperluan keselamatan maklumat hendaklah relevan dan dipersetujui dengan setiap pembekal bagi mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur, maklumat organisasi IT (A.15.1.2 *Addressing security within supplier agreements*). Perkara-perkara yang perlu diambil kira seperti berikut: a. Penerangan maklumat keselamatan b. Skim klasifikasi maklumat c. Keperluan undang-undang dan peraturan d. Obligasi setiap pihak bagi kawalan akses, pemantauan, pelaporan dan pengauditan e. Penerimaan peraturan penggunaan maklumat oleh pembekal f. Latihan teknikal dan kesedaran keselamatan maklumat g. Tapisan keselamatan pembekal h. Hak untuk mengaudit pembekal i. Kewajipan pembekal mematuhi keperluan keselamatan maklumat	BPM dan Pembekal

110103 Kawalan Rantaian Bekalan Maklumat dan Komunikasi	
Perjanjian dengan pembekal hendaklah mengambil kira keperluan keselamatan maklumat untuk menangani risiko yang berkaitan dengan rantaian bekalan maklumat dan komunikasi. (A.15.1.3 *Information and communication technology supply chain*). Perkara-perkara yang perlu diambil kira adalah seperti berikut: a. Menentukan keperluan keselamatan maklumat untuk kegunaan perolehan produk dan perkhidmatan. b. Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada subkontraktor bagi perkhidmatan. c. Pembekal utama hendaklah menyebarkan keperluan keselamatan maklumat kepada pembekal-pembekal lain bagi pembekalan produk. d. Melaksanakan satu proses/kaedah pemantauan yang boleh mengesahkan pembekalan produk dan perkhidmatan mematuhi keperluan keselamatan maklumat KSM. e. KSM hendaklah mengenal pasti komponen produk dan perkhidmatan kritikal dan komponen tambahan. f. Memastikan jaminan dari pembekal bahawa semua komponen produk dan perkhidmatan sentiasa dapat dibekalkan dan berfungsi dengan baik. g. Menentukan kaedah-kaedah bagi perkongsian maklumat mengenai rantaian bekalan (*supply chain*) antara organisasi dan pembekal	BPM dan Pembekal
1102 Pengurusan Penyampaian Perkhidmatan Pembekal	
110201 Pemantauan dan Kajian Perkhidmatan Pembekal	
KSM hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal. Perkara-perkara yang perlu diambil kira adalah seperti berikut: (A.15.2.*1 Monitoring and review supplier services*) a. Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan b. Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan. c. Memaklumkan mengenai insiden keselamatan kepada pembekal dan mengkaji maklumat ini seperti yang dikehendaki dalam perjanjian.	BPM dan Pembekal

110202 Pengurusan Perubahan Perkhidmatan Pembekal Perkara yang perlu diambilkira adalah seperti berikut: (A.15.2.2 *Managing changes to supplier services*) a. Perubahan dalam perjanjian dengan pembekal b. Perubahan yang dilakukan oleh KSM bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur c. Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran pembekal dan sub-kontraktor.	BPM dan Pembekal

BIDANG 12 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN	
1201 Pengurusan dan Penambahbaikan Insiden Keselamatan Maklumat	
Objektif: Memastikan insiden keselamatan maklumat dikendalikan dengan cepat, teratur dan berkesan bagi meminimumkan kesan insiden dan mengenal pasti komunikasi serta kelemahan apabila berlaku insiden.	
120101 Tanggungjawab dan Prosedur	
Tanggungjawab dan prosedur pengurusan hendaklah diwujudkan untuk memastikan maklum balas yang cepat, berkesan dan teratur terhadap insiden keselamatan maklumat. (A.16.1.1 *Responsibilities and procedures*)	ICTSO, Pengurus ICT dan CERT KSM
120102 Mekanisme Pelaporan Insiden	
Insiden keselamatan ICT atau ancaman yang mungkin berlaku ke atas aset ICT yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT atau ancaman yang berlaku hendaklah dilaporkan kepada ICTSO. Selepas itu ICTSO hendaklah melaporkan kepada GCERT MAMPU dengan kadar segera: (A.16.1.2 *Reporting information security events*). Perkara yang perlu dipertimbangkan adalah seperti berikut: a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa b. Maklumat disyaki hilang dan didedahkan kepada pihak-pihak yang tidak diberi kuasa; c. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; d. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; e. Kata laluan atau mekanisme kawalan akses disyaki hilang, dicuri atau didedahkan; f. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan g. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di KSM – Lampiran 3 Prosedur pelaporan insiden keselamatan ICT berdasarkan:	Pengguna, ICTSO dan CERT KSM

a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
120103 Melaporkan Kelemahan Keselamatan ICT	
Kakitangan dan pembekal yang menggunakan sistem dan perkhidmatan maklumat KSM dikehendaki mengambil maklum dan melaporkan sebarang kelemahan keselamatan maklumat ICT. (A.16.1.3 *Reporting security weaknesses*)	Semua Pengguna
120104 Penilaian dan Keputusan Mengenai Aktiviti Keselamatan Maklumat	
Aktiviti keselamatan maklumat hendaklah dinilai dan diputuskan sama ada untuk diklasifikasikan sebagai insiden keselamatan maklumat. (A.16.1.4 *Assessment of and decision on information security events*)	ICTSO dan BPM
120105 Pengurusan Maklumat Insiden Keselamatan ICT	
Insiden keselamatan maklumat hendaklah dikendalikan mengikut prosedur yang telah ditetapkan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (A.16.1.5 *Response to information security incidents*) a. Mengumpul bukti secepat mungkin selepas insiden keselamatan berlaku; b. Menjalankan kajian forensik sekiranya perlu; c. Menghubungi pihak yang berkenaan dengan secepat mungkin; d. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; e. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; f. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; g. Menyediakan tindakan pemulihan segera; dan h. Memaklum atau mendapatkan nasihat pihak berkuasa berkaitan sekiranya perlu.	ICTSO, BPM dan CERT KSM

120106 Pengalaman Dari Insiden Keselamatan Maklumat	
Pengetahuan dan pengalaman yang diperolehi daripada menganalisis dan menyelesaikan kes-kes insiden keselamatan maklumat perlu digunakan untuk mengurangkan kemungkinan dan kesan kejadian pada masa depan. (A.16.1.6 *Learning from information security incidents*)	ICTSO, BPM dan CERT KSM
120107 Pengumpulan Bahan Bukti	
KSM hendaklah menentukan prosedur untuk mengenalpasti koleksi, pemerolehan dan pemeliharaan maklumat yang boleh dijadikan sebagai bahan bukti. (A.16.1.7 *Collection of evidence*)	ICTSO, BPM dan CERT KSM

BIDANG 13 **Aspek keselamatan maklumat dalam Pengurusan Kesinambungan Perkhidmatan**	
1301 Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
Objektif:Keselamatan maklumat hendaklah diberi penekanan dalam sistem pengurusan kesinambungan organisasi	
130101 Rancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
KSM hendaklah membangunkan pelan kesinambungan perkhidmatan dan mengenal pasti aspek keselamatan maklumat. (A.17.1.1 *Planning information security continuity*) Ini bertujuan memastikan tiada gangguan kepada proses dalam penyediaan perkhidmatan organisasi dan mengenal pasti keselamatan maklumat pada lokasi kesinambungan perkhidmatan. Pelan ini mestilah diluluskan oleh CIO.	CIO dan Pasukan Pemulihan Bencana
130102 Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
KSM hendaklah mewujud, mendokumentasi, melaksana dan mengekalkan proses, prosedur serta kawalan untuk memastikan tahap keselamatan maklumat bagi kesinambungan perkhidmatan dalam situasi yang terancam. Perkara berikut perlu diberi perhatian: (A.17.1.2 *Implementing information security continuity*) a. Mengenalpasti aspek keselamatan dalam membangunkan pelan kesinambungan keselamatan. b. Mengenalpasti semua aset, tanggungjawab, struktur organisasi dan menetapkan prosedur kecemasan atau pemulihan amalan terbaik; c. Mengenalpasti peristiwa atau ancaman yang boleh mengakibatkan gangguan terhadap proses organisasi; d. Mengenalpasti kemungkinan dan impak gangguan tersebut serta akibatnya terhadap keselamatan ICT; e. Menjalankan analisis impak organisasi; f. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; g. Mendokumentasikan proses dan prosedur yang telah ditetapkan; h. Mengadakan program latihan secara berkala kepada warga KSM mengenai prosedur kecemasan; i. Membuat *backup* mengikut prosedur yang ditetapkan; dan j. Menguji, menyelenggara dan mengemaskini pelan keselamatan ICT sekurang-kurangnya setahun sekali.	CIO dan Pasukan Pemulihan Bencana

Pelan Keselamatan Maklumat Perkhidmatan perlu dibangunkan dan hendaklah mengandungi perkara berikut: a. Senarai keperluan keselamatan maklumat dalam membangunkan kesinambungan perkhidmatan b. Senarai aktiviti teras dan aset yang dianggap kritikal mengikut susunan keutamaan; c. Senarai personel KSM dan pembekal berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai personel gantian juga hendaklah dikenalpasti bagi menggantikan personel yang tidak dapat hadir untuk menangani insiden; d. Senarai lengkap maklumat yang perlu disalin pendua (*backup*) dan lokasi sebenar penyimpanannya; e. Menetapkan arahan pemulihan maklumat dan kemudahan yang berkaitan; f. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah terancam; g. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan penyambungan semula perkhidmatan mengikut keutamaan; dan h. Menguji tahap keselamatan kesinambungan perkhidmatan Salinan pelan kesinambungan perkhidmatan perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. Pelan hendaklah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi organisasi untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. KSM hendaklah memastikan salinan pelan sentiasa dikemas kini dan dilindungi seperti di lokasi utama.	
130103 Mengkaji, Mengesah dan Menilai Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	
KSM hendaklah mengkaji, mengesah dan menilai tahap keselamatan maklumat yang diwujudkan dan disimpan di lokasi kesinambungan perkhidmatan keselamatan. (A.17.1.3 *Verify, review and evaluate information security continuity*)	CIO, Pasukan Pemulihan Bencana dan ICTSO

1302 *Redundancy*	
130201 Ketersediaan Kemudahan Pemprosesan Maklumat	
Kemudahan pemprosesan maklumat KSM perlu mempunyai *redundancy* yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan *redundancy* perlu diuji (*failover test*) keberkesanannya dari masa ke semasa. (A.17.2.1 *Availability of information process facilities*)	ICTSO dan BPM

BIDANG 14 **PEMATUHAN**	
1401 Pematuhan Terhadap Keperluan Perundangan dan Perjanjian Kontrak	
Objektif: Meningkat dan memantapkan tahap keselamatan ICT bagi mengelak dari pelanggaran mana-mana undang-undang, kewajipan berkanun, peraturan atau kontrak yang berkaitan dengan keselamatan maklumat.	
140101 Mengenalpasti Undang-Undang dan Perjanjian Kontrak	
Semua keperluan undang-undang berkanun, peraturan dan kontrak yang berkaitan dengan KSM perlu ditakrifkan, didokumenkan, dan disimpan sehingga tarikh yang sesuai bagi setiap sistem maklumat. (A.18.1.1 *Identification of applicable legislation and contractual agreement*) Senarai perundangan dan peraturan yang perlu dipatuhi oleh semua warga di KSM adalah seperti di Lampiran 4 dan termasuk Akta dan Peraturan-peraturan lain yang tergunapakai antaranya sepeeti berikut: i. *Emergency (Essential Power) Act 1964;* ii. *Essential (Key Points) Regulations 1965;* iii. Perakuan Jawatankuasa Mengkaji Semula Peraturan Keselamatan Pejabat Tahun 1982; iv. Arahan Keselamatan Yang Dikuat kuasakan Melalui Surat Pekeliling Am Sulit Bil. 1 Tahun 1985; v. Arahan Jawatankuasa Tetap Sasaran Penting Bil. 1 Tahun 1985; vi. Arahan Tetap Sasaran Penting Yang Dikeluarkan Kepada Pihak Yang Terlibat Dalam Pengurusan Sasaran Penting Milik Kerajaan Dan Swasta Yang Diluluskan Oleh Jemaah Menteri Pada 13 Oktober 1993; dan vii. Surat Pekeliling Am Sulit Bil. 1 Tahun 1993 - Meningkatkan Kualiti Kawalan Keselamatan Perlindungan Di Jabatan-Jabatan Kerajaan. **Keselamatan Dokumen** i. *Confidential General Circular Memorandum No.1 of 1959 (Code Words-Allocation & Control);* ii. Akta Rahsia Rasmi 1972; iii. Akta Arkib Negara 2003;	Semua Pengguna

iv. Surat Pekeliling Bil. 8 Tahun 1990 - Arahan Keselamatan Kawalan, Penyelenggaraan, Maklumat-Maklumat Ukur Dan Geografi Yang Antara Lainnya Merangkumi Peta-Peta Rasmi Dan Penderiaan Jauh;

v. Surat Pekeliling Am Sulit Bil. 1 Tahun 1972 - Keselamatan Rahsia-Rahsia Kerajaan Daripada Ancaman Penyuluhan (*espionage*);

vi. Surat Pekeliling Am Bil. 2 Tahun 1987 - Peraturan Pengurusan Rahsia Rasmi Selaras Dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1976;
Peraturan Pengurusan Rahsia Rasmi Selaras dengan Peruntukan-Peruntukan Akta Rahsia Rasmi (Pindaan) 1986 Dan Surat Pekeliling Am Bil. 2 Tahun 1987 Yang Ditandatangani Oleh Ketua Pengarah Negara Melalui Surat M(R)10308/3/(45) Bertarikh 8 Mei 1987; dan

vii. Kawalan Keselamatan Rahsia Rasmi Dan Dokumen Rasmi Kerajaan Yang Dikelilingkan melalui Surat KPKK(R) 200/ 55 Klt.7 (21) Bertarikh 21 Ogos 1999.

Keselamatan Fizikal Bangunan

i. Akta Kawasan Larangan Dan Tempat Larangan Tahun 1959;

ii. Arahan Pembinaan Bangunan Berdekatan Dengan Sasaran Penting, Kawasan Larangan Dan Tempat Larangan;

iii. *State Key Points;*

iv. Surat Pekeliling Am Rahsia Bil.1 Tahun 1975 - Keselamatan Jabatan-jabatan Kerajaan;

vi. Surat Pekeliling Am Bil 4 Tahun 1982 - Permohonan Ruang Pejabat Sama Ada Dalam Bangunan Guna sama Atau pun Disewa Di Bangunan Swasta; dan

vii. Surat Pekeliling Am Bil. 14 Tahun 1982 – Pelaksanaan Pelan Pejabat Terbuka.

Keselamatan Individu

i. *Government Security Officer: Terms of Reference – Extract On Training Of Departmental Security Office Confidential;*
ii. *General Circular Memorandum;*
iii. *Instruction On Positive Vetting Procedure;*
iv. Surat Pekeliling Am Sulit Bil.1/1966 – Perkara Keselamatan Tentang Persidangan-Persidangan/ Perjumpaan/Lawatan Sambil Belajar Antarabangsa;
v. Surat Pekeliling Tahun 1966 – Tapisan Keselamatan Terhadap Pakar/Penasihat Luar Negeri;
vi. Surat Pekeliling Am Sulit Bil.1/1967 – Ceramah Keselamatan bagi Pegawai-Pegawai Kerajaan dan mereka-mereka yang Bukan Pegawai-Pegawai Kerajaan yang bersama dalam Perwakilan Rasmi Malaysia semasa melawat Negara-negara Tabir Buluh dan Tabir besi;
vii. Surat Pekeliling Am Sulit Bil. 2 Tahun 1977 - Melaporkan Perjumpaan/ Percakapan Di Antara Diplomat/ Orang-Orang Perseorangan Dari Negeri-Negeri Asing Dengan Anggota-Anggota Kerajaan; dan
viii. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 Garis Panduan mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan.

Keselamatan Aset ICT

i. Akta Tandatangan Digital 1997;
Akta Jenayah PC 1997;
ii. Akta Hak Cipta (Pindaan) 1997;
iii. Akta Multimedia dan Telekomunikasi 1998;
iv. Surat Pekeliling Am Bil. 1 Tahun 1993 - Peraturan Penggunaan Mesin Faksimile di Pejabat-Pejabat Kerajaan;
v. Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat & Komunikasi (ICT);

vi. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan mengenai Tatacara Penggunaan Internet & Mel Elektronik di Agensi - Agensi Kerajaan; *vii.* *Malaysian Public Sector Management of Information & Communication Technology Security Handbook (MyMIS) 2002;* dan *viii.* Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Melaksanakan Penilaian Risiko Keselamatan Maklumat Sektor Awam bertarikh 7 November 2005. *ix.* Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam. *x.* Akta dan Peraturan-peraturan lain yang berkaitan.	
140102 Hak Harta Intelek (*Intellectual Property Rights*-IPR)	
KSM akan mengiktiraf dan menghormati hak-hak harta intelek yang berkaitan dengan sistem maklumat. KSM mesti mematuhi: - (A.18.1.2 *Intellectual property rights* (IPR)) a. Keperluan hakcipta yang berkaitan dengan bahan proprietari, perisian, dan rekabentuk yang diperolehi daripada KSM. b. Keperluan perlesenan menghadkan penggunaan produk, perisian, rekabentuk dan bahan-bahan lain yang diperolehi oleh KSM. c. KSM perlu memastikan pematuhan berterusan dengan sekatan hakcipta produk dan keperluan perlesenan. d. Pengguna tidak dibenarkan daripada menggunakan kemudahan pemprosesan maklumat bagi tujuan yang tidak dibenarkan.	Semua Pengguna
140103 Perlindungan Rekod	
Rekod-rekod yang penting (fizikal atau media) hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, pelepasan yang tidak dibenarkan mengikut undang-undang, peraturan, kontrak, dan keperluan perniagaan. Perkara yang perlu ditimbangkan ialah: (A.18.1.3 *Protection of records*) a. Pengekalan, penyimpanan, pengendalian dan pelupusan rekod dan maklumat b. Jadual penyimpanan rekod perlu dikenal pasti c. Inventori rekod	Semua Pengguna

140104 Privasi dan perlindungan maklumat peribadi	
KSM perlu mengenal pasti privasi dan melindungan maklumat peribadi penguna dijamin seperti yang ditakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkenaan. (A.18.1.4 *Privacy and protection of personally identifiable information*)	Semua Pengguna
140105 Kawalan Kriptografi	
Kawalan kriptografi hendaklah digunakan dengan mematuhi semua perjanjian, undang-undang, dan peraturan-peraturan. Perkara yang perlu dipatuhi adalah seperti berikut: (A.18.1.5 *Regulation of cryptographic controls*) a. Sekatan ke atas pengimport/pengeksport perkakasan dan perisian komputer yang melaksanakan fungsi-fungsi kriptografi b. Sekatan ke atas pengimport/pengeksport perkakasan dan perisian yang ditambah direka untuk mempunyai fungsi kriptografi c. Sekatan ke atas penggunaan enkripsi d. Kaedah akses oleh pihak berkuasa Malaysia bagi maklumat enkripsi perkakasan dan perisian.	Semua Pengguna
1402 Kajian Keselamatan Maklumat	
140201 Kajian Bebas/Pihak Ketiga Terhadap Keselamatan Maklumat	
Perlaksanan keselamatan maklumat KSM hendaklah dikaji secara bebas atau oleh pihak ketiga pada jangka masa yang dirancang atau apabila perubahan ketara berlaku dalam perlaksanaannya. (A.18.2.1 *Independent review of information security*)	CIO dan JKP ISMS
140202 Pematuhan Dasar dan Standard/Piawaian	
KSM hendaklah membuat kajian semula pematuhan dan prosedur pemprosesan maklumat di dalam kawasan tanggungjawab mereka dengan dasar keselamatan KSM dan piawaian yang berkenaan. Kajian teknikal perlu dilakukan setahun sekali. Sekiranya kajian semula mengenal pasti ketidakpatuhan, KSM perlu; (A.18.2.2 *Compliance with security policies and standards*) a. Mengenal pasti punca-punca ketidakpatuhan b. Menilai keperluan tindakan untuk mencapai pematuhan c. Melaksanakan tindakan pembetulan yang sewajarnya d. Mengkaji semula tindakan pembetulan yang diambil untuk mengesahkan keberkesanannya dan mengenal pasti apa-apa kekurangan dan kelemahan	CIO dan JKP ISMS

140203 Pematuhan Kajian Teknikal	
Sistem maklumat hendaklah dikaji supaya selaras dengan pematuhan dasar dan standard keselamatan maklumat organisasi (eg Kajian *Security Posture Assessment* – SPA). Kajian teknikal perlu dilakukan setahun sekali atau mengikut kesesuaian. (A.18.2.3 *Technical compliance review*)	Pentadbir ICT, Pengurus ICT dan ICTSO

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM, *thumb drive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage*), penipuan (*hoaxes*).
GCERT	*Government Computer Emergency Response Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.

GLOSARI	
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab 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.
HR	Pengurusan Sumber Manusia
ICT	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna boleh membuat capaian maklumat daripada pelayan *(server)* atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat *host* atau rangkaian.

Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan atau *malicious code*. Contohnya: *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.

GLOSARI	
LAN	*Local Area Network* Rangkaian Kawasan Setempat yang menghubungkan komputer.
Logout	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, *trojan horse, worm, spyware* dan sebagainya.
MODEM	MOdulator DEModulator Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreadsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen Saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Sistem informasi	Sistem informasi termasuk sistem operasi, infrastruktur, *business applications*, *off-the-shelf products*, perkhidmatan dan aplikasi yang dibangunkan.

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

Lampiran 1
KSM-BPM-ISMS-P4-030

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT KSM

Nama :……

Jawatan :……

Jabatan / Bahagian :……

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya berjanji bahawa saya akan mematuhi peruntukan Dasar Keselamatan ICT Pejabat Ketua Setiausaha Persekutuan Malaysia serta apa-apa peraturan dan arahan lain yang berkaitan dikeluarkan dan dikuatkuasakan dari masa ke semasa selanjutnya tempoh perkhidmatan saya.

2. Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub di dalam Dasar Keselamatan ICT Jabatan; dan

3. Jika saya ingkar kepada peruntukan–peruntukan yang ditetapkan dan disabitkan kerana melanggar Dasar Keselamatan ICT Jabatan, maka tindakan tatatertib boleh diambil ke atas diri saya mengikut Peraturan-Peraturan Pegawai Awam (Kelakuan dan Tatatertib 1993).

……..
(Tanda Tangan Pegawai / Kakitangan)
Tarikh: ……

Disahkan Oleh:
Pegawai Keselamatan ICT (ICTSO)
……
( )
Tarikh: ……..

Diperakukan Oleh :
Ketua Pegawai Maklumat (CIO)
……
( )
Tarikh: ……..

Lampiran 2

KSM-BPM-ISMS-P4-031

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT KSM

Nama :.....

Jawatan :.....

Syarikat :.....

Adalah saya _____, nombor kad pengenalan _____ yang mewakili Syarikat _____,No Pendaftaran _____ dengan ini mengaku bahawa perhatian saya telah ditarik kepada Dasar Keselamatan ICT Kementerian Sumber Manusia dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam dasar tersebut.

Saya juga berjanji akan melaksanakan tanggungjawab saya sebagaimana yang telah termaktub di dalam Dasar Keselamatan ICT; dan

Sekiranya saya atau mana-mana individu yang mewakili syarikat ini didapati melanggar dasar yang telah ditetapkan, maka saya sebagai wakil syarikat bersetuju tindakan undang-undang boleh diambil ke atas sesiapa yang terlibat mengikut peruntukan-peruntukan undang-undang sedia ada yang sedang berkuatkuasa.

.....

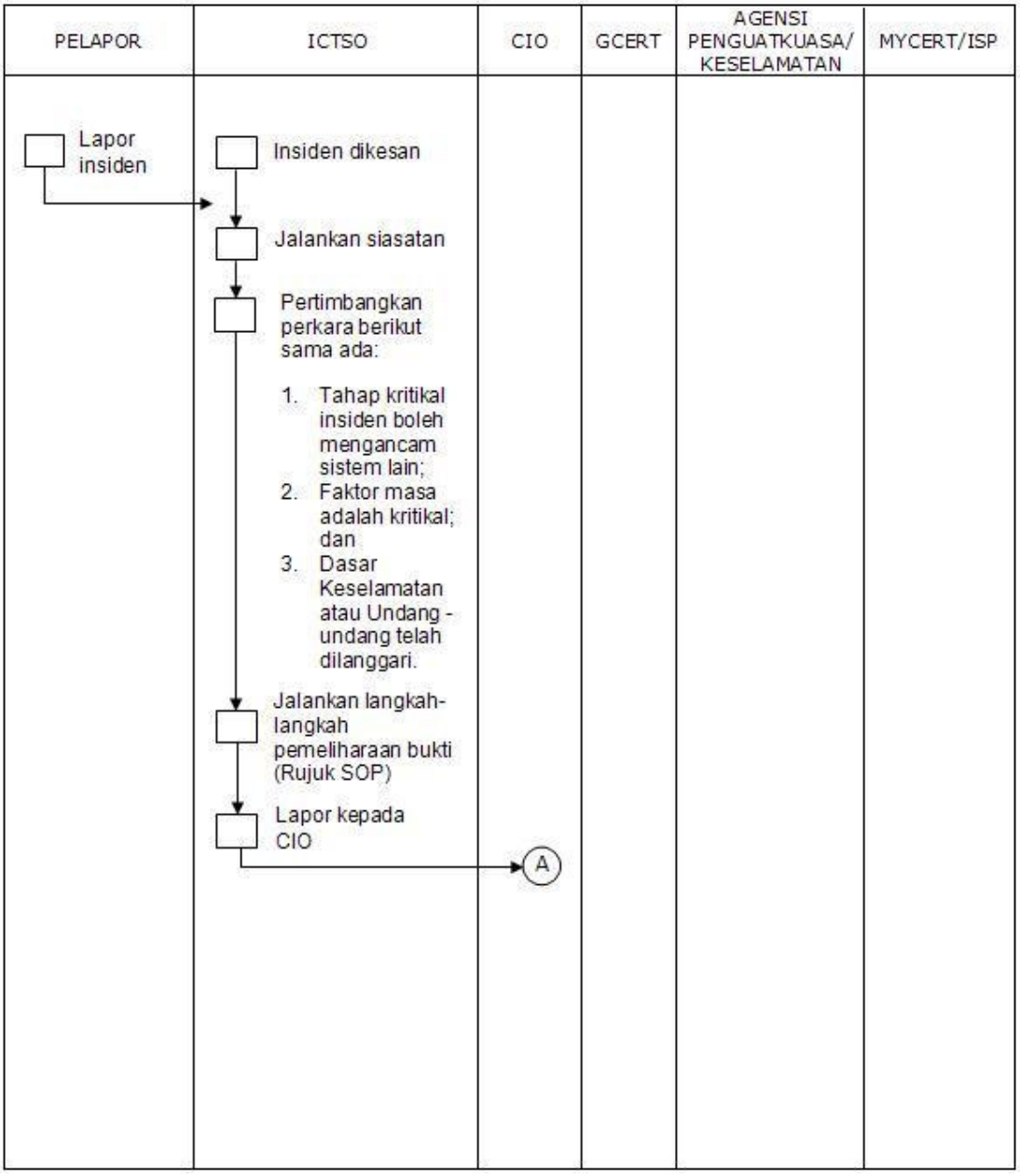
(Tanda Tangan)

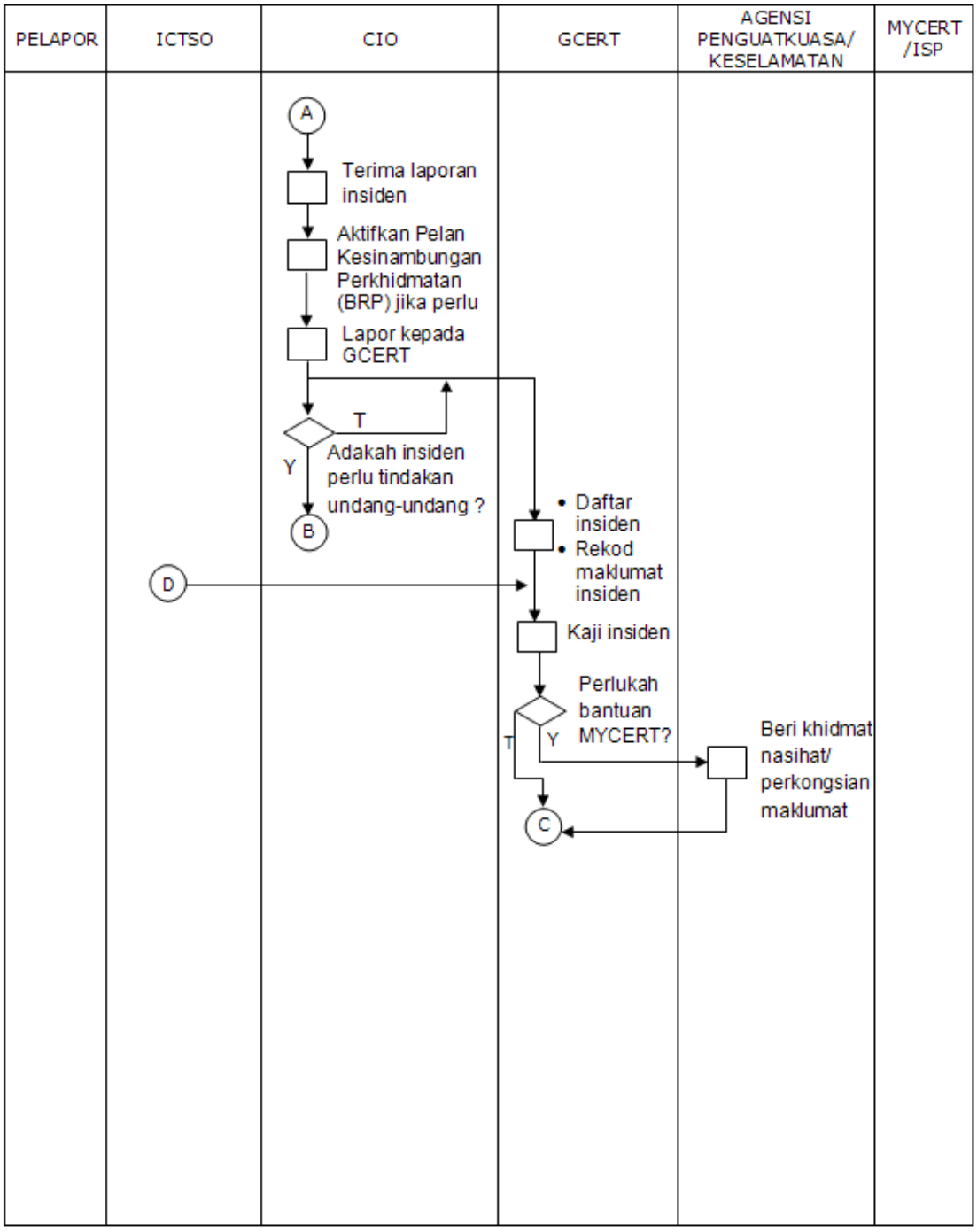
Tarikh: .....

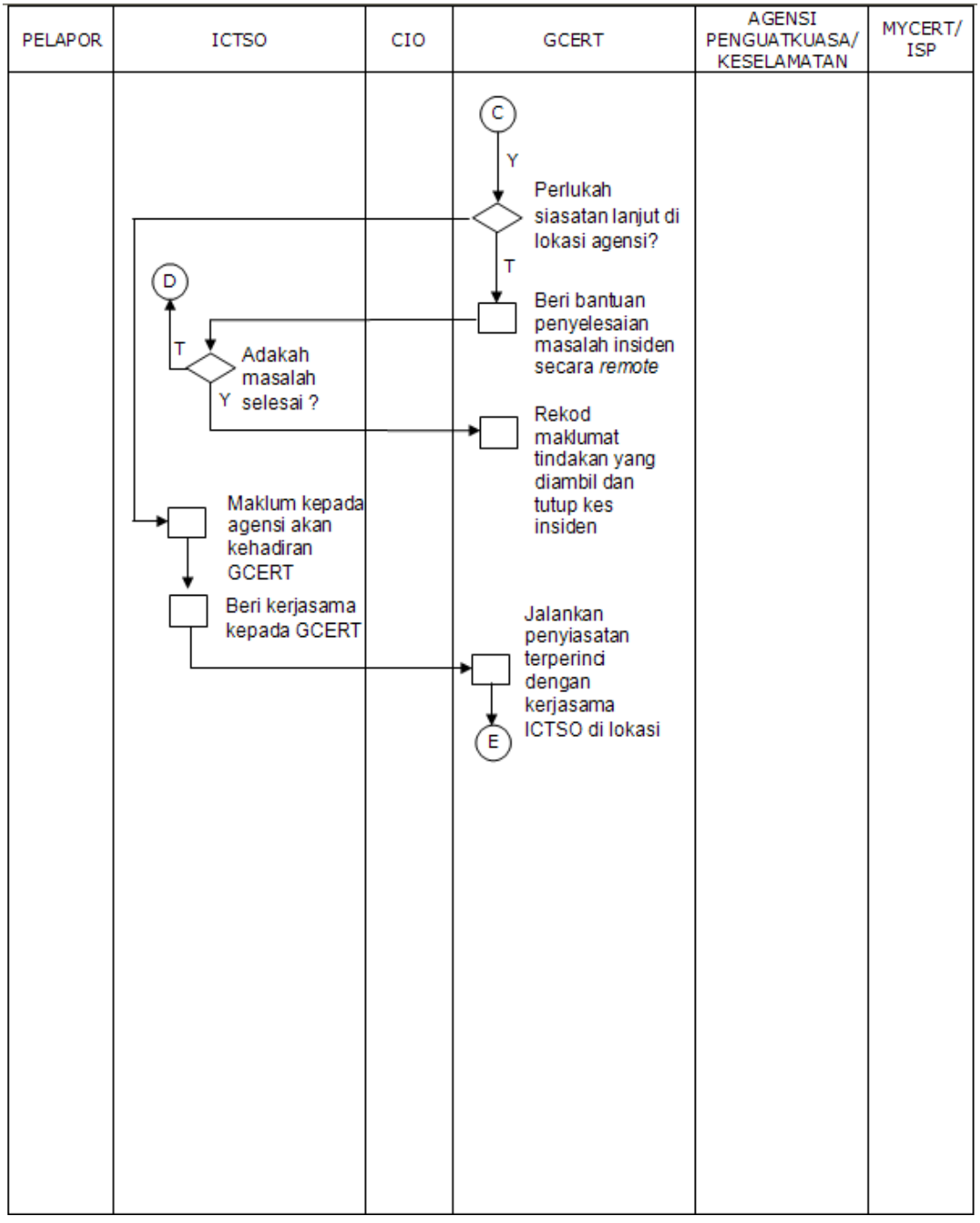
Disahkan Oleh:	**Diperakukan Oleh :**
Pegawai Keselamatan ICT (ICTSO)	**Ketua Pegawai Maklumat (CIO)**
.....	.....
( )	( )
Tarikh:	Tarikh: .....

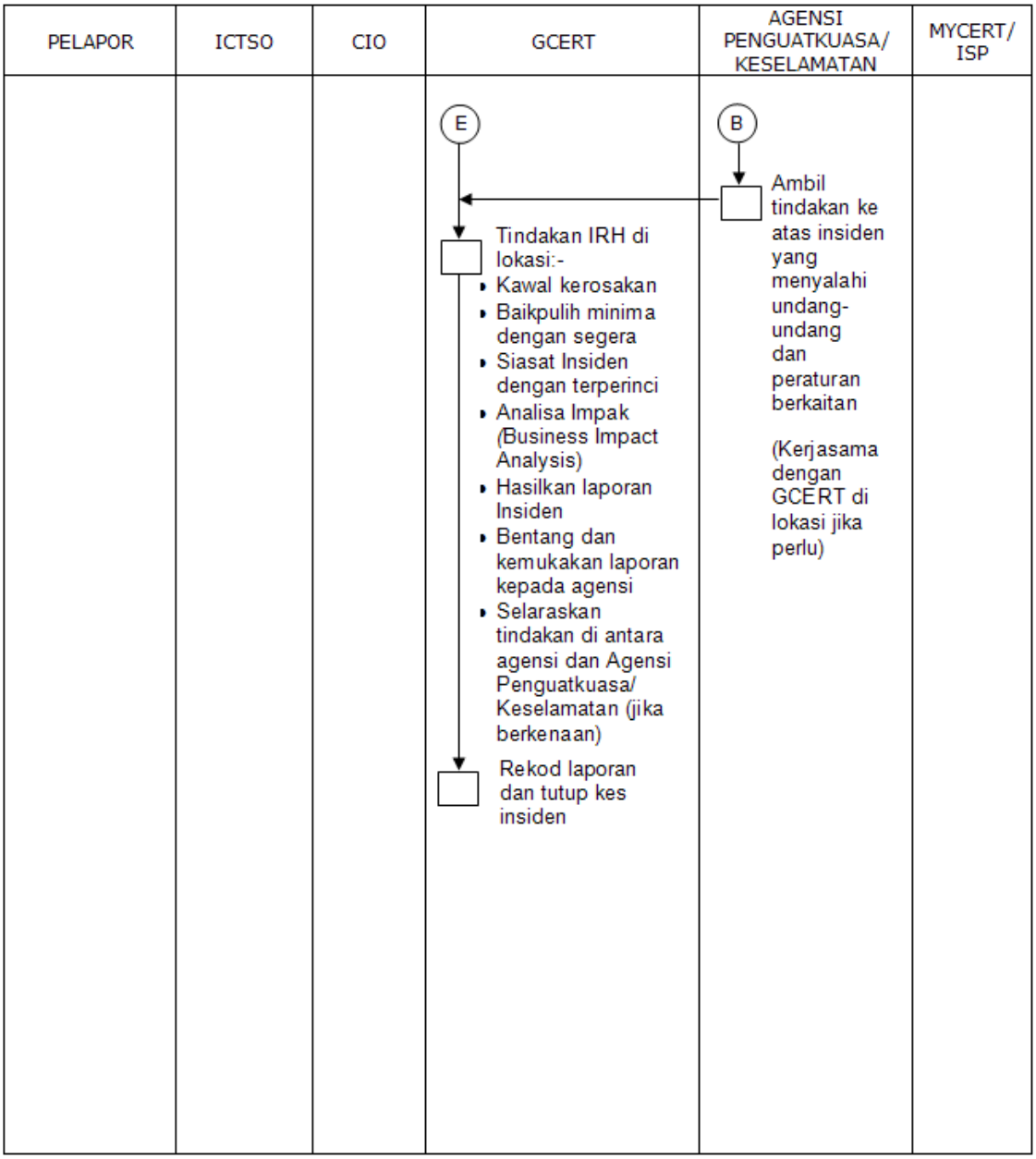
Lampiran 3

Rajah 1: Ringkasan Proses Kerja Pelaporan Insiden Keselamatan ICT PKPMP




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 selesai ?
Y
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



Petunjuk :
SOP - Standard *Operating Procedure*

Lampiran 4

SENARAI PERUNDANGAN DAN PERATURAN

1. Surat Arahan Ketua SetiausahaTahun 2010 Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di KSM;
2. Arahan Keselamatan;
3. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi
    a. Maklumat dan Komunikasi Kerajaan;
4. *Malaysian Public Sector Management of Information and Communications*
    a. *Technology Security Handbook* (MyMIS) 2002;
5. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden
    a. Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
6. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 - Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan;
7. Surat Pekeliling Am Bilangan 6 Tahun 2005 - Garis Panduan Penilaian Risiko
    a. Keselamatan Maklumat Sektor Awam;
8. Surat Pekeliling Am Bilangan 4 Tahun 2006 - Pengurusan Pengendalian Insiden
    a. Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam;

22. 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;
23. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007;
24. Surat Arahan Ketua Pengarah MAMPU - Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007;
25. Surat Pekeliling Am Bil. 2 Tahun 2000 - Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK);
26. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) – Tatacara Penyediaan, Penilaian dan Penerimaan Tender;
27. Surat Pekeliling Perbendaharaan Bil. 3/1995 - Peraturan Perolehan Perkhidmatan Perundingan;
28. Akta Tandatangan Digital 1997 (Akta 562);
29. Akta Rahsia Rasmi 1972 (Akta 88) ;
30. Akta Jenayah Komputer 1997 (Akta 563);
31. Akta Hak Cipta Tahun 1987 (Akta 331);
32. Akta Komunikasi dan Multimedia 1998 (Akta 588);
33. Perintah-Perintah Am;
34. Arahan Perbendaharaan;
35. Arahan Teknologi Maklumat 2007;
36. Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009;
37. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010;
38. Akta-akta/ Kaedah/ Pekeliling/ Arahan lain yang berkaitan.