DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA (KKMM)

Versi 1.0

20 SEPTEMBER 2013

SEJARAH DOKUMEN

DOKUMEN	VERSI	TARIKH KUATKUASA
Dasar Keselamatan ICT Kementerian Penerangan Malaysia (MOI)	2.0	30 Mac 2002
Dasar Keselamatan ICT Kementerian Penerangan Komunikasi dan Kebudayaan (KPKK)	1.0	09 April 2009
Dasar Keselamatan ICT Kementerian Komunikasi dan Multimedia Malaysia (KKMM)	1.0	20 September 2013

KANDUNGAN

PENGENALAN

Dasar Keselamatan ICT KKMM (DKICT KKMM) merangkumi Dasar Keselamatan Kementerian Komunikasi dan Multimedia Malaysia serta semua Jabatan/Agensi di bawahnya. Dasar ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi sebelum, semasa dan selepas menggunakan aset Teknologi Maklumat dan Komunikasi (ICT) Kementerian Komunikasi dan Multimedia (KKMM). Dasar ini juga menerangkan kepada semua pengguna di KKMM mengenai tanggungjawab dan peranan dalam melindungi aset ICT KKMM.

OBJEKTIF

DKICT KKMM diwujudkan untuk menjamin kesinambungan urusan pengoperasian dan pengurusan ICT KKMM dengan meminimumkan kesan insiden keselamatan ICT KKMM.

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat yang bersesuaian dengan keperluan operasi KKMM dengan memastikan semua aset ICT yang terlibat diberikan perlindungan yang sewajarnya.

Objektif utama DKICT KKMM ialah seperti berikut :

a. Memastikan kelancaran pengoperasian dan pengurusan ICT KKMM dengan meminimumkan kerosakan atau kemusnahan;

b. Melindungi kepentingan pihak-pihak yang bergantung kepada operasi ICT KKMM dari kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

c. Mencegah salah guna atau kecurian aset ICT Kerajaan.

PERNYATAAN DASAR

Keselamatan ditakrifkan sebagai keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima. Penjagaan keselamatan adalah suatu proses yang berterusan. Ia melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan di mana segala urusan menyedia dan membekalkan perkhidmatan yang berasaskan kepada sistem ICT berjalan secara berterusan tanpa gangguan yang boleh menjejaskan keselamatan. Keselamatan ICT berkait rapat dengan perlindungan aset ICT. Terdapat empat (4) komponen asas keselamatan ICT iaitu :

a. Melindungi maklumat rahsia rasmi dan maklumat rasmi Kerajaan dari capaian tanpa kuasa yang sah;

b. Menjamin setiap maklumat adalah tepat dan sempurna;

c. Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna; dan

d. Memastikan akses kepada hanya pengguna-pengguna yang sah atau penerimaan maklumat dari sumber yang sah.

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

a. **Kerahsiaan** — Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

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

c. **Tidak Boleh Disangkal** — Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal;

d. **Kesahihan** — Data dan maklumat hendaklah dijamin kesahihannya; dan

e. **Ketersediaan** — Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

SKOP

Aset ICT KKMM terdiri daripada manusia, perkakasan, perisian, telekomunikasi, kemudahan ICT dan data. DKICT KKMM menetapkan keperluan-keperluan asas berikut :

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

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

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

a. Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan KKMM dan Jabatan/Agensi. Contoh: komputer, pelayan, peralatan komunikasi dan sebagainya;

b. Perisian

Program, prosedur atau peraturan yang ditulis dan dokumentasi yang berkaitan dengan sistem pengoperasian komputer yang disimpan di dalam sistem ICT. Contoh perisian aplikasi atau perisian sistem seperti sistem pengoperasian, sistem pangkalan data, perisian sistem rangkaian, atau aplikasi pejabat yang menyediakan kemudahan pemprosesan maklumat kepada KKMM dan Jabatan/Agensi;

c. Perkhidmatan

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

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

ii. Sistem halangan akses seperti sistem kad akses; dan

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

d. Data atau Maklumat

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

e. Manusia

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

f. Premis Komputer dan Komunikasi

Semua kemudahan dan premis yang digunakan untuk menempatkan **Perkara (a) hinga (e)** yang tersebut di atas.

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

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT KKMM dan perlu dipatuhi adalah seperti berikut :

a. Akses atas dasar perlu mengetahui

Akses terhadap penggunaan aset ICT KKMM 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;

b. Hak akses minimum

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

c. Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna termasuklah :

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;

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

iii. Menentukan maklumat sedia untuk digunakan;

iv. Menjaga kerahsiaan kata laluan;

v. Mematuhi piawaian, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

vi. Memberi perhatian kepada maklumat terperingkat dan rahsia rasmi terutamanya 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, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT KKMM daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian serta memisahkan persekitaran pembangunan (*development*) dan persekitaran pelaksanaan (*production*);

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 dan dikonfigurasi supaya dapat menjana dan menyimpan log tindakan keselamatan atau jejak audit yang bersesuaian;

f. Pematuhan

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

g. Pemulihan

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

h. Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

KKMM dan Jabatan/Agensi hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan kelemahan yang semakin meningkat pada masa ini. Sehubungan itu, KKMM perlu mengambil tindakan dan langkah proaktif, munasabah 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.

KKMM dan Jabatan/Agensi hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat KKMM dan Jabatan/Agensi termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber teknologi maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem sokongan yang lain.

KKMM dan Jabatan/Agensi bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan Surat Pekeliling Am Bilangan 6 Tahun 2005 : Garis Panduan Penilaian Risiko Keselamatan ICT Keselamatan Maklumat Sektor Awam.

KKMM dan Jabatan/Agensi 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 KKMM dan Jabatan/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 pada pihak lain seperti pembekal, pakar runding dan pihak-pihak lain yang berkepentingan.

PERKARA 01 – PEMBANGUNAN DAN PENYELENGGARAAN DASAR

Objektif	
Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan KKMM dan Jabatan/Agensi serta perundangan yang berkaitan.	
KENYATAAN	**TINDAKAN**
0101 Dasar Keselamatan ICT	
010101 Pelaksanaan Dasar	
Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha (KSU) dibantu oleh Jawatankuasa CIO dan ICTSO yang dipengerusikan oleh Ketua Pegawai Maklumat (CIO) dengan keahlian terdiri daripada Pengurus ICT, Pegawai Keselamatan ICT (ICTSO) dan Setiausaha /Pengarah/Ketua Bahagian serta semua CIO, Pengurus ICT dan ICTSO Jabatan/Agensi di bawahnya.	KSU
010102 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna KKMM merangkumi semua warga KKMM, pembekal, pakar runding dan lain-lain yang bertugas dan/atau berurusan dengan KKMM dan semua Jabatan/Agensi di bawahnya.	Semua ICTSO
010103 Penyelenggaraan Dasar	
DKICT KKMM adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan DKICT KKMM : a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemukakan cadangan pindaan secara bertulis kepada Jawatankuasa CIO dan ICTSO KKMM untuk pembentangan dan persetujuan Jawatan Kuasa Pemandu ICT (JPICT) yang di pengerusikan oleh KSU; c. Perubahan yang telah dipersetujui oleh JPICT mestilah dimaklumkan kepada semua pengguna; dan d. Dasar ini hendaklah dikaji semula sekurang-kurangnya sekali setahun atau mengikut keperluan semasa.	Semua ICTSO
010104 Pemakaian Dasar	
DKICT KKMM adalah terpakai kepada semua pengguna ICT KKMM dan tiada pengecualian diberikan.	Semua Pengguna

PERKARA 02 – ORGANISASI KESELAMATAN

Objektif	
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT KKMM.	
KENYATAAN	**TINDAKAN**
0201 Infrastruktur Organisasi Keselamatan	
020101 Ketua Setiausaha	
Peranan dan tanggungjawab KSU adalah seperti berikut : a. Membaca, memahami dan mematuhi DKICT KKMM; b. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT KKMM; c. Memastikan semua pengguna mematuhi DKICT KKMM; d. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; e. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT KKMM; f. Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), KKMM; dan g. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA. (Borang DKICT 01)(Lampiran A).	KSU
020102 Ketua Pengarah/Pengarah/Pengurus Besar	
Peranan dan tanggungjawab Ketua Pengarah/Pengarah/Pengurus Besar adalah seperti berikut : a. Membaca, memahami dan mematuhi DKICT KKMM; b. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT KKMM; c. Memastikan semua pengguna mematuhi DKICT KKMM; d. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; e. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT KKMM; f. Mempengerusikan Mesyuarat Jawatankuasa Pemandu ICT (JPICT), Jabatan/Agensi; dan	KP (Terpakai untuk Jabatan/ Agensi KKMM)

g. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA. (Borang DKICT 01)(Lampiran A).	
020103 Ketua Pegawai Maklumat (CIO)	
Ketua Pegawai Maklumat (CIO) adalah Setiausaha Bahagian Kanan Pengurusan KKMM dan semua Ketua Pengarah/Pengurus Besar Jabatan/Agensi atau Pegawai yang dilantik oleh KSU/KP Jabatan/Agensi. Peranan dan tanggung jawab CIO adalah seperti berikut : a. Membaca, memahami dan mematuhi DKICT KKMM; b. Membantu KSU dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT KKMM; c. Menentukan keperluan keselamatan ICT KKMM; d. Menyelaras dan mengurus pelan latihan dan program kesedaran keselamatan ICT seperti penyediaan DKICT KKMM serta pengurusan risiko dan pengauditan; e. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT KKMM; dan f. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA. (Borang DKICT 01)(Lampiran A).	Semua CIO
020104 Pengurus ICT	
Pengurus ICT ialah Setiausaha Bahagian Pengurusan (BPM) KKMM dan semua Pengarah Bahagian/Ketua Cawangan ICT Bahagian/Agensi. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut : a. Membaca, memahami dan mematuhi DKICT KKMM; b. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan KKMM; c. Menentukan kawalan akses semua pengguna terhadap aset ICT KKMM dengan kelulusan/sokongan Setiausaha/Pengarah/Ketua Bahagian/Cawangan/Unit; d. Memaklumkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO; e. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KKMM; dan f. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA. (Borang DKICT 01)(Lampiran A).	Semua Pengurus ICT

020105 Pegawai Keselamatan ICT (ICTSO)	
ICTSO KKMM adalah Ketua Penolong Setiausaha Bahagian Pengurusan Maklumat (BPM) KKMM dan semua Pengarah Bahagian/Ketua Cawangan ICT Bahagian/Agensi atau Pegawai yang dilantik oleh KSU/KP Jabatan/Agensi. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut : a. Membaca, memahami dan mematuhi DKICT KKMM; b. Mengurus keseluruhan program-program keselamatan ICT KKMM; c. Menguatkuasakan pelaksanaan DKICT KKMM; d. Memberi penerangan, taklimat dan pendedahan berkenaan DKICT KKMM kepada semua warga KKMM; e. Mewujudkan dan melaksanakan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT KKMM; f. Menjalankan pengurusan risiko; g. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan Bahagian dan Jabatan/Agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; h. Memberi dan menyebarkan amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; i. Melaporkan insiden keselamatan ICT kepada Pasukan Pengendali Insiden Keselamatan ICT (GCERT) MAMPU, CERT KKMM dan memaklumkannya kepada CIO; j. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; k. Melaporkan sebarang salah laku pengguna yang melanggar DKICT KKMM kepada CIO; l. Memperakui proses pengambilan tindakan tatatertib ke atas pengguna yang melanggar DKICT KKMM; m. Menyedia, melaksanakan dan menyelaras pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; n. Menyedia, melaksanakan dan menyelaras penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT KKMM; o. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan; dan	Semua ICTSO

p. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA. (Borang DKICT 01)(Lampiran A).	
020106 Pentadbir Sistem ICT	
Pentadbir Sistem ICT ialah Penolong Setiausaha (PSU) (BPM) KKMM dan semua Pegawai Teknologi Maklumat/Jurutera Jabatan/Agensi merupakan Pentadbir Sistem ICT di Jabatan/Agensi masing-masing. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut : a. Membaca, memahami dan mematuhi DKICT KKMM; b. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; c. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT KKMM; d. Memantau aktiviti capaian sistem aplikasi harian pengguna; e. Bertanggungjawab memantau setiap perkakasan ICT KKMM yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; f. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; g. Melaporkan sebarang insiden keselamatan ICT kepada ICTSO masing-masing; h. Menyimpan dan menganalisis rekod jejak audit; i. Menyediakan laporan penggunaan rangkaian dan sistem secara berkala dan mengikut keperluan; dan j. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA. (Borang DKICT 01)(Lampiran A).	Semua PTM KKMM, Pegawai yang diturunkan kuasa
020107 Pengguna	
Pengguna adalah semua warga KKMM, pembekal, pakar runding dan lain-lain yang bertugas dan/atau berurusan dengan KKMM dan Jabatan/Agensi di bawahnya. Peranan dan tanggungjawab pengguna adalah seperti berikut : a. Membaca, memahami dan mematuhi DKICT KKMM; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;	Pengguna

c. Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat terperingkat dan rahsia rasmi; d. Melaksanakan prinsip-prinsip DKICT KKMM dan menjaga kerahsiaan maklumat KKMM; e. Melaksanakan langkah-langkah perlindungan seperti berikut :- 1. Menghalang pendedahan dan ketirisan maklumat kepada pihak yang tidak dibenarkan; 2. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; 3. Menentukan maklumat sedia untuk digunakan; 4. Menjaga kerahsiaan kata laluan; 5. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; 6. Memberi perhatian kepada maklumat terperingkat dan rahsia rasmi terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan 7. Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum. f. Melaporkan segera sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO masing-masing; g. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan h. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA. (Borang DKICT 01)(Lampiran A).	
020108 Pasukan Pengendali Insiden Keselamatan ICT KKMM (CERT KKMM)	
Keanggotaan CERT KKMM adalah seperti berikut : **Pengarah CERT:** Pengurus ICT (Setiausaha BPM, KKMM) **Pengurus CERT:** Pegawai Keselamatan ICT (ICTSO, KKMM) **Ahli :** • Pengurus ICT Jabatan/Agensi; • ICTSO Jabatan/Agensi; • Wakil Pegawai Teknologi Maklumat Kementerian/Jabatan/Agensi; dan • Wakil Penolong Pegawai Teknologi Maklumat Kementerian/Jabatan/ Agensi **Urusetia** bagi CERT KKMM adalah Cawangan Rangkaian dan Keselamatan, BPM, KKMM Peranan dan tanggungjawab CERT KKMM adalah seperti berikut: a. Menerima dan mengesan aduan keselamatan ICT KKMM dan menilai tahap dan jenis insiden;	CERT KKMM

b. Merekodkan dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minimum; d. Menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai *input* atau untuk tindakan seterusnya; e. Memberi khidmat nasihat kepada semua CIO mengenai tindakan pemulihan dan pengukuhan; f. Menyebarkan makluman berkaitan pemulihan dan pengukuhan kepada semua pengguna KKMM; dan g. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
0202 Pihak Ketiga	
Objektif : Menjamin keselamatan semua aset ICT KKMM yang digunakan oleh pihak ketiga.	
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar/asing dikawal. Perkara yang perlu dipatuhi termasuk yang berikut : a. Membaca, memahami dan mematuhi DKICT KKMM; b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pengguna; d. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga dan akses kepada aset ICT KKMM perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai : i. DKICT KKMM; ii. Tapisan Keselamatan; iii. Akta Rahsia Rasmi 1972; iv. Hak Harta Intelek; dan v. Arahan Teknologi Maklumat. e. Menandatangani Perakuan Akta Rahsia Rasmi 1972; f. Menandatangani SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA. (Borang DKICT 01)(Lampiran A).	Semua CIO, Pengurus ICT, ICTSO, Pentadbir Sistem ICT dan Pihak Ketiga

PERKARA 03 – PENGURUSAN ASET

Objektif	
Memberi dan menyokong perlindungan keselamatan yang bersesuaian ke atas semua aset ICT KKMM.	
KENYATAAN	**TINDAKAN**
030101 Inventori Aset	
Semua aset ICT KKMM dan Jabatan/Agensi hendaklah direkodkan. Mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Perkara yang perlu dipatuhi adalah seperti berikut : a. Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod dalam Borang Daftar Harta Modal dan Inventori atau Sistem Pengurusan Aset dan sentiasa dikemaskini; b. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna yang dibenarkan sahaja; c. Memastikan semua pengguna mengesahkan penempatan aset ICT yang ditempatkan di KKMM dan Jabatan/Agensi; dan d. Peraturan, prosedur dan tatacara bagi pengendalian dan pengurusan aset ICT hendaklah dikenal pasti, didokumenkan dan dilaksanakan.	Pentadbir Sistem ICT dan Pegawai Aset
Setiap pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah jagaan dan kawalannya.	Semua Pengguna
0302 Pengelasan dan Pengendalian Maklumat	
Objektif : Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
030201 Pengelasan Maklumat	
Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya mengikut dokumen Arahan Keselamatan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut : a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	Pegawai yang diberi kuasa
Setiap pengguna adalah bertanggung jawab mengurus maklumat bersesuaian dengan peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan.	Semua Pengguna

030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnahkan hendaklah mengambil kira langkah-langkah keselamatan berikut : a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. Menentukan maklumat sedia untuk digunakan; d. Menjaga kerahsiaan kata laluan; e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan; f. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan langkah-langkah keselamatan ICT KKMM dari diketahui umum.	Semua Pengguna

PERKARA 04 – KESELAMATAN SUMBER MANUSIA

Objektif	
Memastikan semua sumber manusia yang terlibat termasuk warga KKMM dan Jabatan/Agensi, kontraktor, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT KKMM.	
KENYATAAN	**TINDAKAN**
0401 Keselamatan ICT Dalam Tugas Harian	
040101 Tanggungjawab Keselamatan	
Peranan dan tanggungjawab pengguna terhadap keselamatan ICT KKMM dan Jabatan/Agensi mestilah lengkap, jelas, direkodkan, dipatuhi dan dilaksanakan serta dinyatakan di dalam fail meja atau kontrak. Keselamatan ICT KKMM merangkumi tanggungjawab pengguna dalam menyediakan dan memastikan perlindungan ke atas semua aset atau sumber ICT KKMM dan Jabatan/Agensi yang digunakan di dalam melaksanakan tugas harian.	Semua Pengguna
040102 Terma dan Syarat Perkhidmatan	
Semua pengguna yang dilantik oleh Kerajaan (KKMM dan Jabatan/Agensi) hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa.	Semua Pengguna KKMM yang dilantik
040103 Perakuan Akta Rahsia Rasmi	
Semua pengguna yang menguruskan maklumat terperingkat dan rahsia rasmi hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972 dan Arahan Kesematan yang ditetapkan oleh Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia (CGSO).	Semua Pengguna
040104 Sebelum Berkhidmat	
Semua pengguna mestilah memahami tanggungjawab masing-masing ke atas keselamatan aset ICT KKMM dan Jabatan/Agensi bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi adalah seperti berikut : a. Peranan dan tanggungjawab penjawat awam, kontraktor, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dengan aset ICT Kerajaan perlu dinyatakan dengan jelas dan terperinci sebelum, semasa dan selepas perkhidmatan; dan b. Penyaringan, tapisan keselamatan dan/atau pengesahan latar belakang calon untuk penjawat awam, kontraktor, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan hendaklah dilakukan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan.	Semua Pengguna

040105 Dalam Perkhidmatan	
Semua pengguna hendaklah faham dan sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing untuk menyokong DKICT KKMM dan meminimumkan risiko kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT. Perkara yang perlu dipatuhi adalah seperti berikut : a. Memastikan semua pengguna menguruskan keselamatan berdasarkan perundangan dan peraturan yang ditetapkan oleh KKMM dan Jabatan/Agensi; b. Memastikan latihan kesedaran yang berkaitan mengenai pengurusan keselamatan ICT KKMM dan Jabatan/Agensi diberi kepada semua pengguna dan sekiranya perlu diberikan kepada kontraktor, pembekal, pakar runding dan pihak-pihak lain yang berkepentingan dari semasa ke semasa; c. Memastikan adanya proses tindakan disiplin ke atas semua pengguna, sekiranya berlaku perlanggaran dengan perundangan dan peraturan ditetapkan dalam DKICT KKMM; dan d. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT KKMM. Sebarang kursus dan latihan teknikal yang diperlukan, pihak pengguna boleh merujuk kepada pihak ICT masing-masing.	Semua Pengguna Semua ICTSO Semua Pengguna
040106 Tamat Perkhidmatan Atau Bertukar	
Memastikan semua pengguna diuruskan dengan teratur apabila tamat perkhidmatan atau bertukar dari KKMM dan Jabatan/Agensi. Perkara yang perlu dipatuhi adalah seperti berikut :- a. Memastikan semua aset ICT Kerajaan dikembalikan mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan dan/atau terma perkhidmatan; dan c. Melupuskan semua maklumat terperingkat secara selamat atau memulangkan semula maklumat terperingkat kepada Kerajaan.	Semua Pengguna

PERKARA 05 – KESELAMATAN FIZIKAL DAN PERSEKITARAN

Objektif	
Melindungi pejabat dan maklumat daripada sebarang bentuk pencerobohan dan ancaman.	
KENYATAAN	**TINDAKAN**
050101 Perimeter Keselamatan Fizikal	
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan untuk menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut : a. Kawasan keselamatan fizikal hendaklah 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. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; d. Memperkukuhkan dinding dan siling; e. Memasang alat penggera atau kamera; f. Mengehadkan jalan keluar masuk; g. Mengadakan kaunter kawalan; h. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; i. Mewujudkan perkhidmatan kawalan keselamatan; j. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja dibenarkan melalui pintu masuk; k. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan; l. Mereka bentuk dan melaksanakan keselamatan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; m. Menyediakan garis panduan bagi pengguna KKMM dan Jabatan/Agensi yang bekerja di dalam kawasan terhad; dan n. Memastikan kawasan-kawasan penghantaran dan pemunggahan serta tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	Semua ICTSO, Ketua Pegawai Keselamatan yang dilantik (jika berkaitan)

050102 Kawalan Masuk Fizikal	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pengguna KKMM dan Jabatan/Agensi hendaklah memakai atau mengenakan Pas Keselamatan sepanjang waktu bertugas; b. Setiap pelawat boleh mendapat Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan hendaklah dikembalikan semula selepas tamat lawatan; c. Semua pas keselamatan hendaklah diserahkan balik kepada bahagian berkenaan apabila pengguna berhenti atau bersara; d. Setiap pelawat hendaklah mendaftar di pintu utama terlebih dahulu; e. Kehilangan Pas Keselamatan mestilah dilaporkan dengan segera; dan f. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai dan/atau menggunakan aset ICT KKMM dan Jabatan/Agensi.	Semua Pengguna dan Pelawat
050103 Kawasan Larangan	
Semua pengguna dilarang berada di Pusat Data (*Data Centre*) atau Bilik Server KKMM/Jabatan/Agensi kecuali dengan kebenaran dan/atau diiringi oleh pegawai yang diberi kuasa. Akses kepada kawasan larangan hanyalah kepada pengguna yang dibenarkan sahaja. Pusat Data tau Bilik Server KKMM/Jabatan/Agensi merupakan kawasan larangan yang dihadkan kemasukannya bagi melindungi aset ICT KKMM dan Jabatan/Agensi yang terdapat di dalam kawasan tersebut. Pengguna dilarang merakam sebarang foto atau video dikawasan ini, kecuali mendapat kelulusan bertulis ICTSO KKMM/Jabatan/Agensi terlebih dahulu.	Semua Pengguna
0502 Keselamatan Peralatan	
Objektif : Melindungi peralatan dan maklumat daripada kehilangan, kerosakan, kecurian atau salah guna yang mendatangkan gangguan.	
050201 Peralatan ICT	
Semua pengguna perlu mematuhi langkah-langkah keselamatan seperti berikut: a. Menyemak dan memastikan semua perkakasan ICT di bawah kawalannya berfungsi dengan sempurna; b. Bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; c. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan;	Semua Pengguna

d. Bertanggungjawab sepenuhnya ke atas aset ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

e. Dilarang sama sekali menambah, menanggalkan atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

f. Dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem;

g. Memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan seperti *hard disk*, disket, *thumbdrive* dan *external hard disk*;

h. Melindungi semua peralatan sokongan ICT daripada sebarang kecurian, dirosakkan, diubahsuai tanpa kebenaran dan salah guna;

i. Bertanggungjawab di atas kerosakan atau kehilangan perkakasan ICT di bawah jagaan dan/atau kawalannya;

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

k. Semua perkakasan 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;

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

m. Peralatan ICT yang hilang hendaklah dikendalikan mengikut prosedur semasa yang berkuat kuasa dan dilaporkan kepada Pegawai Aset;

n. Pengendalian Peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa;

o. Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal ianya ditempatkan tanpa kebenaran Pegawai Aset/ Pentadbir Sistem ICT;

p. Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih;

q. Sebarang pelekat selain bagi tujuan rasmi, hiasan atau contengan yang meninggalkan kesan yang lama pada perkakasan ICT tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik;

r. Konfigurasi alamat IP juga tidak dibenarkan diubah daripada alamat IP yang asal;

s. Dilarang sama sekali mengubah *password administrator* yang telah ditetapkan oleh pihak ICT;

t. Memastikan semua perkakasan komputer, pencetak dan pengimbas berkeadaan "SLEEP" apabila tidak digunakan/ditinggalkan sementara dan berkeadaan "OFF" apabila pengguna meninggalkan pejabat; u. Memastikan plag ditanggalkan dari soket pendawaian elektrik bagi mengelakkan kerosakkan perkakasan apabila meninggalkan pejabat atau sekiranya perkakasan tidak digunakan dalam tempoh yang lama; dan v. Sebarang bentuk penyelewengan atau salah guna perkakasan hendaklah dilaporkan kepada ICTSO KKMM/Jabatan/Agensi.	
050202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, *external hard disk, public cloud storage* dan media storan lain. Media-media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut: a. Semua media storan perlu dikawal bagi mencegah dari capaian yang tidak dibenarkan, kecurian dan kemusnahan; b. Semua media storan perlu dipastikan keselamatannya sebelum disambungkan kepada perkakasan ICT KKMM dan Jabatan/Agensi; c. Bagi media storan yang hendak dilupuskan, semua maklumat dalam media tersebut perlu dihapuskan secara selamat terlebih dahulu; d. Semua media storan data yang hendak dilupuskan mesti dihapuskan dengan teratur dan selamat; e. Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan dari dipecahkan, api, air dan medan magnet; f. Media storan dan peralatan *backup* hendaklah disimpan di lokasi yang berasingan yang dikategorikan selamat. Akses untuk memasuki kawasan penyimpanan media hendaklah terhad kepada pengguna yang dibenarkan sahaja; g. Akses dan pergerakan kepada media storan yang mengandungi maklumat terperingkat dan rahsia rasmi perlu direkodkan; h. Hanya maklumat terbuka sahaja boleh disimpan di dalam *public cloud storage* dan aplikasi *public cloud storage client* hendaklah diputuskan dari talian selepas digunakan; i. Perkakasan bagi penduaan hendaklah diletakkan di tempat yang terkawal; dan	Semua Pengguna

j. Mengadakan salinan atau penduaan pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data.	
050203 Media Perisian dan Aplikasi	
Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut: a. Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan di KKMM/Jabatan/Agensi; b. Sistem aplikasi dalaman tidak dibenarkan diagih/didemontrasikan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c. Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada media storan berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; d. Perisian dan Aplikasi milik Kerajaan adalah tidak dibenarkan dipasang pada peralatan milik peribadi; dan e. Kod sumber sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Semua Pengguna
050204 Media Sijil/Tandatangan Digital	
Bagi menjamin keselamatan Media Sijil/Tandatangan Digital seperti *SoftCert* dan Kad Pintar, semua pengguna perlu mengambil langkah-langkah berikut: a. Semua pengguna hendaklah bertanggungjawab sepenuhnya ke atas media sijil/tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; b. Media Sijil/Tandantangan Digital hendaklah digunakan bagi capaian sistem yang dikhususkan sahaja; b. Media ini tidak boleh dipindah milik atau dipinjamkan kepada pengguna lain; dan c. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan segera kepada pihak bertanggungjawab untuk tindakan selanjutnya.	Semua Pengguna yang terlibat
050205 Penyelenggaraan Perkakasan	
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut: a. Bertanggungjawab terhadap setiap perkakasan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;	Semua Pegawai Aset, Pentadbir Sistem ICT Kementerian/ Jabatan/Agensi

b. Semua perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; c. Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; d. Semua perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan; e. Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan mestilah mendapat kebenaran dari Pengurus ICT atau pegawai ICT yang bertanggungjawab.	
050206 Peminjaman Perkakasan Untuk Kegunaan Di Luar Pejabat	
Perkakasan yang dipinjam untuk kegunaan di luar pejabat adalah terdedah kepada pelbagai risiko. Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut: a. Mendapatkan kelulusan Pegawai Aset/ Pentadbir Sistem ICT Kementerian/Jabatan/Agensi bagi membawa keluar peralatan atau maklumat, tertakluk kepada tujuan yang dibenarkan; b. Peralatan yang digunakan di luar pejabat perlu dilindungi dan dikawal sepanjang masa; c. Pergerakakan, penyimpanan atau penempatan peralatan hendaklah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan d. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan bagi tujuan pemantauan.	Semua Pengguna
050207 Pengendalian Peralatan Luar Yang Dibawa Masuk/Keluar	
Bagi peralatan yang dibawa masuk/keluar pejabat, langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Memastikan peralatan yang dibawa masuk tidak mengancam keselamatan ICT KKMM dan Jabatan/Agensi; b. Mendapatkan kelulusan mengikut peraturan yang telah ditetapkan oleh KKMM/Jabatan/Agensinya bagi membawa masuk/keluar peralatan (Lampiran C - Borang Pengisytiharan Barang Keluar/Masuk); dan c. Memusnahkan maklumat dan memastikan peralatan yang dibawa keluar tidak mengandungi maklumat terperingkat dan rahsia rasmi Kerajaan.	Semua Pengguna

050208 Pelupusan Perkakasan	
Pelupusan melibatkan semua peralatan ICT KKMM dan Jabatan/Agensi yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori. Peralatan ICT yang hendak dilupuskan perlu melalui proses pelupusan terkini. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KKMM dan Jabatan/Agensi. Langkah-langkah seperti berikut hendaklah diambil: a. Peralatan ICT yang akan dilupuskan sebelum dipindah milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; b. Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; c. Media storan (*internal/external hard disk*) hendaklah dikeluarkan dan disimpan di tempat yang telah dikhaskan dengan ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; d. Pegawai Aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam Sistem Pengurusan Aset (SPA); e. Pelupusan peralatan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; f. Pengguna ICT adalah DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut : i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggalkan dan menyimpan komponen dalaman CPU seperti RAM, *Hard disk*, *Motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan tambahan komputer seperti UPS, speaker atau mana-mana peralatan yang berkaitan ke mana-mana lokasi lain; iii. Membawa keluar dari pejabat mana-mana peralatan ICT yang hendak dilupuskan; dan iv. Melupuskan sendiri peralatan ICT tanpa melalui prosedur pelupusan yang ditetapkan. g. Semua pengguna ICT KKMM bertanggungjawab memastikan segala maklumat termasuk maklumat terperingkat dan rahsia rasmi di dalam peralatan ICT berkaitan disalin kepada media storan kedua seperti disket, *thumbdrive* atau *external hard drive* sebelum maklumat tersebut dihapuskan daripada peralatan komputer yang hendak dilupuskan.	Semua Pegawai Aset, Pentadbir Sistem ICT Semua Pengguna

050209 Pemulangan Peralatan Sewaan	
Pemulangan Peralatan Sewaan melibatkan pemulangan semua peralatan ICT KKMM dan Jabatan/Agensi yang telah tamat tempoh sewaannya kepada pembekal. Peralatan ICT yang hendak dipulangkan perlu melalui proses pembersihan yang terkini. Pembersihan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KKMM dan Jabatan/Agensi. Langkah-langkah seperti berikut hendaklah diambil: a. Peralatan ICT yang akan dipulangkan hendaklah dipastikan bahawa data-data dalam storan dan konfigurasi yang telah ditetapkan bagi pelbagai tetapan rangkaian/aplikasi/lain-lain telah dihapuskan dengan cara yang selamat; b. Kaedah pengeluaran dan penyimpanan media storan (*internal/external hard disk*) oleh pihak KKMM dan Jabatan/Agensi hendaklah dipertimbangkan bagi menjamin keselamatan maklumat Kerajaan; c. Semua pengguna ICT KKMM bertanggungjawab memastikan segala maklumat termasuk maklumat terperingkat dan rahsia rasmi di dalam peralatan ICT berkaitan disalin kepada media storan kedua seperti disket, *thumbdrive* atau *external hard drive* sebelum maklumat tersebut dihapuskan daripada peralatan komputer yang hendak dipulangkan; dan d. Tidak melakukan sebarang kerosakan ke atas peralatan sewaan yang hendak dipulangkan.	Semua Pegawai Aset, Pentadbir Sistem ICT Semua Pengguna
0503 Keselamatan Persekitaran	
Objektif : Melindungi aset ICT KKMM dan Jabatan/Agensi dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301 Kawalan Persekitaran	
Bagi mengelakkan kerosakan terhadap premis dan aset ICT KKMM dan Jabatan/Agensi, semua cadangan berkaitan pejabat sama ada urusan perolehan, penyewaan atau pengubahsuaian hendaklah dirujuk terlebih dahulu kepada pegawai yang bertanggungjawab. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a. Merancang dan menyediakan pelan keseluruhan susun atur ruang pejabat yang menempatkan pusat data, bilik percetakan, peralatan komputer dan sebagainya dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan;	Semua Pengguna

c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dilihat dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g. Semua peralatan perlindungan hendaklah diperiksa dan diuji sekurang-kurangnya dua (2) kali dalam setahun. Aktiviti ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h. Memastikan akses kepada saluran *riser* hendaklah sentiasa dikunci.	
050302 Pendawaian	
Pendawaian komputer hendaklah dilindungi kerana boleh menjadi punca maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut : a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada sebarang kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel bagi mengelakkan sebarang ancaman; dan d. Membuat pelabelan kabel dengan jelas dan mestilah melalui laluan *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pengurus ICT dan Semua ICTSO
050303 Bekalan Kuasa	
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Langkah-langkah seperti berikut perlu diambil dalam memastikan keselamatan bekalan kuasa: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana kuasa (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data dan Bilik Server supaya mendapat bekalan kuasa berterusan; dan c. Semua peralatan sokongan bekalan kuasa hendaklah diperiksa dan diuji secara berjadual.	Pengurus ICT dan Semua ICTSO

050304 Prosedur Kecemasan	
Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut: a. Hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada 'Garis Panduan Keselamatan KPKK 2007'; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada pegawai yang berkenaan.	Semua Pengguna
0504 Keselamatan Dokumen dan Sistem Dokumentasi	
050401 Dokumen	
Bagi memastikan integriti maklumat, semua pengguna perlu mengambil langkah-langkah beriku: a. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b. Mengawal dan merekodkan aktiviti capaian dokumentasi sedia ada; c. Setiap dokumen hendaklah di fail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; d. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur Arahan Keselamatan; e. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; f. Pelupusan dokumen hendaklah mengikut prosedur keselamatan seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Arkib Negara Malaysia; dan g. Menggunakan penyulitan (*encryption*) ke atas dokumen maklumat terperingkat dan rahsia rasmi yang disediakan dan dihantar secara elektronik.	Semua Pengguna

PERKARA 06 – PENGURUSAN OPERASI DAN KOMUNIKASI

Objektif	
Memastikan pengurusan operasi dan kemudahan pemprosesan maklumat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
KENYATAAN	**TINDAKAN**
0601 Pengurusan Prosedur Operasi	
060101 Pengendalian Prosedur	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur keselamatan ICT KKMM dan Jabatan/Agensi yang di wujud, dikenal pasti dan masih diguna pakai hendaklah didokumenkan, disimpan dan dikawal; b. Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan c. Semua prosedur hendaklah disemak dan dikemas kini dari semasa ke semasa atau mengikut keperluan.	Semua ICTSO
060102 Kawalan Perubahan	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada pegawai yang berkenaan atau pemilik aset ICT terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pegawai yang berkenaan 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 disengajakan.	Semua Pengguna

060103 Pengasingan Tugas dan Tanggungjawab	
Skop tugas dan tanggung jawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahan yang tidak dibenarkan ke atas aset ICT. Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Platform yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai platform pelaksanaan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan pembangun, operasi dan rangkaian.	Semua Pengurus ICT, ICTSO
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Objektif : Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan dan penyampaian yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
060201 Perkhidmatan Penyampaian	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c. Pengurusan perubahan dasar perlu mengambilkira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risko.	Semua Pengguna
0603 Perancangan dan Penerimaan Sistem	
Objektif : Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 Perancangan Kapasiti	
Perkara yang perlu dipatuhi adalah seperti berikut: 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; 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.	Semua ICTSO dan Pentadbir Sistem ICT

060302 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Semua ICTSO dan Pentadbir Sistem ICT
0604 Perisian Berbahaya	
Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus dan trojan.	
060401 Perlindungan dari Perisian Berbahaya	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya (seperti anti -virus, anti-spyware, anti-spam, content filtering, web reputation dan *Intrusion Prevention System* - IPS) dan mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Mengimbas semua data, perisian atau sistem dengan perisian keselamatan yang bersesuaian sebelum menggunakannya; d. Mengemaskini perisian keselamatan dari semasa ke semasa; e. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian/aplikasi yang dibangunkan; dan i. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	Semua ICTSO dan Pentadbir Sistem ICT
060402 Perlindungan dari Kod Mudah Alih (*Mobile Code*)	
Penggunaan Kod Mudah Alih hendaklah dirancang, diuji dan dikawal. Pengugunaan Kod Mudah Alih yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Semua Pengguna

0605 *Housekeeping*	
Objektif : Melindungi integriti maklumat dan perkhidmatan komunikasi agar sentiasa boleh diakses pada bila-bila masa.	
060501 Penduaan	
Bagi memastikan sistem dapat dilaksanakan semula setelah berlakunya bencana, salinan penduaan hendaklah dilakukan setiap kali konfigurasi berubah. Rekod salinan penduaan hendaklah di simpan. Perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat salinan keselamatan ke atas semua konfigurasi dan tetapan serta sistem, perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat salinan penduaan ke atas semua data dan maklumat mengikut keperluan; c. Menguji sistem penduaan sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d. Penduaan hendaklah dilaksanakan secara harian, mingguan, bulanan dan tahunan. Kekerapan penduaan bergantung pada tahap kritikal maklumat; e. Menyimpan sekurang-kurangnya tiga (3) generasi data penduaan; dan f. Merekod dan menyimpan salinan penduaan di lokasi yang berlainan dan selamat selaras dengan peraturan semasa.	Semua Pentadbir Sistem ICT

0606 Pengurusan Rangkaian	
Objektif : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
060601 Kawalan Infrastruktur Rangkaian	
Infrastruktur rangkaian mestilah di kawal dan diuruskan sebaik mungkin bagi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan: a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Semua peralatan mestilah lulus proses *Factory Acceptence Test (FAC)* dan ujian piawaian yang ditetapkan oleh SIRIM atau agensi piawaian antarabangsa semasa dikeluarkan serta lulus *User Acceptance Test* (UAT) semasa pemasangan dan konfigurasi; e. *Firewall* hendaklah dipertimbangkan untuk dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta di konfigurasi secara optimum; f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan KKMM dan Jabatan/Agensi; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO Kementerian/ Jabatan/Agensi; h. Memasang dan mengkonfigurasi secara optimum *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat KKMM dan Jabatan/Agensi; i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk memantau dan/atau menyekat aktiviti yang dilarang; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan KKMM dan Jabatan/Agensi hendaklah mendapat kebenaran ICTSO; k. Semua pengguna hanya dibenarkan menggunakan rangkaian KKMM dan Jabatan/Agensi sahaja; l. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan yang bersesuaian dengannya; dan m. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum.	Semua Pentadbir Sistem ICT

0607 Pengurusan Media	
Objektif : Melindungi aset ICT KKMM dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan.	
060701 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Pentadbir Sistem Kementerian/Jabatan/ Agensi atau Pemilik terlebih dahulu.	Semua Pengguna
060702 Prosedur Pengendalian Media	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Melabelkan semua media termasuk pada antaramuka sistem mengikut tahap sensitiviti sesuatu maklumat (Terhad, Sulit, Rahsia dan Rahsia Besar); b. Mengehadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat terperingkat dan rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang ditetapkan.	Semua Pentadbir Sistem ICT
060703 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut: a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan aktiviti capaian ke atas dokumentasi.	Semua Pengguna
0608 Pengurusan Pertukaran Maklumat	
Objektif : Memastikan keselamatan pertukaran maklumat dan perisian antara KKMM/Jabatan/Agensi dan mana-mana entiti luar terjamin.	

060801 Pertukaran Maklumat	
Langkah-langkah bagi Pengurusan Pertukaran Maklumat adalah seperti berikut : a. Dasar, polisi, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara KKMM dan Jabatan/Agensi dengan pihak ketiga; c. Media yang mengandungi maklumat terperingkat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KKMM dan Jabatan/Agensi; d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	Semua Pengguna
060802 Mel Elektronik (E-mel)	
Penggunaan e-mel KKMM hendaklah dipantau secara berterusan oleh Pentadbir E-mel untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara yang perlu dipatuhi adalah seperti berikut : a. Akaun atau alamat mel elektronik (e-mel) yang diperuntukkan oleh KKMM dan Jabatan/Agensi sahaja boleh digunakan untuk kegunaan rasmi. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Penggunaan e-mel rasmi bagi tujuan peribadi adalah tidak dibenarkan; c. Setiap e-mel yang disediakan perlu mematuhi format yang telah ditetapkan oleh KKMM; d. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perbincangan yang sama, sebelum penghantaran dilakukan; e. Penghantar hendaklah memastikan alamat e-mel penerima adalah betul; f. Dokumen terperingkat yang diterima melalui e-mel hendaklah segera dipindahkan ke storan kedua dan diberikan perlindungan yang sewajarnya; g. Penggunaan fail kepilan (*attachment*) dibuat sekiranya perlu, tidak melebihi yang ditetapkan oleh Pentadbir E-mel semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;	Semua Pengguna

h. Penghantaran lampiran dalam format/*extension* "*.exe, *.bat, *.hta, *.cmd dan *.com" tidak dibenarkan; i. Mengelak dari membuka e-mel dan fail kepilan daripada penghantar yang tidak diketahui atau diragui; j. Mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel; k. Setiap e-mel rasmi yang dihantar atau diterima hendaklah disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan; l. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; m. Memastikan tarikh dan masa sistem komputer adalah tepat berdasarkan Malaysian Standard Time oleh SIRIM; n. Hanya warga KKMM/Jabatan/Agensi sahaja boleh dipertimbangkan untuk mendapat kemudahan e-mel rasmi KKMM/Jabatan/Agensi; o. Fungsi *Auto-Reply* adalah tidak dibenarkan kecuali pengguna yang bercuti atau bertugas di luar pejabat iaitu dengan menggunakan mesej *Out-of-Office*; p. Bahagian Pentadbiran dan Pengurusan Sumber Manusia KKMM/Jabatan/Agensi perlu memaklumkan sebarang status pengguna (bertukar Jabatan, bersara, diberhentikan, tidak dapat dikesan, bertukar keluar atau masuk ke KKMM/Jabatan/Agensi bagi tujuan pengemaskinian e-mel yang terlibat atau mengikut keperluan Jabatan/Agensi; dan q. Pengguna adalah mewakili dirinya sendiri dan bertanggungjawab ke atas maklumat yang dikeluarkan dalam setiap perhubungan yang dibuat secara elektronik.	

0609 Perkhidmatan E-Dagang (*Electronic Commerce Services*)	
Objektif : Memastikan dan mengawal aplikasi dan maklumat dalam perkhidmatan e-dagang dari sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta menghalang pindaan yang tidak sah.	
060901 E-Dagang	
Bagi menggalakkan pertumbuhan e-dagang dan transaksi elektronik sebagai menyokong hasrat kerajaan merakyatkan perkhidmatan awam melalui perkhidmatan elektronik, semua pengguna boleh menggunakan kemudahan Internet Perkara-perkara berikut perlu dipatuhi: a. Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b. Maklumat yang terlibat dalam transaksi dalam talian (on-line) perlu dilindungi bagi mengelakkan penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi dengan perlindungan yang munasabah untuk mencegah sebarang pencerobohan atau pindaan yang tidak diperakukan.	Semua Pengguna
060902 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan dan ketepatan maklumat adalah seperti berikut: a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme perlindungan yang bersesuaian bergantung kepada tahap sensitiviti; b. Memastikan sistem yang boleh diakses oleh orang awam diuji dan disahkan terlebih dahulu; dan c. Memastikan segala maklumat yang hendak dipaparkan tepat dan betul serta telah disah dan diluluskan sebelum dimuat naik ke laman web atau sistem yang boleh diakses oleh orang awam.	Semua Pengguna
060903 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	
Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga. Perkara yang perlu dipatuhi adalah seperti berikut : a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dilaksanakan dan diselenggarakan oleh pihak ketiga;	Semua Pengguna

b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak dan diaudit dari semasa ke semasa; dan c. Pengurusan kepada perubahan penyediaan perkhidmatan termasuk penyelenggaraan dan penambahbaikan polisi keselamatan, prosedur dan kawalan maklumat sedia ada perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	

0610 Pemantauan

Objektif : Memastikan pengesanan dan penjejakan aktiviti pemprosesan maklumat yang dibenarkan.

061001 Pengauditan dan Forensik ICT

ICTSO mestilah bertanggungjawab merekod dan menganalisis : a. Sebarang percubaan pencerobohan kepada sistem ICT KKMM dan Jabatan/Agensi; b. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam* , pemalsuan (*forgery*, *phising*), pencerobohan (*intrusion*) ancaman (*threats*) dan kehilangan fizikal (*physical loss*); c. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti Kerajaan; e. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f. Aktiviti instalasi dan penggunaan perisian yang membebankan lebar jalur (*bandwidth)* rangkaian; g. Aktiviti penyalahgunaan akaun e-mel; dan h. Aktiviti penukaran Alamat IP *(IP address)* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem. Langkah-langkah yang perlu diambil adalah seperti berikut :- a. ICTSO akan menentukan prosedur pengumpulan bahan bukti (*hard disk*/media storan) yang berkenaan bagi memastikan kesahihan ke atas sesuatu laporan yang akan disediakan; b. Proses forensik dan pengauditan aset ICT mestilah dilakukan di tempat yang selamat; dan c. Sekiranya hasil siasatan mensabitkan kesalahan kepada tertuduh, laporan khas perlu disediakan. Semua proses dan hasil siasatan adalah SULIT.	Semua ICTSO

061002 Jejak Audit	
Jejak audit akan merekodkan semua aktiviti sistem. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi : a. Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; c. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan; d. Catatan jejak audit dari semasa ke semasa untuk membantu mengesan aktiviti yang tidak normal dengan lebih awal; e. Menyediakan laporan jika perlu; dan f. Aktiviti perlindungan dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubah suaian yang tidak dibenarkan.	Semua Pentadbir Sistem ICT
061003 Sistem Log	
Perkara yang perlu dipatuhi adalah seperti berikut: a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti tidak sah lain seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan kepada ICTSO Kementerian/ Jabatan/Agensi.	Semua Pentadbir Sistem ICT
061004 Pemantauan Log	
Bertujuan memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan, di antaranya seperti berikut : a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu di wujud dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d. Aktiviti pentadbiran dan operator sistem perlu direkodkan;	Semua Pentadbir Sistem ICT

e. Kesalahan, kesilapan dan / atau penyalahgunaan perlu di log, dianalisis dan diambil tindakan sewajarnya; dan f. Masa yang berkaitan dengan sistem pemprosesan maklumat dalam KKMM atau domain keselamatan perlu diselaraskan dengan satu sumber masa yang dipersetujui.	

PERKARA 07 – KAWALAN CAPAIAN

Objektif	
Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT KKMM.	
KENYATAAN	**TINDAKAN**
0701 Dasar Kawalan Capaian	
070101 Keperluan Dasar	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna sedia ada.	Semua Pentadbir Sistem ICT
0702 Pengurusan Capaian Pengguna	
Objektif : Mengawal capaian pengguna ke atas aset ICT KKMM.	
070201 Akaun Pengguna	
Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan langkah-langkah berikut hendaklah dipatuhi : a. Akaun yang diperuntukkan sahaja boleh digunakan; b. Akaun pengguna yang diwujudkan pertama kali akan diberi tahap capaian yang paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; c. Akaun pengguna mestilah unik dan hendaklah mencerminkan identiti pengguna; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan yang ditetapkan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Pentadbir sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut : i) Pengguna bercuti panjang; ii) Bertukar bidang tugas kerja; iii) Bertukar ke agensi lain; iv) Bersara; atau v) Ditamatkan perkhidmatan.	Semua Pengguna

070202 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Semua Pentadbir Sistem ICT
070203 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan seperti berikut : a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar kata laluan secara berkala, bila disyaki berlakunya kebocoran kata laluan atau di kompromi; c. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan antara huruf dan nombor (alphanumerik) manakala kata laluan bagi pembangunan aplikasi sistem yang baru mestilah sekurang-kurangnya dua belas (12) aksara dengan kombinasi aksara, angka dan aksara khas berkuat kuasa Januari 2008; d. Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; f. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g. Pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula hendaklah dikuatkuasakan mengikut kesusuaian sistem; h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i. Pentadbir Sistem ICT bertanggungjawab memaklumkan agar pengguna menukar kata laluan secara berkala; j. Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; k. Katalaluan hendaklah ditukar secara berkala selepas suatu tempoh masa; dan l. Mengelakkan penggunaan semula kata laluan yang telah digunakan sebelumnya.	Semua Pengguna

070204 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* bermaksud tidak meninggalkan sebarang maklumat penting di atas meja apabila pengguna tidak berada di tempatnya. *Clear Screen* bermaksud tidak memaparkan sebarang maklumat penting di paparan skrin apabila pengguna tidak berada di tempatnya. Bagi menjamin keselamatan, semua pengguna perlu mengambil langkah-langkah berikut: a. Menggunakan kemudahan *password screen saver* atau mengamalkan amalan log keluar atau *sign out* apabila meninggalkan komputer; b. Maklumat-maklumat penting hendaklah disimpan di dalam laci atau kabinet fail yang berkunci; dan c. Semua dokumen hendaklah diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat atau medium output yang lain sebaik sahaja dokumen tersebut dijana, diterima atau digunakan.	Semua Pengguna
0703 Kawalan Capaian	
Objektif : Menghalang capaian yang tidak sah dan tanpa kebenaran serta boleh menyebabkan kerosakan.	
070301 Kawalan Capaian Rangkaian	
Perkara yang perlu dipatuhi adalah seperti berikut :- a. Memastikan pengguna membuat capaian kepada sistem yang dibenarkan sahaja; b. Menempatkan atau memasang antaramuka yang bersesuaian di antara rangkaian KKMM/Jabatan/Agensi dan rangkaian agensi lain atau rangkaian awam; c. Mewujudkan mekanisme pengesahan yang sesuai untuk mengawal capaian oleh pengguna jarak jauh; d. Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan e. Mewujud dan melaksanakan kawalan pengalihan laluan (*routing control*) untuk memastikan rangkaian boleh diakses oleh pengguna.	Semua Pentadbir Sistem ICT

070302 Capaian Jarak Jauh	
a. Penghantaran maklumat yang menggunakan capaian jarak jauh menggunakan kaedah *remote access* mestilah menggunakan kaedah penyulitan (*encryption*);	Semua Pengguna
b. Lokasi bagi akses ke sistem ICT KKMM /Jabatan/Agensi hendaklah dipastikan selamat; dan	
c. Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pengurus ICT. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	
070303 Capaian Internet	
a. Penggunaan Internet hendaklah dipantau secara berterusan bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian KKMM/Jabatan/Agensi;	Semua Pentadbir Sistem ICT
b. Penggunaan Internet hanyalah untuk kegunaan rasmi dan secara berhemah. Pengurus ICT berhak menentukan pengguna yang dibenarkan menggunakan Internet atau sebaliknya;	Semua Pengurus ICT
c. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan;	Semua Pentadbir Sistem ICT
d. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing*, *video streaming, chat, downloading*) perlu dipertimbangkan bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan;	
e. KKMM/Jabatan/Agensi hendaklah mempertimbangkan rangkaian berasingan untuk capaian Internet antara warga dan capaian Internet bagi orang awam melalui kaedah *Virtual LAN* (VLAN) atau lain-lain, termasuk bagi rangkaian tanpa wayar (WiFi);	
f. Penggunaan apa jua modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali;	Semua Pengguna
g. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang ditetapkan mengikut senarai tugas;	
h. Bahan yang diperoleh dari Internet hendaklah ditentukan kesahihan dan ketepatannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan;	
i. Bahan rasami hendaklah disemak dan mendapat pengesahan daripada Ketua Bahagian sebelum dimuat naik ke Internet atau dihantar secara meluas melalui e-mail;	
j. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh KKMM/Jabatan/Agensi sahaja;	

k. Pengguna yang dibenarkan dan diberikuasa sahaja dibenarkan membuat sebaran media berkaitan KKMM/Jabatan/Agensi melalui e-mel dan Internet; l. Perisian atau aplikasi yang boleh menyebabkan kesesakan dan mengganggu prestasi capaian Internet seperti perisian/aplikasi perkongsian *peer-to-peer (P2P)* atau lain-lain yang seumpamanya, atau aktiviti seperti memuat naik/turun fail dan aktiviti *media streaming* yang dilaksanakan secara berterusan tanpa kelulusan adalah tidak dibenarkan. Pentadbir Rangkaian boleh memutus dan menyekat aktiviti ini bagi memastikan kelancaran operasi KKMM/Jabatan/Agensi. m. Pengguna adalah dilarang melakukan aktiviti-aktiviti seperti berikut : i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik dan video/audio/multimedia yang boleh menjejaskan tahap capaian Internet dan prestasi peralatan ICT; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan kandungan serta melibatkan diri secara sosial melalui teks ucapan, komen atau apa jua cara/bahan yang mengandungi unsur-unsur fitnah, hasutan, lucah dan/atau melanggar dasar-dasar semasa Kerajaan. n. Pengguna hendaklah berhenti, menutup aplikasi dan memutuskan talian dengan serta merta sekiranya menerima dan/atau disambungkan ke laman Internet yang mengandungi unsur-unsur tidak menyenangkan atau tidak dibenarkan.	
0704 Kawalan Capaian Sistem Pengoperasian	
Objektif : Melindungi sistem maklumat dan aplikasi sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kerosakan.	
070401 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian komputer yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi : a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; b. Merekodkan capaian yang berjaya dan gagal; dan c. Membekalkan kemudahan untuk pengesahan bagi sistem kata kunci digunakan, kualiti kata kunci perlu mendapat pengesahan. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut :-	Semua Pentadbir Sistem ICT, ICTSO

a. Mengesahkan pengguna yang dibenarkan selaras dengan peraturan Jabatan; b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user;* c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan d. Menyediakan tempoh penggunaan mengikut kesesuaian. Perkara yang perlu dipatuhi termasuk berikut :- a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; b. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja dan satu teknik pengesahan yang bersesuaian hendaklah diwujudkan bagi mengesahkan pengenalan diri pengguna; c. Mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; d. Mengehadkan dan mengawal penggunaan program utiliti yang berkemampuan bagi satu tempoh yang ditetapkan; dan e. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	

0705 Kawalan Capaian Sistem dan Aplikasi

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

070501 Sistem Maklumat dan Aplikasi	
Capaian sistem dan aplikasi di KKMM adalah terhad kepada pengguna dan tujuan yang dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh. Perkara yang perlu dipatuhi adalah seperti berikut : a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; c. Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d. Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna akan disekat; dan	Semua Pentadbir Sistem ICT, ICTSO

e. Memastikan kawalan sistem adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah.	
0706 Peralatan Mudah Alih dan Kerja Jarak Jauh	
Objektif : Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh	
070601 Peralatan Mudah Alih	
Capaian sistem maklumat dan aplikasi melalui peralatan mudah alih adalah digalakkan. Walau bagaimana pun, penggunaannya perlu mematuhi amalan keselamatan ICT. Perkara yang perlu dipatuhi adalah seperti berikut : a. Mengambil kira dan mempertimbangkan peralatan berasaskan Trusted Platform Module (TPM), dikonfigurasi secara optimum dan diaktifkan semasa membuat perolehan ICT; b. Pentadbir ICT hanya menyediakan sokongan terhad *('reasonable endeavors')* kepada pengguna bagi tujuan konfigurasi, tetapan dan penggunaan peralatan mudah alih bagi capaian ke sistem aplikasi yang dibenarkan untuk urusan rasmi sahaja; c. Memasang dan menggunakan kata laluan bagi mengelakkan akses yang tidak dibenarkan; d. Memasang dan menggunakan perisian keselamatan ICT seperti *anti-virus* pada peralatan mudah alih; e. Menyimpan dan mengunci peralatan mudah alih di tempat yang selamat apabila tidak digunakan; f. Melaporkan kehilangan peralatan mudah alih kepada ICTSO; dan g. Mengaktifkan kemudahan 'remote wipe' (sekiranya ada) bagi memadam maklumat Kerajaan dari peralatan mudah alih sekiranya berlaku perkara tidak diingini.	Semua Pentadbir Sistem ICT Semua Pengguna

070602 Kerja Jarak Jauh	
Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja. Perkara yang perlu dipatuhi adalah seperti berikut : a. Capaian yang dibuat bagi kerja jarak jauh hendaklah melalui medium atau antaramuka yang dibenarkan sahaja; b. Tindakan perlindungan hendaklah diambil bagi menghalang pendedahan maklumat dan capaian tidak sah serta penyalahgunaan; c. Pengguna hendaklah memastikan keselamatan maklumat teperingkat terjamin semasa menjalankan Kerja Jarak Jauh, terutamanya Kerja Jarak Jauh yang dilaksanakan melalui rangkaian awam atau komputer guna sama ditempat awam; dan d. Memastikan capaian jarak jauh diputuskan *(log out)*, setelah melaksanakan Kerja Jarak Jauh.	Semua Pengguna

PERKARA 08 – PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

Objektif	
Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
KENYATAAN	**TINDAKAN**
0801 Keselamatan Dalam Membangunkan Sistem dan Aplikasi	
080101 Keperluan Keselamatan	
Perkara yang perlu dipatuhi adalah seperti berikut : a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna dan; sistem output untuk memastikan data yang telah diproses adalah tepat; c. Aplikasi perlu mengandungi semakan pengesahan *(validation)* untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Semua Pentadbir Sistem ICT, ICTSO
080102 Pengesahan Data Input	
Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian.	Semua Pentadbir Sistem ICT
080103 Kawalan Prosesan	
Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Semua Pentadbir Sistem ICT
080104 Pengesahan Data Output	
Data *output* daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Semua Pentadbir Sistem ICT

0802 Kriptografi	
Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	
080201 Penyulitan *(Encryption)*	
Pengguna hendaklah membuat penyulitan (*encryption*) ke atas maklumat terperingkat dan maklumat rahsia rasmi pada setiap masa berdasarkan kepada prosedur, tatacara dan Arahan Keselamatan.	Semua Pengguna
080202 Sijil/Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua Pengguna
080203 Pengurusan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, di musnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua Pengguna
0803 Fail Sistem	
Objektif : Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
080301 Kawalan Fail Sistem	
Perkara yang perlu dipatuhi adalah seperti berikut : a. Proses pengemas kini fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubah suaian tanpa kebenaran, penghapusan dan kecurian; d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Semua Pentadbir Sistem ICT

0804 Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080401 Pengurusan Kawalan Perubahan	
Perkara yang perlu dipatuhi adalah seperti berikut : a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; b. Aplikasi kritikal perlu dikaji semula apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan buruk terhadap keselamatan KKMM/Jabatan/Agensi; c. Pegawai yang dilantik atau Jawatankuasa tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilaksanakan sama ada secara dalaman atau oleh pihak ketiga; d. Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; e. Akses kepada kod sumber *(Source Code)* aplikasi adalah dihadkan kepada pengguna yang dibenarkan sahaja; dan f. Menghalang sebarang peluan untuk membocorkan maklumat.	Semua Pentadbir Sistem ICT
080402 Pembangunan Secara *Outsource*	
Pembangunan perisian aplikasi secara *outsource* perlu dipantau oleh BPM KKMM atau Bahagian/Cawangan/Unit ICT Jabatan/Agensi KKMM. *Source code* adalah hak milik Kerajaan/KKMM.	Semua Pentadbir Sistem ICT
0805 Kawalan Teknikal Keterdedahan (Vulnerability)	
Objektif : Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan terkini dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080501 Kawalan dari Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi. 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 mengenalpasti tahap risiko yang bakal dihadapi; dan c. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Semua Pentadbir Sistem ICT

PERKARA 09 – PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN ICT

Objektif
Untuk memastikan semua insiden dikendalikan dengan cepat, tepat dan berkesan dan memastikan sistem ICT KKMM dapat segera beroperasi semula dengan baik supaya tidak menjejaskan imej KKMM/Jabatan/Agensinya dan sistem penyampaian perkhidmatan.

KENYATAAN	TINDAKAN
0901 Pengurusan Insiden Keselamatan ICT	
090101 Mekanisme Pelaporan Insiden Keselamatan ICT	
Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada CERT KKMM dengan kadar segera :- a. Maklumat didapati hilang, didedahkan kepada pihak-pihak yang tidak diberi kuasa atau, disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak diingini. Sekiranya berlaku insiden keselamatan ICT, maka mekanisme pelaporan adalah seperti berikut :-	Semua Pengguna
i. Pelaporan Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan kepada CERT KKMM untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan.	Semua Pengguna
ii. CERT KKMM Pasukan CERT KKMM akan bertindak menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai *input* atau untuk tindakan seterusnya.	CERT KKMM
iii. Tanggungjawab Pengguna Semua pengguna yang terlibat diingatkan supaya tidak melaksanakan sebarang tindakan peribadi, tapi sebaliknya melaporkan dengan segera sebarang insiden keselamatan ICT kepada ICTSO, kerentanan (*vulnerabality*) yang diperhatikan atau disyaki terdapat dalam sistem maklumat menerusi mekanisme pelaporan yang ditetapkan, bagi mengelakkan kerosakan atau kehilangan bahan bukti pencerobohan dan cubaan menceroboh.	Semua Pengguna
	Semua

iv. Tindakan Dalam Keadaan Berisiko Tinggi Dalam keadaan atau persekitaran berisiko tinggi, pengurusan atasan hendaklah dimaklumkan dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi mengelakkan kesan atau impak kerosakan yang lebih teruk dan mengelakkan kejadian insiden merebak.	CIO, ICTSO
090102 Prosedur Pengurusan Pengendalian Insiden Keselamatan ICT	
Semua pegawai pasukan pengendali insiden keselamatan ICT atau CERT KKMM perlu melaksanakan pengurusan pengendalian insiden keselamatan ICT berpandukan prosedur operasi piawai. CERT KKMM menerima aduan atau laporan daripada pengguna, laporan yang dikesan dari agensi pusat atau laporan dari sumber luar. Seterusnya, maklumat tentang insiden akan didaftarkan. Siasatan awal atau kajian perlu dijalankan bagi mengenal pasti jenis insiden tersebut. Laporan insiden kemudiannya dimaklumkan kepada GCERT MAMPU. Sekiranya insiden tersebut memerlukan tindakan undang-undang susulan, laporan dipanjangkan kepada agensi penguat kuasa undang-undang. CERT KKMM yang diketuai oleh Pengurus ICT akan menjalankan tindakan pengendalian secara capaian jarak jauh *(remote)* atau ditapak *(on-site).* Sekiranya laporan tersebut memerlukan bantuan GCERT MAMPU, permohonan perlu dihantar bagi mendapatkan maklum balas GCERT MAMPU. Bagi laporan yang memerlukan bantuan daripada CERT agensi yang lain, permohonan perlu dihantar melalui GCERT MAMPU dan khidmat nasihat akan disalurkan. CERT KKMM seterusnya akan menyediakan laporan dan ICTSO mengesahkan sekiranya Pelan Kesinambungan Perkhidmatan (PKP) perlu diaktifkan atau sebaliknya. Laporan insiden yang tidak memerlukann PKP akan diteruskan dengan melaksanakan tindakan bagi tujuan pemulihan. Carta lengkap mengenai perjalanan laporan insiden seperti di Lampiran B.	CERT KKMM
0902 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif : Memastikan pendekatan yang konsisten dan efektif dalam pengurusan maklumat insiden keselamatan ICT.	
090201 Pengurusan Maklumat Insiden Keselamatan ICT	
Perkara yang perlu dipatuhi adalah seperti berikut : a. Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan dan tindakan untuk melaksanakan peningkatan dan kawalan tambahan bagi mengawal kekerapan, kerosakan dan kos kejadian insiden akan datang, dan untuk tujuan mengkaji semula dasar-dasar keselamatan aset ICT sedia ada. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KKMM/Jabatan/Agensinya;	Semua ICTSO

b. Memastikan bahan-bahan bukti berkaitan insiden keselamatan ICT dapat disediakan, disimpan, diselenggarakan dan dilindungi. Penyediaan bahan-bahan bukti seperti jejak audit, penduaan secara berkala dan media penduaan di luar talian hendaklah mengikut amalan terbaik yang disarankan oleh Kerajaan dari semasa ke semasa; c. Memastikan semua bahan bukti adalah selaras dengan peraturan pengumpulan maklumat dari segi kualiti, kelengkapan dan kebolehpercayaan bahan bukti yang termaktub dalam bidang kuasa perundangan berkenaan; dan d. Memastikan perkara berikut diambil kira : i. Melindungi integriti semua bahan bukti; ii. Menyalin bahan bukti oleh personel yang dipertanggungjawabkan; iii. Merekodkan semua maklumat aktiviti penyalinan termasuk pegawai terlibat, media, perisian, perkakasan dan *tools* yang digunakan; iv. Memaklumkan pihak berkuasa perundangan, seperti pegawai undang-undang dan polis (jika perlu); dan v. Mendapatkan nasihat dari pihak berkuasa perundangan ke atas bahan bukti yang perlukan.	

PERKARA 10 – PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

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

KENYATAAN	TINDAKAN
1001 Dasar Kesinambungan Perkhidmatan	
100101 Pelan Kesinambungan Perkhidmatan	
Pelan Kesinambungan Perkhidmatan (PKP) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT atau jawatankuasa berkaitan. Perkara berikut yang perlu diberi perhatian : a. Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; b. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap perkhidmatan/proses kerja, kemungkinan serta impak gangguan tersebut dan akibat terhadap keselamatan ICT; c. Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; d. Mendokumentasikan proses dan prosedur yang telah dipersetujui; e. Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; f. Membuat penduaan; dan g. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. PKP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; b. Senarai personel KKMM/Jabatan/Agensi dan pihak ketiga berkaitan berserta maklumat perhubungan hendaklah disediakan bersama senarai kedua bagi menggantikan personel yang tidak dapat dihubungi atau hadir menangani insiden; c. Senarai lengkap maklumat yang memerlukan penduan dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;	Koordinator PKP KKMM/ Jabatan /Agensi

d. Sumber pemprosesan alternatif dan lokasi untuk menggantikan sumber yang telah lumpuh; dan e. Perjanjian dengan pihak ketiga untuk mendapat keutamaan penyambungan semuala perkhidmatan berkaitan.	
100102 Pengurusan Kesinambungan Perkhidmatan	
Pengurusan Kesinambungan Perkhidmatan (PKP) adalah mekanisme bagi mengurus dan memastikan kepentingan *stakeholder* sistem penyampaian perkhidmatan dilindungi dan imej KKMM/Jabatan/Agensi terpelihara. Ini dilakukan dengan mengenal pasti kesan atau impak yang berpotensi menjejaskan sistem penyampaian perkhidmatan di samping menyediakan pelan tindakan bagi mewujudkan ketahanan dan keupayaan bertindak yang berkesan. Perkara yang perlu dipatuhi adalah seperti berikut : a. Salinan PKP perlu disimpan dilokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama; b. PKP hendaklah diuji sekurang-kurangnya sekali setahun atau mengikut keperluan apabila terdapat perubahan dalam persekitaran atau fungsi aktiviti bisnes untuk memastikan ia sentiasa berkesan; c. Penilaian secara berkala pelan tersebut hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi objektifnya; dan d. Salinan PKP hendaklah dikemaskini dan dilindungi. KKMM/Jabatan/Agensi bertanggungjawab untuk memastikan operasi sistem penyampaian perkhidmatan di bawah kawalannya disediakan secara berterusan tanpa gangguan di samping menyediakan perlindungan keselamatan kepada aset ICT KKMM.	Koordinator PKP KKMM/ Jabatan /Agensi

PERKARA 11 – PEMATUHAN

Objektif	
Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran DKICT KKMM.	
KENYATAAN	**TINDAKAN**
1101 Pematuhan dan Keperluan Perundangan	
110101 Pematuhan Dasar	
Semua pengguna di KKMM dan Jabatan/Agensi hendaklah membaca, memahami dan mematuhi DKICT KKMM dan undang-undang atau peraturan-peraturan lain yan berkaitan yang berkuat kuasa. Semua aset ICT KKMM termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT KKMM dan Jabatan/Agensi selain daripada maksud dan tujuan yang ditetapkan adalah merupakan satu penyalahgunaan sumber ICT KKMM serta merupakan suatu pelanggaran dasar.	Semua Pengguna
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem maklumat perlu melalui pemeriksaan secara berkala bagi mematuhi piawaian pelaksanaan keselamatan dan amalan terbaik industri.	Semua ICTSO
110103 Pematuhan Keperluan Audit	
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Semua Pengguna
110104 Keperluan Perundangan	
Keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi adalah seperti di LAMPIRAN D – SENARAI PERUNDANGAN DAN PERATURAN.	Semua Pengguna

Tindakan Tatatertib	
Objektif : Meningkatkan kesedaran dan pematuhan ke atas DKICT KKMM serta memastikan kelancaran operasi ICT KKMM pada setiap masa.	
110201 Pelanggaran Dasar / Perundangan	
Pelanggaran DKICT KKMM dan semua perbuatan kecuaian, kelalaian dan pelanggaran keselamatan ICT yang membahayakan terutamanya melibatkan maklumat terperingkat dan rahsia rasmi di bawah Akta Rahsia Rasmi 1972 akan dikenakan tindakan tatatertib berdasarkan perundangan sedia ada yang berkuat kuasa.	Semua Pengguna

GLOSARI	
Antivirus	Perisian yang mengimbas virus pada media storan, seperti disket, cakera padat, pita magnetik, *optical disk*, *flash disk*, CDROM 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.
CERT KKMM	Organisasi yang ditubuhkan untuk membantu Jabatan/Agensi mengurus pengendalian insiden keselamatan ICT di KKMM dan Jabatan/Agensi di bawah kawalannya.
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.
DKICT KKMM	Dasar Keselamatan ICT KKMM dan terpakai kepada KKMM semua Jabatan/Agensi di bawahnya.
Downloading	Aktiviti muat-turun data.
Encryption	Enkripsi atau penyulitan 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 Pengendali Insiden Keselamatan ICT Kerajaan.
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.
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.

GLOSARI	
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 Prevention System (IPS)	Sistem Pencegah Pencerobohan - Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian atau aktiviti yang berbahaya. Boleh bertindak balas menyekat atau menghalang aktiviti serangan. Contohnya, *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
Instant Messaging	Perisian pada peranti yang membenarkan komunikasi dua hala menggunakan perkhidmatan Internet sebagai medium penghantaran data.
KKMM	Kementerian Komunikasi dan Multimedia Malaysia.
LAN	*Local Area Network* - Rangkaian Kawasan Setempat yang menghubungkan 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.
Media Sosial	Media dalam talian yang membenarkan pengguna bersosial, bersembang dan berhubung. Contohnya Facebook, Twitter, Instagram dan lain-lain.
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.
Pihak Ketiga	Kontraktor, Pembekal, Pakar Runding dan pihak-pihak lain yang berkepentingan
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian, teknologi penyulitan dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Public Cloud Storage	Perkhidmatan storan data dalam talian sama ada yang disediakan secara percuma atau berbayar. Lazimnya digunakan untuk menyimpan data untuk membolehkan ia dicapai dengan mudah melalui peranti yang mempunyai sambungan Internet.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.

GLOSARI	
Screen saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan komputer
Smartphone	Telefon pintar yang mempunyai ciri-ciri kalendar, buku telefon, kamera, storan, pelbagai aplikasi dan kebolehan untuk mencapai maklumat dan perkhidmatan di Internet. Lazimnya mempunyai skrin paparan kurang dari 6.0 inci.
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.
Tablet	Peranti pintar yang menyamai rupa dan fungsi *Smartphone* namun, lazimnya mempunyai paparan skrin lebih besar dari 6.0 inci.
Threats	Gangguan dan ancaman secara aktif atau pasif melalui pelbagai cara termasuk pesanan ringkas, e-mel dan surat yang bermotif peribadi dan atas sebab tertentu atau tindakan-tindakan zahir yang membawa maksud yang sama.
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 Conferencing	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 A

BORANG DKICT 01
SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT
KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA

Nama : .....

No. Kad Pengenalan : .....

Jawatan : .....

Kementerian / Jabatan : .....

*Bagi pihak ketiga sahaja : Syarikat : .....

MyCoID : .....

Alamat Berdaftar : .....

.....

Nombor Telefon : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

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

2. Saya telah mengikuti Taklimat Dasar Keselamatan ICT atau mendapatkan penerangan lanjut mengenai Dasar Keselamatan ICT daripada pegawai bertanggungjawab; dan

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

* Cop Syarikat

.....
(Tanda Tangan)

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

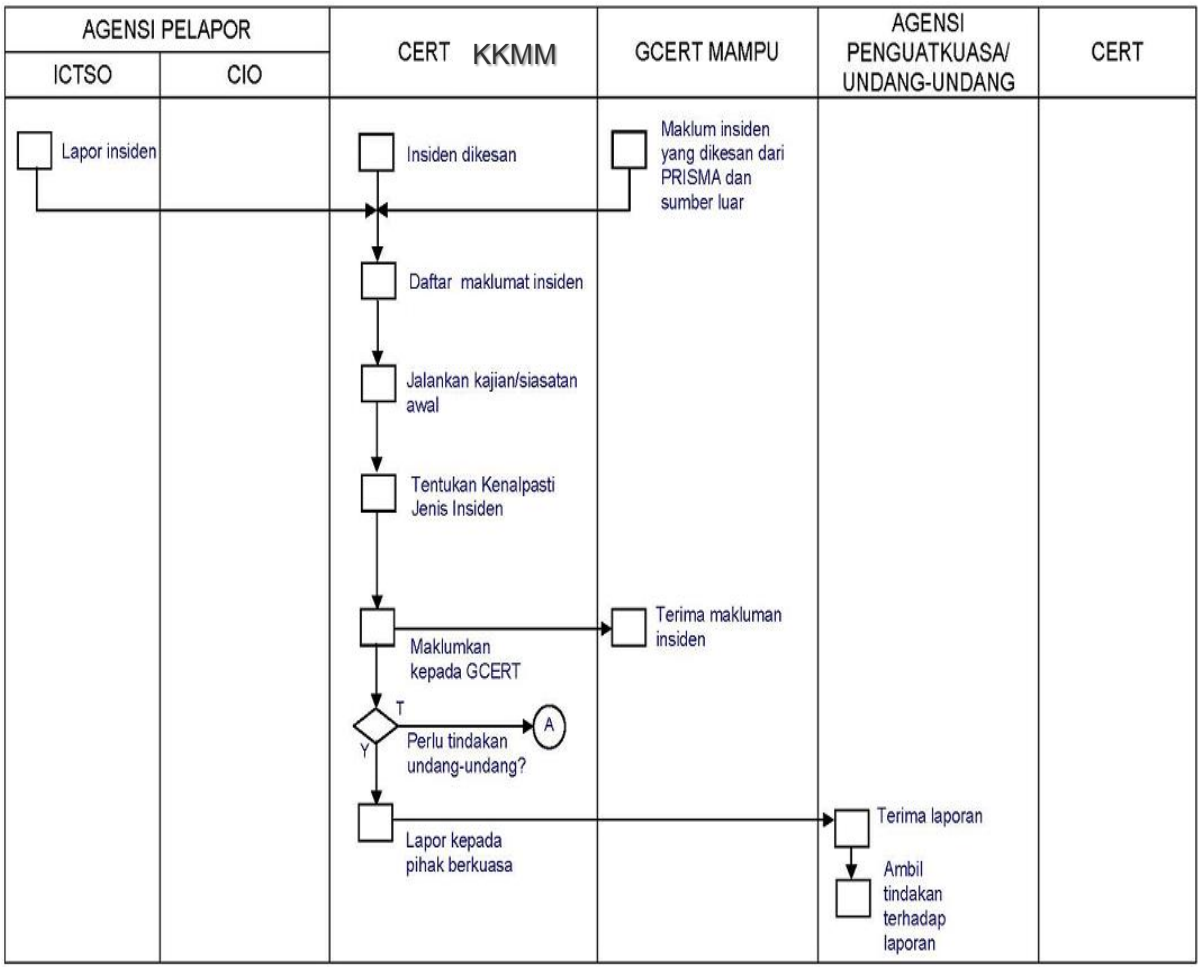
.....
(Nama Pegawai Keselamatan ICT)
b.p Ketua Pengarah
Kementerian / Jabatan

Tarikh : .....

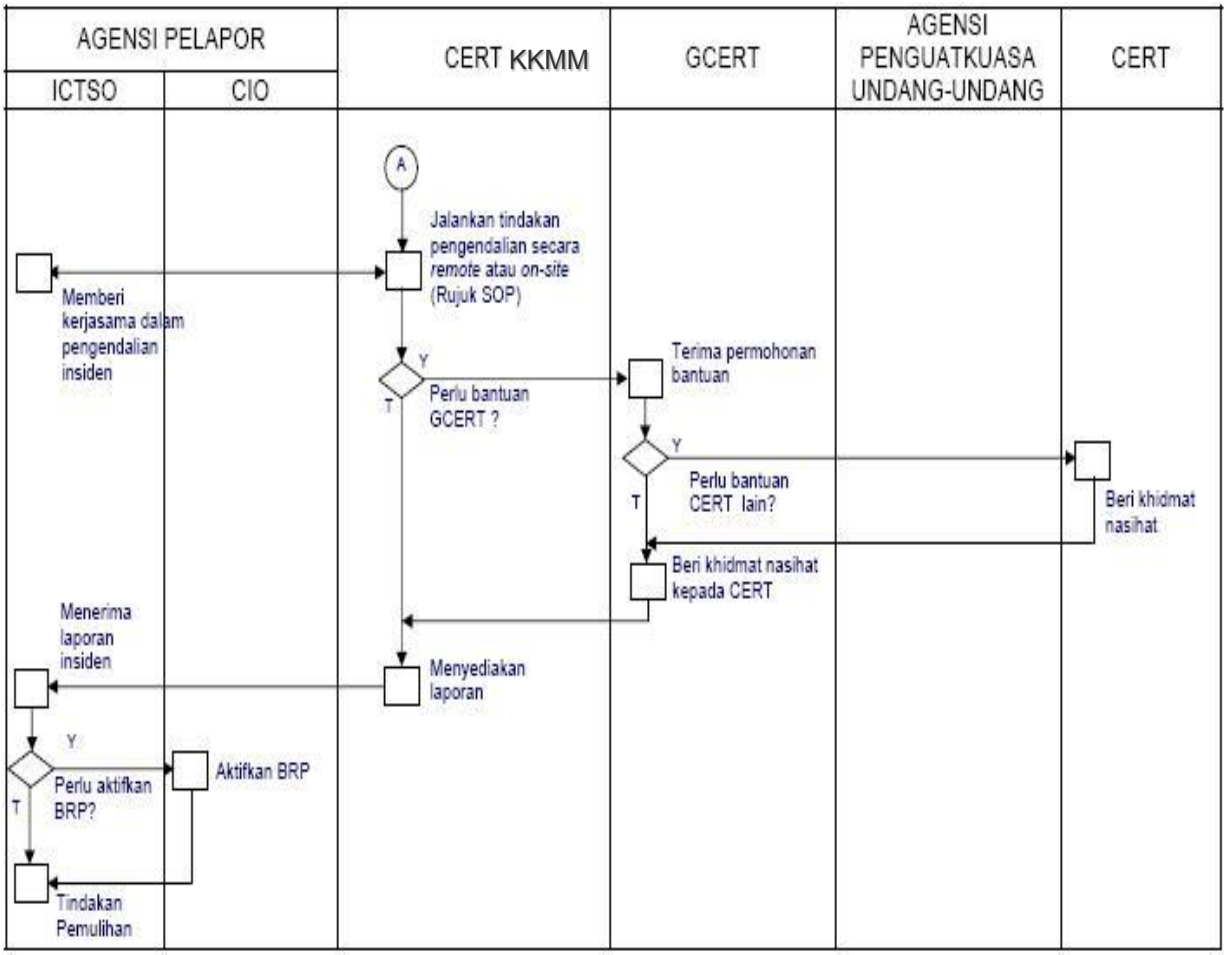
* Bagi pihak ketiga yang bukan terdiri daripada Penjawat Awam, sila lampirkan satu (1) salinan MyKAD.

Lampiran B

PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT KKMM



PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT KKMM
(Sambungan)



Lampiran C

BORANG PENGISYTIHARAN BARANG KELUAR/MASUK
BAHAGIAN KESELAMATAN
KEMENTERIAN KOMUNIKASI DAN MULTIMEDIA MALAYSIA

Nama : ..... Syarikat: .....

No. Kenderaan : .....

Urusan dengan Bahagian/Unit/Cawangan : .....

BHG. A : SENARAI BARANG YANG DI BAWA MASUK

1.
2.
3.
4.
5.

....
Tandatangan Pemilik Kenderaan Tandatangan Pengawal Keselamatan

BHG. : SENARAI BARANG YANG DIBAWA KELUAR

1.
2.
3.
4.
5.

Disahkan oleh : .....
Tandatangan

Nama :

Jab./Caw./Bhg./Unit :

Tarikh :

***Nota :**

Pihak Tuan hendaklah menentukan dan memastikan barangan yang dikeluarkan mempunyai Surat Kebenaran. Sekiranya tiada, ia boleh dianggap barangan curi dan boleh dirampas oleh Bahagian Keselamatan.

Lampiran D

SENARAI PERUNDANGAN DAN PERATURAN

a. Arahan Keselamatan;

b. Surat Pekeliling Am Bilangan 2 Tahun 2000 bertajuk "Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK)" dan pindaanya;

c. Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan";

d. Pekeliling Am Bilangan 1 Tahun 2001 bertajuk "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)";

e. *"Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS)" 2002;

f. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan";

g. Surat Pekeliling Am Bilangan 6 Tahun 2005 bertajuk "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam";

h. Surat Pekeliling Am Bilangan 4 Tahun 2006 bertajuk "Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam";

i. Surat Pekeliling Perbendaharaan Bilangan 8 Tahun 2006 bertajuk "Peraturan Perolehan Perkhidmatan Perunding";

j. Pekeliling Am Bilangan 1 Tahun 2006 bertajuk "Pengurusan laman Web/Portal Sektor Awam";

k. Surat Arahan Ketua Setiausaha Negara dengan rujukan UPTM(S)159/338/8 Jilid 30 (84) bertajuk "Langkah-langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-Agensi Kerajaan" bertarikh 20 Oktober 2006;

l. Surat Arahan MAMPU bertajuk "Langkah-langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan" bertarikh 1 Jun 2007;

m. Surat Arahan MAMPU bertajuk "Langkah-langkah Pemantapan Pelaksanaan Mel Elektronik di Agensi-Agensi Kerajaan" bertarikh 23 November 2007;

n. Surat Pekekliling Am Bilangan 3 Tahun 2009 bertajuk "Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam" bertarikh 17 November 2009;

o. Surat Arahan Ketua Pengarah MAMPU bertajuk "Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam" bertarikh 22 Januari 2010;

p. Akta Rahsia Rasmi 1972;

q. Akta Tandatangan Digital 1997;

SENARAI PERUNDANGAN DAN PERATURAN
(Sambungan)

r. Akta Jenayah Komputer 1997;

s. Akta Hak cipta (Pindaan) Tahun 1997;

t. Akta Komunikasi dan Multimedia 1998;

u. Arahan Teknologi Maklumat 2007;

v. Akta-Akta dan Garis Panduan berkaitan Jabatan/Agensi KKMM;

w. Perintah-Perintah Am;

x. Arahan Perbendaharaan; dan

y. Standard Operating Procedure (SOP) ICT KKMM dan Jabatan/Agensi.

DASAR KESELAMATAN
TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

Kementerian Komunikasi dan Multimedia Malaysia (KKMM)	www.kkmm.gov.my
Jabatan Penyiaran Malaysia (RTM)	www.rtm.gov.my
Jabatan Penerangan Malaysia (JAPEN)	www.penerangan.gov.my
Jabatan Hal Ehwal Khas (JASA)	www.jasa.gov.my
Institut Penyiaran dan Penerangan Tun Abdul Razak (IPPTAR)	www.ipptar.gov.my
Jabatan Perlindungan Data Peribadi (PDP)	www.pdp.gov.my
Perbadanan Kemajuan Filem Nasional Malaysia (FINAS)	www.finas.gov.my
Pertubuhan Berita Nasional Malaysia (BERNAMA)	www.bernama.com