DASAR DAN GARIS PANDUAN KESELAMATAN ICT

JABATAN KERJA RAYA MALAYSIA

PRAKATA

Teknologi maklumat dan komunikasi (ICT) telah digunakan secara meluas dalam urusan harian di Jabatan Kerja Raya (JKR). Kepentingan ICT dalam urusan harian telah dapat membantu memudahkan dan mempercepatkan tugas-tugas yang perlu dilakukan. Oleh itu keselamatan ICT adalah satu perkara penting bagi memastikan kelancaran urusan harian JKR tidak terganggu.

Jabatan Kerja Raya sedar akan tanggungjawab dan kepentingan dalam memastikan keselamatan semua aset ICT kerajaan yang berada di bawah jagaan dan kawalan Jabatan. Ini termasuk semua data dan maklumat, perkakasan, perisian, applikasi, rangkaian dan kemudahan serta perkhidmatan ICT. Tanggungjawab ini harus dipikul bersama oleh semua kakitangan atau sesiapa sahaja yang mengakses dan yang menggunakan kemudahan aset ICT Jabatan.

Bagi menjamin keselamatan aset-aset ICT JKR khasnya dan Kerajaan amnya, maka Dasar dan Garis Panduan Keselamatan ICT JKR digubal. Objektif dasar dan garis panduan ini adalah untuk menjamin kesinambungan urusan di JKR dan meminimumkan kesan insiden keselamatan. Ianya termasuk meminimumkan kesan kerosakan dan kemusnahan, melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dan mencegah salahguna atau kecurian aset ICT.

Dengan adanya Dasar dan Garis Panduan Keselamatan ICT ini diharap dapat membantu meminimumkan kesan insiden keselamatan agar kesinambungan perkhidmatan di JKR dapat dijamin. Adalah menjadi harapan saya agar Dasar dan Garis Panduan Keselamatan ICT JKR ini dibaca, difahami dan dijadikan rujukan dalam sebarang pelaksanaan program ICT Jabatan agar keselamatan ICT di JKR dapat dijamin keberkesanannya.

DATO' IR. HJ. MOHD NOOR BIN YAACOB
KETUA PENGARAH KERJA RAYA
MALAYSIA
OGOS 2011

KANDUNGAN

SINGKATAN

CIO – Ketua Pegawai Maklumat (*Chief Information Officer*)

ICTSO – Pegawai Keselamatan ICT (*Information and Communication Technology Security Officer*)

ICT – Teknologi Maklumat dan Komunikasi (*Information and Communication Technology*)

JKR – Jabatan Kerja Raya

JPICT - Jawatankuasa Pemandu ICT

KPKR – Ketua Pengarah Kerja Raya

MAMPU – Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (Malaysian Administrative Modernisation and Management Planning Unit)

ISTILAH

APLIKASI adalah merujuk kepada sistem berkomputer yang dibangunkan atau diperoleh secara siap guna seperti eSPKB, ePerolehan, Sistem Pengurusan Maklumat Sumber Manusia (HRMIS), MyKJ, CutiWeb, etass dan lain-lain termasuk juga pakej perisian seperti pemprosesan kata dan helaian kerja.

ASET ICT adalah data, maklumat, perkakasan, perisian, aplikasi, sistem, dokumentasi dan sumber manusia serta premis berkaitan dengan ICT yang berada di bawah tanggungjawab JKR.

DASAR adalah pendirian yang menjadi asas segala tindakan yang telah dipersetujui secara rasmi untuk membuat atau melaksanakan sesuatu tindakan dan keputusan, menurut dasar agensi/kerajaan.

DOKUMENTASI adalah semua himpunan atau kumpulan bahan atau dokumen yang disimpan dalam bentuk media cetak, salinan lembut, elektronik luar atau dalam talian, kertas lutsinar, risalah atau slaid.

INSIDEN KESELAMATAN adalah musibah yang berlaku terhadap sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.

INTERNET adalah sistem perangkaian antarabangsa yang membolehkan pengguna mencapai maklumat dari seluruh dunia.

KABEL adalah meliputi semua kabel yang berkaitan dengan ICT dan elektrik seperti kabel rangkaian, kabel sambungan elektrik, kabel elektrik dan sebagainya.

KESELAMATAN adalah keadaan yang bebas daripada ancaman dan risiko yang tidak boleh diterima.

KOMUNIKASI adalah pengaliran maklumat daripada sumber pengeluar maklumat ke sumber penerima maklumat.

MEL SAMPAH adalah mel yang tidak berkaitan yang dihantar kepada seseorang.

MEL BOM adalah penghantaran mel secara bertalu-talu (*looping*) yang menyebabkan penerima mengalami masalah.

MEL SPAM adalah mel yang dihantar oleh penghantar yang tidak diketahui seperti menerima mel daripada seorang jurujual yang cuba menjual produknya melalui emel.

MEDIA STORAN adalah perkakasan yang berkaitan dengan penyimpanan data dan maklumat seperti disket, katrij, cakera padat, cakera mudah alih, pita, cakera keras dan pemacu pena.

PANGKALAN DATA adalah kumpulan fail atau rekod komputer yang berkait secara logik.

PENCEGAHAN adalah kerja-kerja pengawalan supaya sistem ICT tidak mengalami gangguan atau kerosakan.

PENGGUNA adalah semua pengguna-pengguna ICT JKR termasuk kakitangan dan bukan kakitangan JKR, pembekal, pakar runding dan sebagainya yang bertugas dengan JKR.

PENTADBIR SISTEM adalah termasuk Pentadbir Sistem Aplikasi, Pentadbir Sistem Rangkaian, Pentadbir Server dan Pentadbir Sistem Lain.

PERISIAN adalah bahagian sistem komputer yang berfungsi menjalankan sistem, dan terdiri daripada aturcara, rutin, subrutin, dan suruhan yang ditulis dalam bahasa pengaturcaraan. Penghimpun, penyusun, penjana dan sistem pengendalian digolongkan sebagai perisian.

PERISIAN BERBAHAYA adalah aturcara yang dibina bagi tujuan mendatangkan kemudaratan kepada pengguna dan sistem ICT atau yang belum diuji dari segi keselamatannya.

PERKAKASAN adalah komponen fizikal atau peralatan yang membentuk sistem komputer serta sistem rangkaian dan komunikasi seperti monitor, papan kekunci, unit pemprosesan, pelayan, pencetak, pengimbas, peranti, stesen kerja, media storan dan seumpamanya.

PREMIS KOMPUTER DAN KOMUNIKASI adalah premis yang digunakan untuk menempatkan semua perkakasan ICT.

SISTEM adalah terdiri daripada kesemua atau sebahagian daripada aplikasi dan perkakasan.

TEKNOLOGI MAKLUMAT adalah bidang yang meliputi penggunaan teknologi komputer dan telekomunikasi.

PENGENALAN

Dasar dan Garis Panduan Keselamatan ICT JKR mengandungi peraturan-peraturan yang perlu dibaca, difahami dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) JKR. Tujuan utama dasar dan garis panduan ini adalah untuk menerangkan kepada semua pengguna yang bertugas di JKR (termasuk kakitangan JKR, kakitangan bukan JKR, pembekal, pakar runding dan lain-lain) mengenai tanggungjawab dan peranan mereka dalam penggunaan dan perlindungan aset ICT JKR.

OBJEKTIF

Dasar dan Garis Panduan Keselamatan ICT JKR diwujudkan bagi menjamin kesinambungan urusan di JKR dan meminimumkan kesan insiden keselamatan.

PERNYATAAN DASAR ICT

Keselamatan boleh ditakrifkan sebagai keadaan yang bebas daripada risiko yang tidak boleh diterima. Keselamatan adalah suatu proses yang berterusan yang mana ianya melibatkan aktiviti berkala yang mesti dilakukan dari semasa ke semasa untuk menjamin keselamatan daripada ancaman yang sentiasa berubah-ubah.

Sebarang penggunaan aset ICT Kerajaan (perkakasan, perisian, data/maklumat, perkhidmatan dan manusia) selain daripada maksud dan tujuan yang telah ditetapkan adalah tidak dibenarkan.

PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar dan Garis Panduan Keselamatan ICT JKR adalah seperti berikut:

a. Akses Atas Dasar Perlu Mengetahui

   Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar perlu mengetahui sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk akses adalah

berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, mukasurat 15;

b. Hak Akses Minimum

Hak akses kepada pengguna hanya diberikan pada tahap yang paling minimum iaitu untuk membaca dan/atau melihat. Kelulusan khas adalah diperlukan untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu data atau maklumat;

c. Akauntabiliti

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

d. Pengasingan

Tugas mewujud, memadam, kemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian, pembangunan sistem dan pentadbir pengkalan data.

e. Pengauditan

Pengauditan adalah perlu untuk mengenalpasti insiden keselamatan atau keadaan yang mengancam keselamatan. Dengan ini aset ICT hendaklah mempunyai jejak audit.

f. Pemulihan

Pemulihan system amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Ianya juga dapat meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan dan mewujudkan Pelan Pemulihan Bencana atau Pelan Kesinambungan Perkhidmatan; dan

g. Pematuhan

Dasar dan Garis Panduan Keselamatan ICT JKR hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang bentuk perlanggaran ke atasnya yang boleh membawa kepada ancaman terhadap keselamatan ICT.

SKOP DASAR KESELAMATAN ICT JKR

Dasar dan Garis Panduan Keselamatan ICT JKR meliputi semua sumber-sumber dan aset-aset ICT berikut:

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

b. Perkakasan – semua peralatan dan periferal komputer tidak terhad kepada komputer peribadi, stesen kerja, kerangka utama dan alat-alat prasarana seperti punca kuasa, pendingin hawa dan UPS dan media storan seperti *thumb drives*, disket, CDROM, pita, cakera, pemacu cakera dan pemacu pita dan perlatan komunikasi seperti *server*, *gateway*, *router*, *switch* dan peralatan PABX;

c. Perisian – semua perisian dan applikasi yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data/maklumat. Ini termasuklah sistem pengoperasi, aturcara applikasi, perisian utiliti, perisian kolaboratif, perisian komunikasi dan fail-fail data.

d. Sumber manusia – semua pengguna (termasuk kakitangan JKR, kakitangan bukan JKR, pembekal, pakar runding dan lain-lain) yang bertugas di JKR atau menggunakan aset ICT JKR; dan

e. Perkhidmatan – semua perkhidmatan ICT yang ditawarkan atau digunakan tidak terhad kepada perkhidmatan *e-mail, internet*, telefon dan membaikpulih.

DASAR KESELAMATAN YANG BERKAITAN

Sebagai tambahan kepada dasar ini, semua kakitangan juga adalah terikat kepada dasar dan peraturan berikut:

a. Arahan Keselamatan;
b. Akta Kawasan Larangan dan Tempat Larangan 1959;
c. Akta Rahsia Rasmi 1972;
d. Akta Jenayah Komputer 1997;
e. Akta Tandatangan Digital 1997;

f. Pekeliling Am Bil. 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
g. Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
h. MyMIS;
i. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan;
j. Surat Pekeliling Am Bil. 6 Tahun 2005 – Garis Panduan Risiko Keselamatan Maklumat Sektor Awam;
k. Surat Pekeliling Am Bil. 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam;
l. Surat Ketua Setiausaha Negara – Langkah Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayer Di Agensi Agensi Kerajaan;
m. Surat Ketua Setiausaha Negara – Langkah Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain Lain Peralatan Komunikasi ICT Tanpa Kebenaran Kuasa Yang Sah Di Agensi-Agensi Kerajaan;
n. Undang-undang Malaysia Akta 680 – Akta Aktiviti Kerajaan Elektronik 2007; dan
o. Arahan Teknologi Maklumat 2007 (MAMPU).

PERUBAHAN MAKLUMAT

Sebarang maklumbalas atau perubahan berkaitan dengan dasar ini hendaklah ditujukan kepada ICTSO:

Nama	:	Pegawai Keselamatan ICT (ICTSO)
Alamat	:	Unit Rangkaian dan Keselamatan ICT, Bahagian Teknologi Maklumat, Cawangan Pengurusan Korporat, Tingkat 16, Ibu Pejabat JKR Malaysia, Jln Sultan Salahuddin, 50582 Kuala Lumpur.
Telefon	:	26967065
Faks	:	26112909
E-mel	:	ictso@jkr.gov.my

PERKARA 1
DASAR DAN GARIS PANDUAN KESELAMATAN ICT

0101 Pengurusan Dasar dan Garis Panduan Keselamatan ICT

Objektif:
Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan JKR dan perundangan yang berkaitan.

010101 Pelaksanaan Dasar

Kelulusan dan pelaksanaan dasar dan garis panduan ini adalah di bawah bidang kuasa KPKR dengan dibantu oleh Jawatankuasa Pemandu ICT JKR (JPICT) yang dipengerusikan oleh Ketua Pengarah Kerja Raya (KPKR).	KPKR

010102 Penyebaran Dasar

Dasar dan garis panduan ini perlu disebarkan kepada semua pengguna aset ICT JKR termasuk kakitangan JKR, kakitangan bukan JKR, pembekal, pakar runding dan lain-lain. Pengguna perlu menandatangani SURAT AKUAN PEMATUHAN DASAR DAN GARIS PANDUAN KESELAMATAN ICT JKR (Lampiran A).	ICTSO

010103 Penyelenggaraan Dasar

Dasar dan Garis Panduan Keselamatan ICT JKR adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar dan Garis Panduan Keselamatan ICT JKR: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Kemuka cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu	ICTSO

ICT (JPICT) JKR; dan c. Sebarang perubahan ke atas Dasar dan Garis Panduan Keselamatan ICT JKR yang telah dipersetujui hendaklah dimaklumkan kepada semua kakitangan JKR dan pengguna aset ICT JKR sama ada melalui risalah, pekeliling, papan buletin atau laman web intranet JKR.	
010104 Pengecualian Dasar	
Dasar dan Garis Panduan Keselamatan ICT JKR ini adalah terpakai kepada semua pengguna ICT JKR dan tiada pengecualian diberikan.	Pengguna

PERKARA 2
ORGANISASI KESELAMATAN ICT

0201 Infrastruktur Organisasi Keselamatan

Objektif:
Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar dan Garis Panduan Keselamatan ICT JKR.

020101 Ketua Pengarah Kerja Raya (KPKR)

Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut: a. Mempengerusikan/ melantik Pengerusi Gantian bagi Mesyuarat Jawatankuasa Pemandu ICT JKR; b. Memastikan pelaksanaan Dasar dan Garis Panduan Keselamatan ICT JKR; c. Berkuasa meluluskan pindaan Dasar dan Garis Panduan Keselamatan ICT JKR; d. Memastikan semua pengguna memahami peruntukan-peruntukan di bawah Dasar dan Garis Panduan Keselamatan ICT JKR; e. Memastikan semua pengguna mematuhi Dasar dan Garis Panduan Keselamatan ICT JKR; f. Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; g. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar dan Garis Panduan Keselamatan ICT JKR; dan h. Menggunakan budibicara berkaitan keselamatan ICT DENGAN SYARAT berpandukan prosedur keselamatan ICT yang berkuatkuasa.	KPKR

020102 Ketua Pegawai Maklumat (CIO)	
Ketua Pegawai Maklumat (CIO) yang dilantik oleh KPKR berperanan dan bertanggungjawab untuk: a. Membantu KPKR dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Mengesah dan mengawal Dokumen Dasar dan Garis Panduan Keselamatan ICT JKR; c. Merancang dan menyelaras pelaksanaan Dasar dan Garis Panduan Keselamatan ICT JKR; d. Memantau pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; e. Menentukan keperluan keselamatan ICT; e. Memantau keberkesanan pelaksanaan Dasar dan Garis Panduan Keselamatan ICT JKR dan pencapaian Objektif Dasar dan Garis Panduan Keselamatan ICT JKR; dan f. Melapor keberkesanan pelaksanaan Dasar dan Garis Panduan Keselamatan ICT JKR kepada KPKR.	CIO
020103 Pengurus ICT	
Ketua Bahagian Teknologi Maklumat (BTM) adalah merupakan Pengurus ICT JKR. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. Membentang laporan keselamatan ICT dalam Mesyuarat Jawatankuasa Pemandu ICT JKR; b. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan JKR; c. Menentukan kawalan akses semua pengguna terhadap aset ICT JKR; d. Memaklumkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO; e. Memaklumkan insiden keselamatan ICT kepada CIO dan	Pengurus ICT

melaporkan kepada Pasukan Tindakbalas Insiden Keselamatan ICT (GCERT) MAMPU jika perlu; dan f. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT JKR.	
020104 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Mengurus keseluruhan program-program keselamatan ICT JKR; b. Menguatkuasakan Dasar dan Garis Panduan Keselamatan ICT JKR; c. Memberi penerangan dan pendedahan berkenaan Dasar dan Garis Panduan Keselamatan ICT JKR kepada semua pengguna; d. Menyelaras garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar dan Garis Panduan Keselamatan ICT JKR; e. Menjalankan pengurusan dan penilaian risiko keselamatan ICT; f. Menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h. Memaklumkan insiden keselamatan ICT kepada CIO dan melaporkan kepada Pengurus ICT; i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; dan j. Memperakui proses pengambilan tindakan ke atas pengguna yang melanggar Dasar Keselamatan ICT JKR.	ICTSO
020105 Pentadbir Sistem ICT	
Pentadbir Sistem ICT bagi JKR ialah Ketua Unit di Bahagian Teknologi Maklumat. Semua Pentadbir Sistem ICT JKR berperanan dan	Pentadbir Sistem

bertanggungjawab terhadap perkara-perkara seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar dan Garis Panduan Keselamatan ICT JKR; c. Memantau aktiviti capaian harian pengguna; d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. Menyimpan dan menganalisis rekod jejak audit; dan f. Menyediakan laporan mengenai aktiviti capaian kepada Pengurus ICT atau ICTSO jika perlu.	
020106 Penyelaras ICT	
Penyelaras ICT Cawangan Negeri dan Daerah yang dilantik oleh CIO berperanan dan bertanggungjawab : a. Sebagai perantara di antara Bahagian Teknologi Maklumat, Pentadbir Sistem dan Pengguna di bawah kawalannya; b. Melaporkan dengan segera kepada Pentadbir Sistem ICT apabila terdapat kakitangan yang berhenti, bertukar, berkursus dan bercuti jangka panjang atau berlaku perubahan dalam bidang tugas; c. Menyimpan dan kemaskini rekod aset ICT JKR di bawah kawalannya; dan d. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera;	Penyelaras ICT
020107 Pengguna	
Pengguna adalah kakitangan dan bukan kakitangan JKR yang	Pengguna

menggunakan aset dan fasiliti ICT JKR. Peranan dan tanggungjawab pengguna adalah seperti berikut:

a. Membaca, memahami dan mematuhi Dasar dan Garis Panduan Keselamatan ICT JKR;
b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya;
c. Melaksanakan prinsip-prinsip Dasar dan Garis Panduan Keselamatan ICT;
d. Melaksanakan langkah-langkah perlindungan seperti berikut :-
   i. menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
   ii. memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa;
   iii. menentukan maklumat sedia untuk digunakan;
   iv. menjaga kerahsiaan kata laluan;
   v. mematuhi standard, prosedur dan garis panduan keselamatan yang ditetapkan; dan
   vi. memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan.
e. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Penyelaras ICT dengan segera;
f. Menghadiri program kesedaran mengenai keselamatan ICT; dan
g. Menandatangani SURAT AKUAN PEMATUHAN DASAR DAN GARIS PANDUAN KESELAMATAN ICT JKR (Lampiran A).

0202 Pihak Ketiga

Objektif:

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Mereka yang ada hubungan bisnes dengan JKR tidak terhad kepada Agensi lain, Pembekal, Kontraktor dan Perunding).

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Akses kepada aset ICT JKR perlu berlandaskan kepada perjanjian kontrak. Perkara-perkara berikut hendaklah diambilkira di dalam perjanjian yang dimeterai:- a. Dasar dan Garis Panduan Keselamatan ICT JKR; b. Tapisan Keselamatan; c. Perakuan Akta Rahsia Rasmi 1972; dan d. Hak Harta Intelek.	CIO, ICTSO, Pengurus ICT, Pentadbir Sistem dan Pihak Ketiga

PERKARA 3
PENGURUSAN ASET ICT

0301 Akauntabiliti Terhadap Aset ICT

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

030101 Inventori Aset ICT

Semua aset ICT JKR hendaklah direkodkan mengikut Tatacara Pengurusan Aset Alih Kerajaan. Ini termasuklah mengenal pasti aset, mengelas aset mengikut tahap sensitiviti aset berkenaan dan merekodkan maklumat seperti pemilik dan sebagainya. Setiap pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah kawalannya.	Pentadbir Sistem, Penyelaras ICT dan Pengguna

030102 Pentadbir Aset ICT

Pentadbir Aset ICT bagi JKR ialah Pegawai Aset ICT Cawangan/ Negeri/ Daerah yang dilantik. Semua Pentadbir Aset ICT JKR berperanan dan bertanggungjawab terhadap perkara-perkara seperti berikut: a. Pengelasan dan Pengendalian Maklumat dan dokumen; b. Mewujudkan dan menyelenggara inventori ICT (perisian dan perkakasan); c. Menyelaras dan melaksana penyenggaraan perisian dan perkakasan; d. Melaporkan kepada Pegawai Aset JKR mengikut arahan dalam Tatacara Pengurusan Aset Kerajaan.	Pentadbir Aset ICT

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. 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.	Pengguna
030202 Pengendalian Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambilkira 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,	Pengguna

penyampaian, pertukaran dan pemusnahan; dan g. Menjaga kerahsiaan mengenai keselamatan ICT dari diketahui umum.	
030203 Pengelasan dan Pengendalian Dokumen	
Bagi memastikan integriti maklumat, langkah-langkah pengurusan dokumentasi yang baik dan selamat seperti berikut hendaklah dipatuhi: a. Memastikan sistem dokumentasi atau penyimpanan maklumat adalah selamat dan terjamin; b. Menggunakan tanda atau label keselamatan seperti Rahsia Besar, Rahsia, Sulit, atau Terhad kepada dokumen; c. Menggunakan penyulitan (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik; dan d. Memastikan dokumen yang mengandungi bahan atau maklumat sensitif diambil segera dari pencetak.	Pengguna

PERKARA 4
KESELAMATAN SUMBER MANUSIA

0401 Keselamatan ICT Dalam Tugas Harian

Objektif:
Meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT JKR oleh pengguna.

040101 Peranan dan Tanggungjawab Pengguna

Pengguna mestilah jelas, patuh dan melaksanakan peranan dan tanggungjawabnya terhadap keselamatan ICT. Keselamatan ICT merangkumi tanggungjawab pengguna dalam menyedia dan memastikan perlindungan ke atas semua aset atau sumber ICT yang digunakan di dalam melaksanakan tugas harian.	Pengguna

040102 Terma dan Syarat Perkhidmatan

Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan serta peraturan semasa yang berkuat kuasa.	Pengguna

040103 Perakuan Akta Rahsia Rasmi dan Pematuhan Lain-lain Peraturan yang Berkuatkuasa

Semua warga JKR yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972. Pihak ketiga yang terlibat hendaklah mematuhi semua peruntukan dalam Dasar dan Garis Panduan Keselamatan ICT JKR. Pihak ketiga yang menggunakan dan mengakses aset ICT JKR perlu menandatangani borang akuan menyimpan rahsia Kerajaan (Lampiran B).	Pengguna dan pihak ketiga

0402 Semasa Berkhidmat	
Objektif: Memastikan semua pengguna sedar dan bertanggungjawab mengenai ancaman keselamatan maklumat bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT JKR.	
040201 Tanggungjawab Pengurusan	
a. Memastikan semua pengguna menguruskan keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh JKR. b. Memastikan latihan kesedaran yang berkaitan mengenai pengurusan keselamatan ICT JKR diberikan semua pengguna JKR dan sekiranya perlu diberikan kepada pihak ketiga yang tidak terhad kepada kontraktor, pembekal, pakar runding dan pihak-pihak lain dari semasa ke semasa.	CIO, Pengurus ICT dan ICTSO
040202 Kesedaran Keselamatan ICT	
Setiap pengguna di JKR perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah preventif yang boleh mengurangkan ancaman keselamatan ICT JKR.	ICTSO dan Pengguna
040203 Tindakan Tatatertib	
Perlanggaran Dasar dan Garis Panduan Keselamatan ICT JKR boleh dikenakan tindakan tatatertib mengikut tatacara pengurusan tindakan	Pengguna

tatatertib, salah laku dan jenayah yang berkuatkuasa.	
0403 Bertukar atau Tamat Perkhidmatan	
Objektif: Memastikan semua pengguna yang bertukar atau tamat perkhidmatan diuruskan dengan teratur bagi meminimumkan risiko keselamatan ICT.	
040301 Pertukaran dan Penamatan Perkhidmatan	
Segala urusan penamatan perkhidmatan ICT bagi pengguna yang bertukar, bersara atau tamat perkhidmatan perlu dilakukan dengan teratur dengan mengambilkira perkara-perkara berikut: a. Memastikan semua aset ICT dikembalikan kepada JKR mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan proses maklumat mengikut peraturan yang ditetapkan oleh JKR dan/atau terma perkhidmatan; c. Memastikan pengguna yang bertukar Cawangan/ Negeri/ Bahagian tidak dibenarkan membawa bersama aset ICT ke tempat baru; dan d. Menandatangani borang akuan tidak mendedahkan maklumat-maklumat asset ICT JKR selepas penamatan perkhidmatan di JKR (Lampiran C).	Pengurus ICT dan Pentadbir Sistem

PERKARA 5
KESELAMATAN FIZIKAL

0501 Keselamatan Fizikal

Objektif:

Mencegah akses fizikal yang tidak dibenarkan, kerosakan dan gangguan kepada premis dan maklumat Jabatan.

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 dikenalpasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; b. Memperkukuhkan tingkap dan pintu serta dikunci untuk mengawal kemasukan; c. Memperkukuhkan dinding dan siling; d. Memasang alat penggera atau kamera litar; e. Menghadkan jalan keluar masuk ke premis JKR; f. Mengadakan kaunter kawalan; g. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; dan h. Mewujudkan perkhidmatan kawalan keselamatan.	CIO dan ICTSO

050102 Kawalan Masuk Fizikal

Pengguna a. Setiap pengguna JKR hendaklah memakai atau mengenakan pas keselamatan pengguna sepanjang waktu bertugas; b. Semua pas keselamatan pengguna hendaklah diserahkan balik	Pengguna dan Pelawat

kepada Jabatan apabila pengguna bertukar, berhenti atau bersara; c. Hanya pengguna yang diberi kebenaran sahaja boleh mencapai atau menggunakan aset ICT JKR; dan d. Kehilangan pas mestilah dilaporkan dengan segera; Pelawat a. Setiap pelawat hendaklah mendaftar di pintu utama JKR terlebih dahulu; b. Setiap pelawat mestilah mendapatkan Pas Keselamatan Pelawat di pintu masuk ke kawasan atau tempat berurusan dan perlu dikembalikan semula selepas tamat lawatan; c. Kehilangan pas mestilah dilaporkan dengan segera;	
050103 Kawasan Larangan	
Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. "Kawasan Larangan" ertinya mana-mana kawasan yang diisytiharkan sebagai kawasan larangan mengikut Seksyen 4 Akta Kawasan Larangan dan Tempat Larangan 1959 (Akta 298). Kawasan larangan tidak terhad kepada perkara-perkara berikut: a. Diletakkan papan tanda/ menampal pelekat di pintu masuk kawasan larangan; b. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; c. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan KECUALI bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, serta mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai; d. Mengambil gambar, video, audio adalah dilarang KECUALI dengan	Pengguna

kebenaran pihak Pengurusan Jabatan, CIO, Pengurus ICT atau ICTSO; dan e. Semua penggunaan peralatan yang melibatkan penghantaran, kemaskini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	
0502 Keselamatan Persekitaran	
Objektif: Melindungi aset ICT JKR dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050201 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis samada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk terlebih dahulu kepada Ketua Pegawai Keselamatan JKR. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah di ambil: a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna adalah dilarang merokok atau menggunakan peralatan	Pengurus ICT, ICTSO dan Pentadbir Sistem

memasak seperti cerek elektrik berhampiran peralatan komputer; g. Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya sekali dalam setahun; dan h. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu.	
050202 Bekalan Kuasa	
a. Bekalan elektrik dan penyaman udara mestilah berasingan dari bekalan bangunan/ tingkat; b. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; c. Peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa berterusan; d. Genset mestilah disediakan secara khusus untuk Pusat Data dan berasingan dari bekalan kepada bangunan/ tingkat. Penjaga jentera dipertanggungjawabkan untuk memastikan genset berada dalam keadaan siapsiaga; dan e. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Pengurus ICT, ICTSO dan Pentadbir Sistem
050203 Prosedur Kecemasan	
a. Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan Keselamatan MAMPU dan CGSO (*The Chief Government Security Office*); b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan Jabatan (PKJ) yang dilantik; dan c. Mengadakan latihan *fire drill* mengikut jadual.	Pengguna

050204 Keselamatan Pengkabelan	
Kabel hendaklah dilindungi kerana boleh menjadi punca maklumat terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping*; d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat; dan e. Pelan susun atur perlu dikemukakan kepada Bahagian Teknologi Maklumat sekiranya berlaku kerja-kerja pengkabelan baru.	Pentadbir Sistem dan Pentadbir Rangkaian
0503 Keselamatan Peralatan	
Objektif: Melindungi peralatan ICT JKR dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
050301 Peralatan ICT	
Perlatan ICT perlu dilindungi kerana boleh menjadi punca maklumat terdedah. Langkah-langkah keselamatan yang perlu dipatuhi adalah seperti berikut : a. Pengguna hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Pengguna bertanggungjawab sepenuhnya ke atas komputer masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna dilarang sama sekali menambah, menanggal atau	Pengguna

mengganti sebarang perkakasan ICT yang telah ditetapkan;

d. Pengguna adalah bertanggungjawab untuk melapor di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

e. Pengguna perlu memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan;

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

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

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

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

j. Peralatan ICT yang hendak dibawa keluar dari premis JKR, perlulah mendapat kelulusan Pengurus ICT dan direkodkan bagi tujuan pemantauan;

k. Peralatan ICT yang hilang hendaklah dilaporkan kepada Pegawai Aset dan dimaklumkan kepada ICTSO dengan segera;

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

m. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih;

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

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

p. Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja;

q. Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dipadamkan apabila meninggalkan pejabat; dan r. Sebarang bentuk penyelewengan atau salahguna peralatan ICT hendaklah dilaporkan kepada ICTSO.	
050302 Penyelenggaraan Peralatan/ Perkakasan	
Peralatan/ Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan dan integriti: a. Semua peralatan/ perkakasan yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b. Peralatan/ Perkakasan hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; dan c. Semua peralatan/ perkakasan hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan.	Pegawai Aset dan Pentadbir Sistem
050303 Keselamatan Peralatan Untuk Kegunaan Di Luar Pejabat/ Premis	
Peralatan yang dipinjam untuk kegunaan di luar pejabat/ premis adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan: a. Peralatan, maklumat atau perisian yang dibawa keluar pejabat/ premis mestilah mendapat kelulusan Pegawai Aset ICT Bahagian/ Cawangan/ Negeri dan tertakluk kepada tujuan yang dibenarkan; b. Aktiviti peminjaman dan pemulangan peralatan mestilah direkodkan; c. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan d. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Pengguna

050304 Pelupusan Perkakasan	
Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan JKR: a. Semua kandungan peralatan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding* atau pembakaran; b. Maklumat lanjut pelupusan bolehlah merujuk kepada Tatacara Pengurusan Aset terkini; dan c. Peralatan ICT yang akan dilupuskan sebelum dipindahmilik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat.	Pegawai Aset, Pentadbir Sistem dan Pengguna

PERKARA 06
PENGURUSAN OPERASI DAN KOMUNIKASI

0601 Pengurusan Prosedur Operasi

Objektif:
Memastikan perkhidmatan dan pemprosesan maklumat dapat berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.

060101 Pengendalian Prosedur

Semua prosedur operasi yang diwujud, dikenalpasti dan masih diguna pakai hendaklah didokumenkan dengan jelas lagi teratur, dikemaskini, disimpan dan dikawal. Setiap perubahan kepada sistem dan kemudahan pemprosesan maklumat mestilah dikawal. Setiap prosedur mestilah mengandungi arahan-arahan yang lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; Setiap prosedur bagi aktiviti *system housekeeping* seperti *backup*, penyenggaraan peralatan ICT dalam Bilik Server/ Pusat Data dan pengurusan pengendalian mel *elektronik* hendaklah direkodkan; Semua prosedur hendaklah dikemaskini dari semasa ke semasa atau mengikut keperluan. Tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset organisasi.	Pentadbir Sistem dan Pengguna

Kemudahan ICT untuk pembangunan, pengujian dan operasi mestilah diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah kepada sistem yang sedang beroperasi.	
060102 Kawalan Perubahan	
Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah dipantau dan mendapat kebenaran daripada pegawai bertanggungjawab atau pemilik aset ICT terlebih dahulu. Aktiviti-aktiviti seperti memasang, menyenggara, menghapus dan mengemaskini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Pengguna
060103 Prosedur Pengurusan Insiden	
Bagi memastikan tindakan menangani insiden keselamatan ICT diambil dengan cepat, teratur dan berkesan, prosedur pengurusan insiden mestilah mengambil kira kawalan-kawalan berikut: a. Mengenalpasti semua jenis insiden keselamatan ICT seperti gangguan perkhidmatan yang disengajakan, pemalsuan identiti dan pengubahsuaian perisian tanpa kebenaran; b. Menyedia pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; c. Menyimpan jejak audit dan memelihara bahan bukti;	ICTSO dan Pentadbir Sistem

d. Menyediakan tindakan pemulihan segera; dan e. Melaporkan kepada pihak pengurusan atasan.	
0602 Perancangan dan Penerimaan Sistem	
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060201 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambilkira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. Penggunaan peralatan mestilah dipantau, ditala (*tuned*) dan perancangan perlu dibuat bagi memastikan prestasi sistem di tahap optimum.	Pentadbir Sistem dan ICTSO
060202 Penerimaan Sistem	
Semua sistem baru (termasuklah sistem yang dikemaskini, dinaiktaraf atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui seperti berikut: a. Memenuhi kapasiti dan prestasi yang ditetapkan; b. Prosedur *error recovery* dan *restart procedures* serta pelan kecemasan; c. Persediaan dan pengujian berterusan bagi mengenalpasti piawaian dan prosedur; d. Persetujuan kawalan keselamatan;	Pentadbir Sistem dan ICTSO

e. Dokumen (manual) prosedur yang berkesan; dan f. Latihan untuk menggunakan sistem baru.	
0603 Perisian Berbahaya	
Objektif : Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti *virus, trojan* dan sebagainya.	
060301 Perlindungan dari Perisian Berbahaya	
Dalam proses pengendalian perisian dan maklumat, perkara-perkara berikut perlu diambil perhatian: a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti *anti virus* atau sistem pengesanan pencerobohan (IDS) dan mengikut prosedur penggunaan yang betul dan selamat; b. Memasukkan klausa tanggungan di dalam mana-mana kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baikpulih sekiranya perisian tersebut mengandungi program berbahaya; c. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; d. Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus; e. Memasang dan menggunakan hanya perisian yang berdaftar dan dilindungi di bawah undang-undang bertulis yang berkuatkuasa; f. Mengimbas semua perisian atau sistem dengan *anti virus* sebelum menggunakannya; g. Memastikan *pattern anti virus* sentiasa dikemaskini; h. Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; dan	Pentadbir Sistem dan Pengguna

i. Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya;	
060302 Perlindungan dari *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pentadbir Sistem
0604 *Housekeeping*	
Objektif: Melindungi integriti maklumat dan perkhidmatan komunikasi agar boleh diakses pada bila-bila masa.	
060401 *Backup*	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Aktiviti *backup* hendaklah direkod dan disimpan di lokasi yang berlainan. Perkara-perkara berikut hendaklah diambil perhatian: a. Membuat *backup* ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat *backup* ke atas semua maklumat secara berkala; c. Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; dan d. Menyimpan sekurang-kurangnya tiga (3) generasi *backup*.	Pentadbir Sistem

060402 Sistem Log	
Sistem log perlu diwujudkan bagi merekodkan aktiviti harian pengguna ICT setiap hari. Langkah-langkah yang perlu dipertimbangkan adalah : a. Memastikan sistem log disimpan sekurang-kurangnya selama satu (1) tahun; b. Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan baikpulih dengan segera; dan c. Sekiranya wujud aktiviti-aktiviti tidak sah seperti kecurian maklumat dan pencerobohan, hendaklah dilaporkan segera kepada ICTSO.	Pentadbir Sistem ICT
0605 Pengurusan Rangkaian	
Objektif: Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
060501 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Berikut adalah langkah-langkah yang perlu dipertimbangkan: a. Sebarang kerja-kerja operasi rangkaian dan komputer perlu mendapat kebenaran daripada Pengurus ICT untuk mengelakkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e. *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem	Pentadbir Sistem dan Pengguna

yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh pentadbir sistem; f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan JKR; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang sama sekali dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO; h. Memasang perisian *Intrusion Detection System (IDS) atau Intrusion Prevention System (IPS)* bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat JKR; i. Memasang *Web Content Filter* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan"; j. Sebarang penyambungan rangkaian yang bukan di bawah Kawalan JKR Malaysia hendaklah mendapat kebenaran ICTSO; k. Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum; dan l. Semua pengguna hanya dibenarkan menggunakan rangkaian dalaman JKR sahaja. Penggunaan modem persendirian seperti *broadband* adalah dilarang sama sekali ke atas aset ICT Jabatan.	
0606 Pengurusan Media	
Objektif: Melindungi aset ICT dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.	
060601 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Pengguna

060602 Prosedur Pengendalian Media	
Pengendalian media perlu mengambilkira perkara-perkara berikut: a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Menghadkan dan menentukan capaian media kepada pengguna yang sah sahaja; c. Menghadkan pengedaran maklumat atau media untuk tujuan yang dibenarkan; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat rahsia rasmi hendaklah dihapus atau dimusnahkan mengikut prosedur yang betul dan selamat apabila tidak diperlukan.	Pengguna
060603 Keselamatan Sistem Dokumentasi	
Sistem dokumentasi perlu mengambilkira perkara-perkara berikut: a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyediakan dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Pengguna
0607 Keselamatan Komunikasi	
Objektif: Melindungi aset ICT melalui sistem komunikasi yang selamat.	

060701 Internet

a. Laman-laman yang boleh dilayari, dilanggan dan diguna adalah berbentuk akademik dan pengetahuan serta untuk urusan kerja harian. Laman yang berbentuk keganasan, lucah, hasutan dan yang boleh menimbul atau membawa kepada keganasan, keruntuhan akhlak dan kebencian adalah tidak dibenarkan sama sekali; b. Capaian laman yang berbentuk hiburan, hobi atau *leisure* tidak dibenarkan termasuk laman *game online*, *radio online* dan *video streaming*; c. Melayari internet tanpa tujuan atau meninggalkan capaian internet *unattended* adalah amat tidak beretika dan tidak digalakkan kerana ianya boleh menyebabkan kesesakan rangkaian JKR; d. Ketua Pengarah atau Wakil Pengurusan berhak menapis, menghalang dan menegah penggunaan mana-mana laman web yang dianggap tidak sesuai; e. Pengguna dilarang mengganggu atau menceroboh laman web mana-mana Jabatan, Organisasi atau Negara; f. Pengguna dilarang memasuki, menyalin, menciplak, mencetak dan menyebarkan maklumat daripada Internet yang menyalahi undang-undang negara; g. Pengguna tidak dibenarkan mencapai atau cuba mencapai sumber elektronik (data, paparan, *keystrokes*, fail atau media storan) dalam sebarang bentuk yang dimiliki oleh pengguna yang lain tanpa mendapat kebenaran atau kelulusan pengguna terbabit terlebih dahulu. Ini termasuk membaca, menyalin, menukar, merosak atau memadam data, program dan perisian. Penggunaan penganalisis rangkaian (*network analyzer*) atau pengintip (*sniffer*) adalah dilarang sama sekali. h. Pengguna yang mencapai sesuatu perkhidmatan yang perlu dibayar (contohnya pangkalan data *online* komersial), hendaklah bertanggungjawab ke atas segala bayaran yang dikenakan. i. Maklumat lanjut mengenai keselamatan Internet hendaklah merujuk kepada PKPA Bil. 1 Tahun 2003 bertajuk “Garis Panduan	Pengguna

Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".

Penggunaan jaringan media sosial tanpa kawalan akan menyebabkan gangguan kepada capaian ke atas perkhidmatan online yang disediakan kepada pelanggan. Berikut adalah amalan terbaik dalam penggunaan jaringan media sosial yang perlu dipatuhi:

Pegawai Bertanggungjawab Mengendalikan Laman Web Media Sosial Agensi

a. Memastikan kandungan yang tidak bercanggah dengan dasar Kerajaan;
b. Menjadikan laman web jaringan sosial sebagai media dalam mempromosi dan memberi publisiti kepada perkara-perkara yang berkaitan dengan Kerajaan;
c. Memastikan kandungan dan kesesuaiannya serta yang mempunyai kepentingan untuk dimaklumkan kepada orang awam;
d. Memastikan kekerapan pengemaskinian maklumat dan memastikan ia relevan;
e. Menghapuskan kandungan dan maklumat yang diterima dari orang awam yang tidak relevan dengan aktiviti agensi;
f. Memastikan pautan dan kandungan antara laman web jaringan sosial dan laman web rasmi agensi hendaklah jelas dan tidak bertindih;
g. Menggunakan logo rasmi agensi di dalam laman web jaringan sosial;
h. Menggunakan e-mel rasmi di dalam profil laman web jaringan sosial;
i. Menggunakan foto dan/atau video yang dapat memperjelaskan mesej yang hendak disampaikan dalam keadaan yang bersesuaian;
j. Memasukkan penerangan terhadap foto dan/atau video yang digunakan bagi membantu carian oleh pengguna;
k. Menggunakan perkataan hak cipta terpelihara pada semua kandungan foto dan/atau video;
l. Menggunakan ayat yang ringkas, padat, tepat dan jelas

maksudnya; dan m. Menyediakan penyataan penafian (*disclaimer*) terhadap sebarang kerosakan sekiranya dialami oleh pengguna semasa menggunakan laman web jaringan sosial. Pengguna Di Agensi a. Mencapai laman web jaringan sosial yang hanya berkaitan dengan urusan rasmi agensi pada waktu pejabat; b. Menggunakan ayat yang lengkap dan jelas maksudnya; c. Tidak memaparkan isu-isu sensitif seperti agama, politik dan perkauman serta yang berunsur fitnah atau hasutan; d. Tidak memaparkan kenyataan-kenyataan yang boleh menjejaskan imej Kerajaan; dan e. Tidak menggunakan laman web jaringan sosial untuk mengaibkan individu tertentu. Pentadbir Rangkaian a. Memastikan pengurusan *content filtering* sentiasa berfungsi dalam menapis capaian ke laman web jaringan sosial yang tiada kaitan dengan kegunaan rasmi agensi; dan b. Memantau serta menganalisis transaksi capaian pengguna agensi ke atas laman web jaringan sosial luar agar tidak mengganggu prestasi rangkaian di agensi.	
060702 Mel Elektronik	
Penggunaan e-mel tanpa kawalan boleh menyebabkan gangguan kepada perkhidmatan JKR. Perkara-perkara berikut perlu diambilkira bagi memantapkan pengurusan dan penggunaan e-mel JKR: a. Akaun mel elektronik (e-mel) JKR hanya diperuntukkan kepada pegawai dan kakitangan yang mempunyai maklumat di dalam Sistem Maklumat Kakitangan Jabatan semasa. b. Pengguna hanya boleh menggunakan akaun atau alamat e-mel yang diperuntukkan oleh JKR sahaja. Penggunaan akaun milik orang lain	Pengguna

tidak dibenarkan;

c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan;

d. Akaun e-mel rasmi JKR hanyalah untuk kegunaan urusan rasmi sahaja. Sebarang penyalahgunaan e-mel akan di ambil tindakan tatatertib mengikut peraturan semasa yang berkuatkuasa.

e. Pengguna hendaklah memastikan alamat e-mel persendirian seperti e-mel yahoo, gmail, streamyx dan sebagainya tidak boleh digunakan untuk tujuan rasmi;

f. Pengguna dinasihatkan menggunakan fail kepilan, sekiranya perlu tidak melebihi sepuluh (10) MB semasa penghantaran. Kaedah pemampatan untuk mengurangkan saiz adalah disarankan;

g. Pengguna hendaklah mengelak dari membuka e-mel daripada penghantar yang tidak diketahui atau diragui;

h. Pengguna hendaklah mengenal pasti dan mengesahkan identiti pengguna yang berkomunikasi dengannya sebelum meneruskan transaksi maklumat melalui e-mel;

i. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan;

j. Pengguna hendaklah menentukan tarikh dan masa sistem komputer adalah tepat;

k. Pengguna adalah dilarang menggunakan apa-apa cara pun untuk menyamar sebagai penghantar e-mel yang sah. Sebarang penyalahgunaan hendaklah dilaporkan kepada ICTSO;

l. Akaun e-mel yang tidak aktif selama 3 bulan akan *disable* dan seterusnya akan dihapuskan selepas 6 bulan;

m. Mengambil tindakan segera dan memberi maklum balas terhadap e-mel yang diterima;

n. Sekiranya pengguna akan bercuti atau berkursus dalam jangkamasa yang panjang atau bertukar tempat kerja, makluman kepada pentadbir e-mel perlu dilakukan supaya kerja-kerja penyenggaraan e-mel dapat dilaksanakan;

o. Pengguna tidak boleh melibatkan diri dalam aktiviti penghantaran mel sampah (*flaming*), mel bom (*mail bombing*) dan mel spam

(*spamming*); dan p. Pengguna hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing. Maklumat lanjut mengenai keselamatan dan garis panduan e-mel hendaklah merujuk kepada: a. PKPA Bil 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan."; dan b. E-mel edaran Ketua Pengarah MAMPU rujukan MAMPU.BDPICT.700-2/36 (1) bertarikh 07 Januari 2010 "Pemantapan Penggunaan Dan Pengurusan E-Mel Di Agensi-Agensi Kerajaan."	

PERKARA 07
KAWALAN CAPAIAN

0701 Dasar Kawalan Capaian

Objektif:
Memahami dan mematuhi keperluan keselamatan dalam mengawal capaian ke atas aset ICT JKR.

070101 Keperluan Kawalan Capaian

Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna yang berbeza. Ia perlu direkodkan, dikemaskini dan menyokong dasar kawalan capaian pengguna sedia ada: a. Kawalan capaian ke atas capaian aset ICT mengikut keperluan keselamatan dan peranan pengguna; b. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d. Kawalan ke atas kemudahan pemprosesan maklumat.	ICTSO dan Pentadbir Sistem

0702 Pengurusan Capaian Pengguna

Objektif :
Mengawal capaian pengguna ke atas aset ICT Jabatan.

070201 Akaun Pengguna

Pengguna adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, langkah-	Pengguna dan Pentadbir

langkah berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh Jabatan sahaja boleh digunakan; b. Akaun pengguna mestilah unik; c. Akaun pengguna sistem aplikasi yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Pentadbir sistem ICT boleh membeku atau menamatkan akaun pengguna atas sebab-sebab berikut; i. pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan; ii. Melanggar peraturan yang telah ditetapkan dalam Dasar dan Garis Panduan Keselamatan ICT; iii. Bertukar bidang tugas kerja (untuk sistem aplikasi); iv. Bertukar keluar ke agensi lain (kecuali staf JKR); v. Bersara; atau vi. Ditamatkan perkhidmatan.	Sistem
070202 Jejak Audit	
Jejak audit akan merekodkan semua aktiviti sistem yang digunapakai oleh pengguna. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi: a. Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b. Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan	Pentadbir Sistem

c. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Pentadbir sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
070203 Hak Capaian	
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem
070204 Pengurusan Katalaluan	
Pemilihan, penggunaan dan pengurusan katalaluan sebagai laluan utama bagi mencapai maklumat dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JKR seperti berikut: a. Dalam apa jua keadaan dan sebab, katalaluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna hendaklah menukar katalaluan apabila disyaki berlakunya kebocoran katalaluan atau dikompromi; c. Panjang katalaluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan aksara khusus; d. Katalaluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; e. Katalaluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang gunasama; f. Katalaluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g. Kuatkuasakan pertukaran katalaluan semasa login kali pertama atau selepas login kali pertama atau selepas katalaluan diset semula; h. Katalaluan hendaklah berlainan daripada pengenalan identiti	Pentadbir Sistem dan Pengguna

pengguna; i. Tentukan had masa pengesahan dengan maksimum selama lima (5) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi perlu ditamatkan; j. Katalaluan perlu ditukar dalam tempoh satu (1) tahun; dan k. Mengelakkan penggunaan semula tiga (3) katalaluan yang terbaru.	
070205 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kemudahan katalaluan *screen saver* atau log keluar apabila meninggalkan komputer; b. Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan c. Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Pengguna
0703 Kawalan Capaian Maklumat dan Aplikasi	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
070301 Capaian Maklumat dan Aplikasi	
Capaian sistem dan aplikasi di JKR adalah terhad kepada pengguna dan tujuan yang dibenarkan sahaja. Untuk memastikan kawalan capaian	ICTSO dan Pentadbir

sistem dan aplikasi adalah kukuh, langkah-langkah berikut hendaklah dipatuhi: a. Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan sensitiviti maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (log) bagi mengesan aktiviti-aktiviti yang tidak diingini; c. Memaparkan notis amaran pada skrin komputer pengguna sebelum memulakan capaian bagi melindungi maklumat dari sebarang bentuk penyalahgunaan; d. Menghadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau katalaluan pengguna akan disekat; e. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan f. Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah digalakkan. Walaubagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Sistem

0704 Peralatan Komputer Mudah Alih
Objektif : Memastikan keselamatan maklumat apabila menggunakan kemudahan atau peralatan komputer mudah alih.
070401 Penggunaan Peralatan Komputer Mudah Alih

a. Merekodkan aktiviti keluar masuk penggunaan peralatan komputer mudah alih bagi mengesan kehilangan atau pun kerosakan; b. Komputer mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan; dan	Pengguna

c. Semua peralatan mudah alih seperti notebook, PDA dan sebagainya yang digunakan di dalam rangkaian JKR perlulah mematuhi syarat-syarat berikut: i. Memastikan perisian antivirus dan penampalan (*patches*) dipasang dan dikemaskini (*updated virus pattern & patches*); ii. Keselamatan peralatan adalah di bawah tanggungjawab pengguna; iii. Memastikan tiada perisian yang boleh mengganggu gugat keselamatan rangkaian JKR; iv. Penggunaan adalah atas urusan rasmi sahaja.	
0705 Kawalan Capaian Sistem Pengoperasian	
Objektif: Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
070501 Capaian Sistem Pengoperasian	
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Kemudahan keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti, komputer atau lokasi bagi setiap pengguna yang dibenarkan; dan b. Merekodkan capaian yang berjaya dan gagal. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a. Mengesahkan pengguna yang dibenarkan; b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem.	Pentadbir Sistem

Perkara-perkara yang perlu dipatuhi adalah seperti 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; c. Menghadkan dan mengawal penggunaan program; dan d. Menghadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
070502 Kad Pintar	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali; dan d. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada pemilik sistem.	

PERKARA 08
PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0801 Keselamatan Dalam Membangunkan Sistem Dan Aplikasi

Objektif:

Memahami dan mematuhi keperluan keselamatan dalam mencapai dan menggunakan aset ICT JKR.

080101 Keperluan Keselamatan

a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambilkira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat. Segala perolehan sistem hendaklah berpandukan kepada pekeliling dan garis panduan yang berkaitan (Kementerian Kewangan, MAMPU & Jabatan); b. Keperluan keselamatan hendaklah dikenal pasti, dipersetujui dan didokumenkan terlebih dahulu semasa fasa mengkaji keperluan projek sebelum pembangunan dan pelaksanaan aplikasi jabatan. c. 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; 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. e. Aplikasi perlu mengandungi semakan pengesahan (*validation and verification*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan.	Pentadbir Sistem, Pemilik Sistem dan ICTSO

f. Penggunaan alamat *Universal Resource Locator* (URL) berkaitan dengan jabatan hendaklah menggunakan nama domain jkr.gov.my atau jkr.my. Penggunaan nama domain lain perlu mendapat kebenaran Pengurus ICT Jabatan. g. *Outsourced hosting* tidak dibenarkan menggunakan domain jkr.gov.my atau jkr.my.	
0802 Kriptografi	
Objektif: Melindungi kerahsiaan, integriti dan kesahihan maklumat.	
080201 Penyulitan (*encryption*)	
Pengguna hendaklah membuat penyulitan ke atas maklumat sensitif atau maklumat rahsia rasmi pada setiap masa.	Pengguna
080202 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pengguna
080203 Pengurusan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Pengguna

0803 Fail Sistem	
Objektif: Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.	
080301 Kawalan Fail Sistem	
a. Proses pengemaskinian fail fizikal dan fail sistem hanya boleh dilakukan oleh pentadbir sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau aturcara sistem yang telah dikemaskini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau aturcara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan d. Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem dan Pemilik Sistem
0804 Keselamatan Dalam Proses Pembangunan dan Sokongan	
Objektif: Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
080401 Kawalan Perubahan	
a. Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai. b. Akses kepada kod sumber program hendaklah dihadkan kepada pengguna yang dibenarkan sahaja untuk mencegah fungsi aplikasi ditambah tanpa izin dan bagi mengelakkan perubahan yang tidak	Pentadbir Sistem dan Pemilik Sistem

disengajakan.	
080402 Pembangunan Perisian Secara *Outsource*	
Pembangunan aplikasi secara outsource perlu diselia dan dipantau oleh pemilik sistem. Kod sumber (*source code*) bagi semua aplikasi adalah menjadi hak milik Jabatan.	Pentadbir Sistem dan Pemilik Sistem

PERKARA 09
PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901 Mekanisme Pelaporan Insiden Keselamatan ICT

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

090101 Mekanisme Pelaporan

Pengguna

Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar Dasar dan Garis Panduan Keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO 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. Katalaluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan, atau disyaki hilang, dicuri atau didedahkan;
d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan
e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka.

Prosedur pelaporan insiden keselamatan ICT berdasarkan:

a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan
b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan

Komunikasi Sektor Awam.	
0902 Pengurusan Maklumat Insiden Keselamatan ICT	
Objektif: Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
090201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada JKR. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: a. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; d. Menyediakan tindakan pemulihan segera; dan e. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	Pengurus ICT, ICTSO dan Pentadbir Sistem

PERKARA 10
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001 Dasar Kesinambungan Perkhidmatan

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

100101 Pengurusan Kesinambungan Perkhidmatan

Pengurusan Kesinambungan Perkhidmatan (*Business Continuity Management - BCM*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Perkara-perkara berikut perlu diberi perhatian: a. Mengenalpasti semua tanggungjawab dan prosedur kecemasan dan pemulihan; i. Pelan tindakan (menilai situasi, siapa yang terlibat); ii. Prosedur kecemasan yang bersangkut paut dengan agensi keselamatan (polis, bomba dll); iii. *Fallback procedure* – menyediakan lokasi sementara jika perkhidmatan tidak dapat diperolehi degan segera (cth: *backup* di komputer sendiri); dan iv. *Resumption procedures*. b. Semua pengurusan strategi kesinambungan perkhidmatan mestilah mendapat persetujuan dan pengesahan Jawatankuasa Pemandu ICT; c. Adalah menjadi tanggungjawab jabatan untuk melantik pegawai-pegawai yang bertanggungjawab untuk memastikan Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan* - BCP); d. Mendokumentasikan proses dan prosedur yang telah dipersetujui untuk mengelakkan risiko yang akan menjejaskan kesinambungan	Pengurus ICT dan pegawai-pegawai yang terlibat

perkhidmatan; e. Mengadakan program kesedaran dan latihan tentang proses dan prosedur kesinambungan perkhidmatan secara berterusan dan efektif; f. Membuat jadual pengujian dan mengemaskini (penambahbaikan) pelan BCP sekurang-kurangnya setahun sekali; g. Membuat *backup*; h. Membuat pemeriksaan semula (*restore data*) untuk kenalpasti data tersebut masih boleh digunapakai atau tidak dengan kekerapan sekurang-kurangnya setahun sekali, mengikut keperluan pengguna atau arahan dari pihak atasan; i. Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama.	

PERKARA 11
PEMATUHAN

1101 Pematuhan dan Keperluan Perundangan

Objektif:
Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar dan Garis Panduan Keselamatan ICT JKR.

110101 Pematuhan Dasar

Setiap pengguna di JKR hendaklah membaca, memahami dan mematuhi Dasar dan Garis Panduan Keselamatan ICT dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuatkuasa. Semua aset ICT di JKR termasuk maklumat yang disimpan di dalamnya adalah hakmilik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Penggunaan dan pengendalian data digital perlu mematuhi prosedur-prosedur yang telah ditetapkan.	Pengguna

110102 Keperluan Perundangan

Keperluan perundangan atau peraturan-peraturan lain yang perlu dipatuhi oleh pengguna JKR: a. Arahan Keselamatan; b. Akta Kawasan Larangan dan Tempat Larangan 1959; c. Akta Rahsia Rasmi 1972; d. Akta Jenayah Komputer 1997; e. Akta Tandatangan Digital 1997; f. Pekeliling Am Bil. 3 Tahun 2000 – Rangka Dasar Keselamatan	

Teknologi Maklumat dan Komunikasi Kerajaan;

g. Pekeliling Am Bil. 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

h. MyMIS;

i. Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan;

j. Surat Pekeliling Am Bil. 6 Tahun 2005 – Garis Panduan Risiko Keselamatan Maklumat Sektor Awam;

k. Surat Pekeliling Am Bil. 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam;

l. Surat Ketua Setiausaha Negara – Langkah Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayer Di Agensi Agensi Kerajaan;

m. Surat Ketua Setiausaha Negara – Langkah Langkah Keselamatan Perlindungan Untuk Larangan Penggunaan Telefon Bimbit Atau Lain Lain Peralatan Komunikasi ICT Tanpa Kebenaran Kuasa Yang Sah Di Agensi-Agensi Kerajaan;

n. Undang-undang Malaysia Akta 680 – Akta Aktiviti Kerajaan Elektronik 2007; dan

o. Arahan Teknologi Maklumat 2007 (MAMPU).

LAMPIRAN A

SURAT AKUAN PEMATUHAN
DASAR DAN GARIS PANDUAN KESELAMATAN ICT JKR

Nama (Huruf Besar) : .....
No. Kad Pengenalan : .....
Jawatan : .....
Bahagian/ Cawangan : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

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

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

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT

.....
(Nama Pegawai Keselamatan ICT)
b.p. Ketua Pengarah JKR
Tarikh: .....

LAMPIRAN B

PERAKUAN UNTUK DITANDATANGANI
BERKENAAN DENGAN AKTA RASMI 1972

Adalah saya dengan ini mengaku bahawa perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan bahawa saya faham dengan sepenuhnya akan segala yang dimaksudkan Dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu rahsia atau apa-apa tingkahlaku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut, yang boleh dihukum maksimum penjara seumur hidup.

Saya faham bahawa segala maklumat rasmi yang saya perolehi dalam perkhidmatan Seri Paduka Baginda Yang Di-pertuan Agong atau perkhidmatan mana-mana Kerajaan dalam Malaysia, adalah milik Kerajaan dan tidak akan membocorkan, menyiarkan, atau menyampaikan, sama ada secara lisan atau dengan bertulis, kepada sesiapa jua dalam apa-apa bentuk, kecuali pada masa menjalankan kewajipan-kewajiipan rasmi saya, sama ada dalam masa atau selepas perkhidmatan saya dengan Seri Paduka Baginda Yang Di-pertuan Agong atau dengan mana-mana Kerajaan dalam Malaysia dengan tidak terlebih dahulu mendapat kebenaran bertulis pihak berkuasa yang berkenaan. Saya berjanji dan mengaku akan menandatangani suatu akauan selanjutnya bagi maksud ini apabila meninggalkan Perkihidmatan Awam.

Tandatangan:.....

Nama dengan huruf besar :.....

No. Kad Pengenalan :.....

Jawatan :.....

Jabatan :.....

Tarikh:.....

Disaksikan oleh:.....

(Tandatangan)

Nama dengan huruf besar :.....

No. Kad Pengenalan :.....

Jawatan :.....

Jabatan :.....

Tarikh:.....

Cop Jabatan:.....

LAMPIRAN C

PERAKUAN UNTUK DITANDATANGANI APABILA MENINGGALKAN PERKHIDMATAN KERAJAAN

Perhatian saya telah ditarik kepada peruntukan-peruntukan Akta Rahsia Rasmi 1972 dan saya faham dengan sepenuhnya akan segala yang dimaksudkan dalam Akta itu. Khususnya saya faham bahawa menyampaikan, menggunakan atau menyimpan dengan salah, sesuatu benda rahsia, tidak menjaga dengan cara yang berpatutan sesuatu benda rahsia atau apa-apa tingkahlaku yang membahayakan keselamatan atau rahsia sesuatu benda rahsia adalah menjadi suatu kesalahan di bawah Akta tersebut yang boleh dihukum maksimum penjara seumur hidup.

Semua maklumat yang telah saya dapat atau lihat dalam masa menjalankan kewajipan-kewajipan saya adalah diliputi oleh Akta tersebut. Adalah menjadi satu kesalahan di bawah Akta tersebut bagi saya menyampaikan dengan tiada kebenaran apa-apa maklumat itu kepada mana-mana orang lain, sama ada atau tidak orang itu memegang atau telah memegang jawatan di bawah Duli Yang Maha Mulia Seri Paduka Baginda Yang di-Pertuan Agong atau di bawah mana-mana Kerajaan Malaysia, sebelum dan selepas saya berhenti memegang jawatan itu.

Apa-apa tingkahlaku saya yang membahayakan keselamatan atau rahsia sesuatu maklumat atau apa-apa sebutan oleh saya dengan tiada kebenaran sama ada sebutan itu secara lisan atau terkandung dalam apa-apa gambarfoto, filem, negatif, pita rakam, peta, pelan, model, graf, lukisan, piringhitam, runut bunyi, benda, atau lain-lain alat dsb., dan sama ada di Malaysia atau di negara luar mengenai apa-apa perkara yang telah saya ketahui atau sifat rasmi saya itu boleh menyebabkan saya didakwa di bawah Akta tersebut.

Saya mengaku bahawa tidak lagi ada dalam milik saya atau kawalan saya apa-apa perkataan kod rasmi, isyaratimbal, atau katajodoh rasmi yang rahsia, atau apa-apa benda, suratan atau maklumat, anak kunci, lencana, alat meteri, atau cap bagi atau yang dipunyai, atau diguna, dibuat atau diadakan oeh mana-mana Jabatan Kerajaan atau oleh mana-mana pihak berkuasa diplomat yang dilantik oleh atau yang bertindak di bawah kuasa Kerajaan Malaysia atau Seri Paduka Baginda yang tidak dibenarkan dalam milik atau kawalan saya.

Tandatangan:.....

Nama dengan huruf besar :.....

No. Kad Pengenalan :.....

Jawatan :.....

Jabatan :.....

Tarikh:.....

Disaksikan oleh:.....

(Tandatangan)

Nama dengan huruf besar :.....

No. Kad Pengenalan :.....

Jawatan :.....

Jabatan :.....

Tarikh:.....

Cop Jabatan:.....

LAMPIRAN D

Daftar Perubahan Dokumen

Versi	Tarikh	Deskripsi	Kemaskini	TT
1.0	18 Okt 2008	Dokumen asal DKTMK JKR (berdasarkan BS7799:2005)	ICTSO	
2.0	20 Mei 2011	Perubahan keseluruhan dokumen DKTMK JKR kepada DGPKICT JKR yang berdasarkan ISO/IEC 27001:2005.	ICTSO	