DASAR KESELAMATAN ICT (DKICT)

JABATAN KERJA RAYA (JKR) MALAYSIA

VERSI 4.0

5 DISEMBER 2017

https://www.jkr.gov.my

SENARAI VERSI

Versi	Tarikh	Keterangan
1.0	18 Oktober 2008	Dokumen asal Dasar Keselamatan Teknologi Maklumat (DKTMK) JKR berpandukan BS7799:2005.
2.0	20 Mei 2011	Perubahan dokumen DKTMK JKR kepada Dasar dan Garis Panduan Keselamatan ICT (DGPKICT) JKR berpandukan ISO/IEC 27001:2005.
3.0	17 April 2015	Perubahan dokumen DGPKICT JKR berpandukan ISO/IEC 27001:2013.
4.0	5 Disember 2017	Perubahan dokumen DGPKICT JKR kepada Dasar Keselamatan ICT (DKICT) JKR yang berpandukan Pelan RAKKSSA MAMPU versi 01 bertarikh April 2016.

PRAKATA

Teknologi maklumat dan komunikasi (ICT) telah digunakan untuk memudah cara di dalam urusan harian di Jabatan Kerja Raya (JKR). Kepentingan ICT dalam urusan harian telah dapat mempercepatkan tugas-tugas yang perlu dilakukan secara berkesan. Justeru, keselamatan ICT adalah satu perkara penting bagi memastikan kelancaran urusan harian JKR tidak terganggu.

Bagi menjamin keselamatan aset-aset ICT JKR khasnya dan Kerajaan amnya, maka Dasar Keselamatan ICT (DKICT) JKR digubal. Objektif dasar 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 salah guna atau kecurian aset ICT.

Insiden yang ketara dan sering berlaku pada masa kini termasuk kejadian-kejadian seperti berikut:

a) Percubaan untuk mencapai sistem atau data tanpa kebenaran;
b) Serangan kod jahat (*malicious code*) seperti *virus, trojan horse, worms* dan sebagainya;
c) Gangguan yang disengajakan (*unwanted distruption*) atau halangan pemberian perkhidmatan (*denial of service*);
d) Menggunakan sistem untuk pemprosesan data atau penyimpanan data tanpa kebenaran (*unauthorized access*); dan
e) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak.

Dengan adanya penambahbaikan dasar yang terkini diharap dapat membantu meminimumkan kesan insiden keselamatan agar tahap perlindungan keselamatan ICT JKR berada ditahap terbaik. Adalah menjadi harapan saya agar DKICT JKR ini dapat dibaca, difahami dan dijadikan rujukan dalam sebarang pelaksanaan program ICT Jabatan agar keselamatan ICT di JKR dapat dijamin keberkesanannya.

YBhg. Dato' Sri Ir. Dr. Roslan bin Md. Taha
Ketua Pengarah
Jabatan Kerja Raya Malaysia
5 Disember 2017

ISI KANDUNGAN

TAJUK **MUKA SURAT**

TAJUK **MUKA SURAT**

PERKARA 07: PENGURUSAN OPERASI DAN KOMUNIKASI

PERKARA 08 KAWALAN CAPAIAN

TAJUK **MUKA SURAT**

TAJUK

LAMPIRAN

LAMPIRAN A: Surat Akuan Pematuhan Dasar Keselamatan ICT JKR

LAMPIRAN B: Surat Akuan Akta Rahsia Rasmi 1972 (Menggunakan Perkhidmatan Kerajaan)

LAMPIRAN C: Surat Akuan Akta Rahsia Rasmi 1972 (Meninggalkan Perkhidmatan Kerajaan)

LAMPIRAN D: Struktur Tadbir Urus Keselamatan ICT JKR

LAMPIRAN E: Jadual Pindaan Dasar Keselamatan ICT (DKICT) JKR

SINGKATAN

APS	-	Aplikasi
BTM	-	Bahagian Teknologi Maklumat
BPSM	-	Bahagian Pengurusan Sumber Manusia
BYOD	-	*Bring Your Own Device*
CERT JKR	-	Jawatankuasa Tindakbalas Insiden Keselamatan ICT Jabatan
CIO	-	*Chief Information Officer* (Ketua Pegawai Maklumat)
DKICT	-	Dasar Keselamatan ICT
DT	-	Data Terbuka
ICTSO	-	ICT *Security Officer* (Pegawai Keselamatan ICT)
ICT	-	*Information and Communication Technology* (Teknologi Maklumat dan Komunikasi)
JKR	-	Jabatan Kerja Raya
JPICT		Jawatankuasa Pemandu ICT
KPKR	-	Ketua Pengarah Kerja Raya
LAN	-	Rangkaian setempat *(LAN)*
MAMPU	-	*Malaysian Administrative Modernisation and Management Planning Unit* (Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia)
MDF	-	*Main Distribution Frame*
MRR	-	Maklumat Rahsia Rasmi
MyKJ		Sistem Maklumat Perjawatan Pegawai JKR
PF	-	Persekitaran Fizikal
PICT	-	Pengurus ICT
PII	-	*Personally Identifiable Information* (Maklumat Pengenalan Peribadi)
PKI	-	*Public Key Infrastructure*
PPP	-	Peranti Pengkomputeran Peribadi
PR	-	Peranti Rangkaian
SSO	-	*Single Sign-On*
TKPKR	-	Timbalan Ketua Pengarah Kerja Raya
UPS	-	*Uninterrupted Power Supply*

ISTILAH

APLIKASI

- adalah sistem berkomputer yang dibangunkan secara dalaman atau *outsource* atau diperolehi secara siap guna seperti Sistem ePerolehan, *Human Resources Management Information System* (HRMIS), Sistem Kedudukan Jawatan (MyKJ), *Electronic Time Attendance and Security System* (eTASS), Web Portal, sistem aplikasi berasaskan web dan lain-lain sistem aplikasi termasuk pakej perisian seperti pemprosesan kata dan helaian kerja.

ASET ICT

- adalah data serta maklumat ICT, perkakasan ICT, perisian ICT, sistem aplikasi serta laman web, perkhidmatan ICT 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 keputusan, menurut dasar agensi/kerajaan.

DATA TERBUKA

- adalah maklumat bebas digunakan, dikongsi dan digunakan oleh orang awam, agensi kerajaan dan organisasi swasta untuk pelbagai tujuan.

DOKUMENTASI

- adalah semua dokumen, himpunan atau kumpulan bahan yang disimpan, direkod dan digunakan dalam bentuk *softcopy*, *hardcopy*, media elektronik, media cetak, cetakan berkomputer, elektronik luar atau dalam talian, kertas lut sinar, risalah atau slaid.

FASILITI ICT

- adalah kemudahan fasiliti ICT yang disediakan seperti mel elektronik, perisian, perkakasan dan aset ICT yang berkaitan.

INSIDEN KESELAMATAN

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

INTERNET

- adalah sistem rangkaian antarabangsa yang membolehkan pengguna mencapai maklumat dari seluruh dunia.

KABEL

- adalah meliputi semua kabel seperti kabel rangkaian *fiber* dan *unshielded twisted pair* (UTP), kabel elektrik, kabel sambungan elektrik dan sebagainya yang berkaitan dengan ICT.

KESELAMATAN

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

KOMUNIKASI

- adalah pengaliran data atau maklumat daripada sumber pengeluar maklumat kepada sumber penerima maklumat menggunakan medium penghantaran dan jaringan komunikasi.

MAKLUMAT RAHSIA RASMI

- adalah jenis maklumat yang mempunyai erti yang diberikan kepadanya di bawah Akta Rahsia Rasmi 1972 [Akta 88].

MEDIA

- adalah alat yang digunakan untuk menyimpan dan menyampaikan informasi atau data.

MEDIA SOSIAL

- adalah sejenis media yang digunakan terus secara talian dengan membolehkan para pengguna dengan mudah untuk menyertai, berkongsi dan mencipta isi meliputi blog, rangkaian sosial, wiki, forum dan dunia virtual.

MEDIA STORAN

- adalah perkakasan, perisian dan sistem aplikasi yang berkaitan dengan penyimpanan data dan maklumat seperti disket, katrij, cakera padat, cakera mudah alih, pita, *hard disk*, *pen drive*, pangkalan data, *Storage Area Network* (SAN), *Network Area Storage* (NAS), *cloud storage* and *online storage* dan sebagainya yang menyimpan, merekod dan digunakan sebagai transaksi penerimaan dan penghantaran data atau maklumat.

MEL ELEKTRONIK

- adalah mel yang digunakan secara elektronik dalam penghantaran dan penerimaan data atau maklumat.

MEL BOM

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

MEL SAMPAH

- adalah mel yang tidak berkaitan yang dihantar kepada seseorang.

MEL SPAM

- adalah penggunaan mel elektronik untuk menghantar email yang tidak diinginkan atau *unsolicited message* dalam bentuk *electronic spam*, *instant messaging spam, newsgroup spam, web search engine spam, mobile phone messaging scam, online classified ads scam, Internet forum spam, social spam, file sharing spam, scam spam, blog spam*, pengiklanan dan sebagainya dalam jumlah yang banyak, sama atau hampir sama serta sentiasa berulang-ulang.

PANGKALAN DATA

- adalah himpunan fail, kumpulan fail atau rekod komputer yang disimpan di suatu tempat simpanan data yang berkait dan saling berhubung.

PELAYAN

- adalah peranti pengkomputeran yang menyimpan aplikasi dan storan.

PEMILIK SISTEM

- adalah Unit, Bahagian, Cawangan, Daerah dan Negeri atau Agensi Kerajaan atau individu yang dilantik bagi mewakili Unit, Bahagian, Cawangan, Daerah dan Negeri atau Agensi Kerajaan yang memiliki sistem serta bertanggungjawab dalam urus tadbir pengoperasian sistem yang telah dibangunkan.

PENCEGAHAN

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

PENGGUNA

- adalah semua pengguna ICT JKR iaitu kakitangan JKR, agensi Kerajaan, pembekal, kontraktor, pakar runding dan sebagainya yang menggunakan aset ICT, fasiliti ICT, sistem aplikasi ICT dan perkhidmatan ICT di JKR Malaysia.

PENTADBIR SISTEM

- adalah pegawai dan kakitangan yang ditugaskan sebagai Pentadbir Sistem-sistem aplikasi, pentadbir laman web, pentadbir sistem rangkaian dan keselamatan, pentadbir *server*, pentadbir storan, pentadbir *backup & recovery*, pentadbir mel elektronik dan pentadbir-pentadbir sistem yang berkaitan ICT.

PENYELARAS ICT

- adalah pegawai dan kakitangan yang ditugaskan sebagai penyelaras ICT untuk menyelaras semua urusan berkaitan ICT termasuk aset ICT, perkakasan ICT, perisian ICT, fasiliti ICT dan perkhidmatan ICT yang disediakan di JKR Bahagian, Cawangan, Daerah atau Negeri.

PERANTI PENGKOMPUTERAN PERIBADI

- adalah peranti komputer yang digunakan oleh pengguna untuk berinteraksi dengan sistem.

PERANTI RANGKAIAN

- adalah peranti yang digunakan untuk membolehkan saling hubung antara peranti komputer dan sistem aplikasi dan Internet seperti *switches*, *hub* dan *router*.

PERISIAN

- adalah semua perisian ICT yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data dan maklumat. Ini termasuklah sistem pengoperasian, aturcara aplikasi, perisian utiliti, perisian kolaboratif, perisian lembaran kerja, perisian komunikasi, perisian kejuruteraan, perisian pangkalan data, perisian *backup* dan lain-lain perisian berkaitan ICT.

PERISIAN BERBAHAYA

- adalah aturcara yang dibina bagi tujuan mendatangkan kemudaratan kepada pengguna dan sistem ICT atau yang belum diuji daripada aspek keselamatannya.

PERKAKASAN

- adalah semua perkakasan ICT yang tidak terhad kepada komputer, *work station, mobile workstation, laptop, mobile, server, mainframe, network appliances, security appliances* dan peralatan seperti bekalan kuasa, jana kuasa sokongan, *precision aircond*, UPS dan media storan seperti *thumb drives, disket, compact disc, tape, hard disk, storage area network* dan *tape library* dan peranti rangkaian.

PERKHIDMATAN ICT

- adalah perkhidmatan berkaitan ICT yang disediakan seperti kemudahan sistem aplikasi, web, *single sign-on* (SSO), mel elektronik, Internet, Intranet, rangkaian setempat (LAN), rangkaian tanpa wayar, rangkaian mobil dan perkhidmatan penyelenggaraan berkaitan ICT serta lain-lain perkhidmatan yang berkaitan ICT.

PERSEKITARAN FIZIKAL

- adalah lokasi fizikal yang menempatkan sistem ICT.

PERSONALLY IDENTIFIABLE INFORMATION

- adalah maklumat yang boleh digunakan secara tersendiri atau digunakan secara tersendiri atau digunakan dengan maklumat lain untuk mengenalpasti individu tertentu. Juga dikenali sebagai maklumat pengenalan peribadi.

PIHAK KETIGA

- adalah semua mereka yang ada hubungan bisnes dengan JKR tidak terhad kepada agensi lain, pembekal, kontraktor, pakar perunding dan sebagainya yang menggunakan aset ICT, fasiliti ICT, sistem aplikasi ICT dan perkhidmatan ICT di JKR Malaysia.

PREMIS KOMPUTER DAN KOMUNIKASI

- adalah premis, kawasan atau tempat yang digunakan untuk menempatkan dan menggunakan aset ICT, fasiliti ICT, sistem aplikasi ICT dan perkhidmatan ICT.

PUSAT DATA

- adalah lokasi berpusat penempatan semua perkakasan, perisian dan sistem aplikasi kritikal ICT yang tidak terhad kepada *enterprise server, enterprise storage, enterprise backup and recovery, enterprise database, enterprise network*, sistem aplikasi, web *portal* dan *security appliances* dan lain-lain perkhidmatan yang berkaitan ICT bagi menjamin kesinambungan perkhidmatan ICT.

RANGKAIAN

- adalah jaringan rangkaian yang dihubungkan seperti Internet, Intranet, rangkaian setempat (LAN), rangkaian tanpa wayar dan rangkaian mobil.

SISTEM

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

SISTEM PENGOPERASIAN

- adalah sistem komputer yang berfungsi menjalankan sistem operasi dan terdiri daripada aturcara, rutin, subrutin dan suruhan yang ditulis dalam bahasa pengaturcaraan.

TEKNOLOGI MAKLUMAT

- adalah bidang yang meliputi penggunaan teknologi komputer dan telekomunikasi.

VIRUS

- adalah perisian berbahaya dan aturcara yang dibina bagi tujuan mendatangkan kemudaratan kepada pengguna dan sistem ICT.

DASAR KESELAMATAN ICT (DKICT)

A. PENGENALAN

Dasar Keselamatan ICT (DKICT) JKR mengandungi peraturan-peraturan yang perlu dibaca, difahami dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) JKR. Tujuan utama dasar ini adalah untuk menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam penggunaan dan perlindungan aset ICT JKR.

B. OBJEKTIF

DKICT JKR diwujudkan bagi menjamin kesinambungan perkhidmatan di JKR dan meminimumkan kesan insiden keselamatan.

C. PERNYATAAN DASAR ICT

C1. 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.

C2. Sebarang penggunaan aset ICT seperti perkakasan, perisian, data atau maklumat, perkhidmatan dan manusia selain daripada maksud dan tujuan yang telah ditetapkan adalah tidak dibenarkan.

D. PRINSIP-PRINSIP

D1. 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.

D2. 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, memadam atau membatalkan sesuatu data atau maklumat.

D3. AKAUNTABILITI

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

D4. PENGASINGAN

Tugas mewujud, memadam, mengemaskini, 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.

D5. PENGAUDITAN

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

D6. PEMULIHAN

Pemulihan sistem 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.

D7. PEMATUHAN

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

E. SKOP

E1. DATA DAN MAKLUMAT

Semua data dan maklumat yang disimpan atau digunakan di pelbagai media storan atau perkakasan atau perisian yang berkaitan ICT.

E2. PERKAKASAN

Semua peralatan tidak terhad kepada komputer, *work station, mobile workstation, laptop, mobile, server, mainframe, security appliances*, bekalan kuasa, jana kuasa sokongan, pendingin hawa, *uninterrupted power supply* (UPS), *thumb drives, disket, compact disc, tape, hard disk*, *storage area network*, *tape library*, *router, core switch, switches, fiber cable, UTP cable,* aset rangkaian tanpa wayar dan sistem PABX.

E3. PERISIAN

Semua perisian ICT yang digunakan untuk mengendali, memproses, menyimpan dan menghantar data dan maklumat. Ini termasuklah sistem pengoperasian, aturcara aplikasi, perisian utiliti, perisian kolaboratif, perisian lembaran kerja, perisian komunikasi, perisian kejuruteraan, perisian pangkalan data, perisian *backup* dan lain-lain perisian berkaitan ICT.

E4. SUMBER MANUSIA

Semua pengguna termasuk kakitangan JKR, agensi Kerajaan, pembekal, kontraktor, pakar runding dan lain-lain yang menggunakan aset ICT, fasiliti ICT, sistem aplikasi ICT dan perkhidmatan ICT di JKR Malaysia; dan

E5. PERKHIDMATAN

Semua perkhidmatan ICT yang ditawarkan atau digunakan tidak terhad kepada kemudahan sistem aplikasi, web, *single sign-on* (SSO), mel elektronik, Internet, Intranet, rangkaian setempat (LAN), rangkaian tanpa wayar, rangkaian mobil dan perkhidmatan penyelenggaraan berkaitan ICT serta lain-lain perkhidmatan yang berkaitan ICT.

F. DASAR KESELAMATAN YANG BERKAITAN

Sebagai tambahan kepada dasar ini, semua pengguna ICT juga adalah terikat kepada dasar-dasar dan peraturan-peraturan berikut:

a) Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) MAMPU;
b) Arahan Keselamatan (CGSO);
c) Akta Kawasan Larangan dan Tempat Larangan 1959;
d) Akta Rahsia Rasmi 1972;
e) Akta Jenayah Komputer 1997;
f) Akta Tandatangan Digital 1997;
g) Pekeliling Am Bil. 3 Tahun 2000: Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan;
h) Pekeliling Am Bil. 1 Tahun 2001: Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);
i) Malaysia Management Information System (MyMIS);
j) Pekeliling Kemajuan Pentadbiran Awam Bil. 1 Tahun 2003: Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan;
k) Surat Pekeliling Am Bil. 6 Tahun 2005: Garis Panduan Risiko Keselamatan Maklumat Sektor Awam;
l) Surat Pekeliling Am Bil. 4 Tahun 2006: Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat Dan Komunikasi (ICT) Sektor Awam;

m) Surat Ketua Setiausaha Negara: Langkah-langkah untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar di Agensi-agensi Kerajaan;
n) 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;
o) Undang-undang Malaysia Akta 680 - Akta Aktiviti Kerajaan Elektronik 2007;
p) Arahan Teknologi Maklumat 2007 (MAMPU); dan
q) Dasar, Peraturan dan Pekeliling-pekeliling yang sedang berkuatkuasa.

G. PERUBAHAN MAKLUMAT

Sebarang maklum balas atau perubahan berkaitan dengan dasar ini hendaklah diajukan kepada:

Nama : Pegawai Keselamatan ICT (ICTSO)
Alamat : Bahagian Teknologi Maklumat,
Cawangan Dasar dan Pengurusan Korporat,
Tingkat 16, Ibu Pejabat JKR Malaysia,
Jalan Sultan Salahuddin,
50582 Wilayah Persekutuan Kuala Lumpur.
Telefon : 03-2610 7065
Faksimili : 03-2611 2909
E-mel : ictso@jkr.gov.my

PERKARA 01

DASAR KESELAMATAN ICT

PERKARA 01: DASAR KESELAMATAN ICT

0101 Pengurusan Dasar Keselamatan ICT

OBJEKTIF:

Menerangkan hala tuju, sokongan dan komitmen pengurusan ICT JKR terhadap keselamatan maklumat dan aset selaras dengan keperluan JKR dan perundangan yang berkaitan serta arahan pekeliling kerajaan yang sedang berkuatkuasa.

010101 Pelaksanaan Dasar	
Kelulusan dan pelaksanaan dasar ini adalah di bawah bidang kuasa KPKR dengan dibantu oleh Jawatankuasa Keselamatan ICT JKR yang dipengerusikan oleh Ketua Pengarah Kerja Raya (KPKR) atau Ketua Pegawai Maklumat (CIO).	KPKR dan CIO

010102 Penyebaran Dasar	
Dasar ini perlu disebarkan, difahami, dipatuhi dan dikuatkuasakan kepada semua pengguna termasuk kakitangan JKR, agensi kerajaan, pembekal, kontraktor, pakar runding dan lain-lain yang menggunakan aset ICT, fasiliti ICT, sistem aplikasi ICT dan perkhidmatan ICT di JKR Malaysia. Pengguna perlu menandatangani **Surat Akuan Pematuhan DKICT JKR** seperti di **Lampiran A**.	ICTSO

010103 Penyelenggaraan Dasar	
DKICT JKR adalah tertakluk kepada semakan dan pindaan dari masa ke semasa selaras dengan perubahan piawaian antarabangsa ISO/IEC, dasar nasional dan Kerajaan, dasar JKR, teras bisnes JKR, teknologi, sistem aplikasi, prosedur, perundangan dan kepentingan lain JKR. Berikut adalah prosedur berhubung dengan penyelenggaraan DKICT JKR: a) Mengenalpasti dan menentukan perubahan yang diperlukan selaras dengan perkembangan terkini; b) Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Keselamatan ICT JKR; c) Memaklumkan kepada semua kakitangan JKR dan pengguna aset ICT JKR sama ada melalui risalah, pekeliling, papan buletin atau laman	ICTSO dan JK Keselamatan ICT

web intranet JKR bagi sebarang perubahan ke atas DKICT JKR yang telah dipersetujui; dan d) Mengkaji semula DKICT JKR sekurang-kurangnya **satu (1) kali setahun** atau **mengikut keperluan semasa**.	

010104 Pengecualian Dasar

Dokumen DKICT JKR ini adalah terpakai kepada semua pengguna ICT JKR dan tiada pengecualian diberikan.	Pengguna dan pihak ketiga

PERKARA 02

ORGANISASI KESELAMATAN ICT

PERKARA 02: ORGANISASI KESELAMATAN ICT

0201 Infrastruktur Organisasi Keselamatan

OBJEKTIF:

Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur di dalam mencapai objektif DKICT JKR.

020101 Ketua Pengarah Kerja Raya (KPKR)	
Peranan dan tanggungjawab Ketua Pengarah adalah seperti berikut: a) Mempengerusikan atau melantik pengerusi gantian bagi Mesyuarat Jawatankuasa Keselamatan ICT JKR; b) Memastikan pelaksanaan DKICT JKR; c) Berkuasa meluluskan pindaan DKICT JKR; d) Memastikan semua pengguna memahami peruntukan-peruntukan di bawah DKICT JKR; e) Memastikan semua pengguna mematuhi DKICT JKR; f) Memastikan semua keperluan organisasi seperti sumber kewangan, perkakasan dan perisian ICT, sumber manusia dan perlindungan keselamatan ICT adalah mencukupi; g) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT JKR; h) Menggunakan budi bicara berkaitan keselamatan ICT dengan syarat berpandukan dasar, garis panduan dan prosedur keselamatan ICT yang berkuatkuasa; dan i) Melantik Ketua Pegawai Maklumat (CIO), Pengurus ICT dan Pegawai Keselamatan ICT (ICTSO).	KPKR

020102 Ketua Pegawai Maklumat (CIO)	
Ketua Pegawai Maklumat (CIO) yang dilantik oleh KPKR berperanan dan bertanggungjawab untuk: a) Membantu KPKR di dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b) Mengesah dan mengawal dokumen DKICT JKR;	CIO

c) Merancang, menyelaras dan menguatkuasakan pelaksanaan DKICT di JKR; d) Memantau pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; e) Menentukan keperluan keselamatan ICT; f) Memantau keberkesanan pelaksanaan DKICT JKR dan pencapaian objektif DKICT JKR; g) Melapor keberkesanan pelaksanaan DKICT JKR kepada KPKR; h) Menguruskan penilaian risiko dan program keselamatan ICT; dan i) Mempengerusikan mesyuarat Jawatankuasa Keselamatan ICT JKR.	

020103 Pengurus ICT

Ketua Bahagian Teknologi Maklumat (KBTM) adalah merupakan Pengurus ICT JKR. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a) Membentang laporan keselamatan ICT di dalam Mesyuarat Jawatankuasa Keselamatan 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) Menyelaras garis panduan dan prosedur keselamatan ICT supaya selaras dengan keperluan DKICT JKR; e) Memastikan Pelan Strategik ICT Jabatan mengandungi aspek perlindungan keselamatan ICT; f) Memperakukan langkah-langkah membaik pulih insiden pada kadar segera berdasarkan dasar, prosedur dan pekeliling yang sedang berkuatkuasa; g) Memperakukan proses pengambilan tindakan ke atas pengguna yang melanggar DKICT JKR berdasarkan dasar, prosedur dan pekeliling yang sedang berkuatkuasa; h) Memaklumkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO; dan i) Memaklumkan insiden keselamatan ICT kepada CIO dan melaporkan kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU jika perlu.	Pengurus ICT

020104 Pegawai Keselamatan ICT (ICTSO)	
Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a) Menguatkuasakan DKICT JKR; b) Mengurus keseluruhan program keselamatan ICT JKR dengan memberi penerangan dan pendedahan berkenaan DKICT JKR kepada semua pengguna dibantu oleh Unit Keselamatan dan Rangkaian, Bahagian Teknologi Maklumat (BTM) JKR; c) Menjalankan pengurusan dan penilaian risiko keselamatan ICT dengan melaksanakan pengauditan ICT, kajian semula, merumus tindak balas pengurusan keselamatan ICT berdasarkan hasil penemuan dan menyediakan laporan dan tindakan yang sewajarnya; d) Memberikan kerjasama dengan semua Pentadbir Sistem, Penyelaras ICT, Pengguna dan pihak yang berkaitan untuk mengenal pasti punca insiden keselamatan ICT; e) Memberikan amaran kepada Pengguna ICT terhadap sebarang ancaman keselamatan ICT yang berbahaya, memberi khidmat nasihat dan menyediakan langkah-langkah perlindungan ICT yang bersesuaian; f) Memaklumkan insiden keselamatan ICT kepada Pengurus ICT; g) Mengambil tindakan ke atas pengguna yang melanggar DKICT JKR berdasarkan dasar, prosedur dan pekeliling yang sedang berkuatkuasa; h) Menyemak, menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT di JKR; i) Memastikan DKICT dikemaskini sesuai dengan perubahan teknologi, arahan Jabatan & ancaman-ancaman baharu dari masa ke semasa; j) Mempengerusikan Jawatankuasa CERT 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 bertanggungjawab terhadap perkara-perkara seperti berikut: a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai insiden keselamatan ICT, b) Menyediakan perkhidmatan berkaitan ICT kepada Pengguna yang memulakan tugas, berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas berdasarkan dasar, prosedur dan garis panduan yang telah ditetapkan;	Pentadbir Sistem ICT

c) Memantau dan menyediakan laporan aktiviti capaian harian, mingguan, bulanan dan tahunan semua Pengguna ICT; 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 semua rekod jejak audit dan laporan mengenai aktiviti capaian secara berkala; f) Memastikan kerahsiaan kata laluan semua aset ICT, fasiliti ICT, perkakasan dan perisian yang berada di bawah tanggungjawabnya dan disimpan di tempat yang selamat; dan g) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera.	

020106 Pemilik Sistem	
Pemilik Sistem adalah unit, bahagian, cawangan, daerah, negeri, mana-mana agensi kerajaan atau individu yang dilantik mewakili pihak pemilik sebenar sistem aplikasi. Ia bertanggungjawab di dalam urus tadbir pengoperasian sistem aplikasi yang telah dibangunkan. Peranan dan tanggungjawab Pemilik Sistem adalah seperti berikut: a) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai insiden keselamatan ICT; b) Menyediakan perkhidmatan berkaitan ICT kepada Pengguna yang memulakan tugas, berhenti, bertukar, bercuti, atau berlaku perubahan di dalam bidang tugas berdasarkan dasar, prosedur dan garis panduan yang telah ditetapkan; c) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan melaporkan kepada Pentadbir Sistem ICT untuk membatalkan atau memberhentikannya dengan serta merta; d) Memastikan kerahsiaan kata laluan semua aset ICT, fasiliti ICT, perkakasan dan perisian yang berada di bawah tanggungjawabnya dan disimpan di tempat yang selamat; dan e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Pentadbir Sistem ICT dengan segera.	Pemilik Sistem

020107 Penyelaras ICT	
Penyelaras ICT di bahagian, cawangan, daerah dan negeri yang telah dilantik adalah berperanan dan bertanggungjawab: a) Sebagai perantara di antara BTM, Pentadbir Sistem ICT dan Pengguna di bawah kawalannya; b) Melaporkan dengan segera kepada Pentadbir Sistem ICT dan Pemilik Sistem apabila terdapat kakitangan yang berhenti, bertukar, berkursus dan bercuti jangka panjang atau berlaku perubahan dalam bidang tugas; c) Menyimpan dan menyelenggara rekod aset ICT di bawah kawalannya dan melaporkan kepada Pegawai Aset Alih pejabat; d) Menyelaras dan melaksana penyelenggaraan perisian dan perkakasan; dan e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada Pengurus ICT atau ICTSO dengan segera.	Penyelaras ICT

020108 Pengguna	
Pengguna adalah kakitangan JKR, agensi kerajaan, pembekal, kontraktor, pakar runding dan lain-lain yang menggunakan aset ICT, fasiliti ICT, sistem aplikasi ICT dan perkhidmatan ICT di JKR Malaysia. Peranan dan tanggungjawab pengguna adalah seperti berikut: a) Membaca, memahami dan mematuhi DKICT JKR; b) Mengetahui dan memahami implikasi keselamatan ICT kesan daripada tindakannya; c) Melaksanakan prinsip-prinsip DKICT; d) Melaksanakan langkah-langkah perlindungan seperti berikut: - i. Menghalang pendedahan dan ketirisan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi piawai, prosedur dan garis panduan keselamatan yang ditetapkan; dan	Pengguna

vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan maklumat. e) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada sama ada Penyelaras ICT, Pentadbir Sistem ICT, Pemilik Sistem, ICTSO atau Pengurus ICT dengan segera; f) Menghadiri program kesedaran mengenai keselamatan ICT; dan g) Menandatangani **Surat Akuan Pematuhan DKICT JKR** seperti di **Lampiran A**.	

020109 Jawatankuasa Keselamatan ICT

Jawatankuasa Keselamatan ICT juga merupakan Jawatankuasa Pemandu ICT (JPICT) JKR. Ia adalah jawatankuasa yang bertanggungjawab di dalam memastikan keselamatan ICT serta berperanan sebagai penasihat dan jawatankuasa dalam memastikan tujuan dan objektif keselamatan ICT JKR tercapai. Keanggotaan Jawatankuasa Keselamatan ICT JKR adalah sama dengan JPICT JKR iaitu seperti berikut: Pengerusi : CIO Jabatan Ahli : a) Pengurus ICT Jabatan b) ICTSO Jabatan c) Pengarah-pengarah Cawangan d) Pentadbir Sistem ICT Jabatan Urusetia : Bahagian Teknologi Maklumat Bidang kuasa : a) Memperakukan dokumen DKICT JKR; b) Memantau tahap pematuhan keselamatan ICT; c) Memperakukan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT JKR; d) Memastikan sistem ICT sentiasa mematuhi keperluan keselamatan dari semasa ke semasa; e) Menilai kesesuaian teknologi untuk keperluan keselamatan ICT; f) Memastikan DKICT JKR selaras dengan dasar-dasar ICT kerajaan semasa;	Jawatankuasa Keselamatan ICT

g) Membincangkan laporan keselamatan ICT dan menyelesaikan isu-isu berbangkit; h) Menimbang dan melulus Pelan Kesinambungan Perkhidmatan (PKP) JKR; i) Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden; dan j) Membincangkan pelanggaran DKICT JKR dan tindakan yang perlu diambil.	

020110 Jawatankuasa Tindakbalas Insiden Keselamatan ICT (CERT)

Jawatankuasa Tindakbalas Insiden Keselamatan ICT Jabatan (CERT) merupakan jawatankuasa khas yang berfungsi untuk membincang dan memperkemaskan pengurusan pengendalian insiden keselamatan ICT JKR. Keanggotaan CERT adalah seperti berikut: Pengarah : Pengurus ICT Pengerusi : ICTSO Ahli : a) Pentadbir Sistem ICT b) Penyelaras ICT c) Pemilik Sistem Urusetia : Unit Rangkaian dan Keselamatan, BTM Bidang kuasa : a) Menerima, mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; b) Merekod dan menjalankan siasatan awal insiden yang diterima; c) Menangani atau bertindak balas terhadap insiden keselamatan ICT dan mengambil tindakan baik pulih dan pengukuhan; d) Menghubungi dan melaporkan insiden yang berlaku kepada Pengurus ICT dan GCERT MAMPU samada sebagai input atau untuk tindakan seterusnya; e) Menyedia dan mematuhi prosedur piawaian (SOP); dan f) Menilai aspek teknikal keselamatan projek-projek dan sistem aplikasi ICT JKR.	

0202 Pihak Ketiga

OBJEKTIF:

Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga iaitu mereka yang ada hubungan bisnes dengan JKR tidak terhad kepada agensi lain, pembekal, kontraktor dan perunding.

020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
Keperluan keselamatan kontrak bertujuan untuk memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dapat dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: a) Membaca, memahami dan mematuhi DKICT JKR; b) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c) Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d) Memastikan semua syarat keselamatan dinyatakan dengan jelas di dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. DKICT JKR; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. e) Akses kepada aset ICT JKR perlu berlandaskan kepada perjanjian kontrak; dan f) Menandatangani Surat Akuan Pematuhan DKICT JKR seperti di **Lampiran A, B dan C**.	CIO, Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pemilik Sistem dan Pengguna

* Struktur tadbir urus Keselamatan ICT JKR adalah seperti pada **Lampiran D**.

PERKARA 03

PENGURUSAN ASET ICT

PERKARA 03: 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 mengenalpasti aset, mengelas aset mengikut tahap sensitiviti dan merekodkan maklumat seperti pemilik dan sebagainya. Setiap pengguna adalah bertanggung jawab ke atas semua aset ICT di bawah kawalannya. Ini bertujuan untuk memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkod di dalam borang daftar harta modal dan inventori 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 JKR; d) Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumen dan dilaksanakan; e) Sebarang pelanggaran hendaklah dilaporkan kepada Penyelaras ICT atau ICTSO; dan f) Maklumat Rahsia Rasmi hendaklah disimpan dan diproses di dalam elemen persekitaran pengkomputeran yang disahkan CIO. Kategori elemen tersebut adalah seperti: i. Peranti pengkomputeran peribadi ii. Peranti rangkaian iii. Aplikasi iv. Pelayan; dan v. Persekitaran fizikal	Pentadbir Sistem ICT, Penyelaras ICT dan Pengguna

Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya dan mengikut Tatacara Pengurusan Aset Alih Kerajaan yang sedang berkuatkuasa. Pengguna dan pihak ketiga hendaklah memulangkan semua aset organisasi di dalam pegangan serta merta setelah bertukar tempat bertugas, bersara, diberhentikan, tamat kontrak atau apabila perjanjian ditamatkan. Proses penamatan hendaklah dilaksanakan secara formal dengan memasukkan semua aset fizikal dan elektronik termasuk yang menjadi hak milik Kerajaan. Di dalam kes di mana pengguna atau pihak ketiga membuat pembelian aset organisasi atau menggunakan aset peribadi hendaklah mematuhi untuk menyerahkan maklumat berkaitan kepada Jabatan dan memadam maklumat daripada aset tersebut. Di dalam kes di mana pengguna dan pihak ketiga mempunyai pengetahuan penting bagi tujuan operasi semasa atau berterusan, maklumat tersebut hendaklah didokumentasi dan diserahkan kepada Jabatan. Di dalam tempoh notis penamatan, Jabatan hendaklah mengawal salinan maklumat terlarang seperti *intellectual property* oleh pengguna dan pihak ketiga yang ditamatkan perkhidmatannya.	

0302 Pengelasan dan Pengendalian Maklumat

OBJEKTIF:

Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan berdasarkan tahap kerahsiaan.

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	Pemilik Sistem, Pentadbir Sistem ICT dan Pengguna

d) Terhad. Semua maklumat yang dijana atau dikumpul oleh Jabatan hendaklah diasingkan mengikut kategori Maklumat Rasmi dan Maklumat Rahsia Rasmi. Kedua-dua kategori boleh mengandungi *Personally Identifiable Information* (PII). Maklumat Rasmi boleh juga mengandungi Data Terbuka.	

030202 Pengendalian Maklumat

Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambil kira langkah-langkah keselamatan berikut: a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b) Memeriksa maklumat dan menentukan ia tepat dan lengkap dari masa ke semasa; c) Menentukan maklumat sedia untuk digunakan; d) Menjaga kerahsiaan kata laluan; e) Mematuhi piawaian, 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 mengenai keselamatan ICT daripada diketahui umum. Jabatan hendaklah mengenal pasti kawasan terperingkat. Kawasan terperingkat meliputi kawasan premis atau sebahagian daripada premis di mana rahsia rasmi disimpan atau diuruskan atau di mana kerja terperingkat dijalankan. Peranti milik persendirian dilarang penggunaannya di kawasan terperingkat.	Pengguna, Penyelaras ICT

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;	Pengguna

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.	

PERKARA 04

KESELAMATAN SUMBER MANUSIA

PERKARA 04: KESELAMATAN SUMBER MANUSIA

0401 Keselamatan ICT Dalam Tugas Harian

OBJEKTIF:

Memastikan semua sumber manusia mematuhi aspek keselamatan ICT di dalam tugas harian.

Semua pengguna mestilah melaksanakan tanggungjawab dan peranan, meningkatkan pengetahuan dalam keselamatan aset ICT serta mematuhi terma dan syarat perkhidmatan termasuk peraturan semasa yang berkuatkuasa di dalam melaksanakan tugas rasmi harian.	Pengguna

0402 Sebelum Perkhidmatan

OBJEKTIF:

Memastikan semua pengguna mematuhi terma dan syarat perkhidmatan yang ditawarkan serta peraturan semasa yang berkuat kuasa.

040201 Peranan dan Tanggungjawab Pengguna

Semua pengguna mestilah jelas, patuh dan melaksanakan peranan dan tanggungjawabnya terhadap pematuhan keselamatan ICT. Keselamatan ICT merangkumi tanggungjawab Pengguna untuk menyedia dan memastikan perlindungan ke atas semua aset ICT yang digunakan di dalam melaksanakan tugas harian. Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab pengguna serta pembekal yang terlibat di dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b) Menjalankan tapisan keselamatan untuk pengguna serta pembekal yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuatkuasa berdasarkan perjanjian yang telah ditetapkan; dan d) Ketua Jabatan/Bahagian perlu memastikan setiap kakitangan seliaannya menandatangani" Surat Akuan Pematuhan DKICT JKR" (Lampiran A).	Pengguna

040202 Terma dan Syarat Perkhidmatan	
Semua pengguna hendaklah mematuhi terma dan syarat perkhidmatan yang ditawarkan serta peraturan semasa yang berkuat kuasa.	Pengguna

040203 Perakuan Akta Rahsia Rasmi dan Pematuhan Lain-lain Peraturan yang Berkuatkuasa	
Semua Pengguna dan Pihak Ketiga yang menguruskan maklumat terperingkat hendaklah mematuhi semua peruntukan Akta Rahsia Rasmi 1972. Pihak ketiga yang terlibat hendaklah mematuhi semua peruntukan di dalam DKICT JKR. Pihak ketiga yang menggunakan dan mengakses aset ICT JKR mesti menandatangani Surat Akuan Rahsia Rasmi 1972 seperti di **Lampiran B.**	Pengguna dan pihak ketiga

0403 Semasa Berkhidmat

Objektif:

Memastikan semua pengguna sedar dan bertanggungjawab terhadap ancaman keselamatan ICT bagi meminimumkan risiko seperti kesilapan, kecuaian, kecurian, penipuan dan penyalahgunaan aset ICT JKR.

040301 Tanggungjawab Pengurusan	
a) Memastikan semua Pengguna menguruskan keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh JKR. b) Memastikan latihan kesedaran keselamatan ICT JKR diberikan kepada semua pengguna JKR dan sekiranya perlu diberikan kepada pihak ketiga yang tidak terhad kepada kontraktor, pembekal, pakar runding dan pihak-pihak lain dari masa ke semasa.	CIO, Pengurus ICT, ICTSO dan Pengguna

040302 Kesedaran Keselamatan ICT	
Setiap pengguna di JKR perlu diberikan program kesedaran, latihan atau kursus mengenai keselamatan ICT yang mencukupi secara berterusan di dalam melaksanakan tugas-tugas dan tanggungjawab mereka. Program menangani insiden juga dilihat penting sebagai langkah pencegahan yang boleh mengurangkan ancaman keselamatan ICT JKR.	ICTSO dan Pengguna

040303 Tindakan Tatatertib	
Perlanggaran DKICT JKR boleh dikenakan tindakan tatatertib mengikut tatacara pengurusan tindakan tatatertib, salah laku dan jenayah pekeliling-pekeliling Kerajaan yang berkuatkuasa.	Pengguna

0404 Bertukar atau Tamat Perkhidmatan

Objektif:

Memastikan semua urusan pertukaran atau penamatan perkhidmatan pengguna dilaksanakan dengan teratur bagi meminimumkan risiko keselamatan ICT.

040401 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 membawa bersama aset ICT ke tempat baru kecuali berlaku penstrukturan semula organisasi JKR Malaysia; dan d) Menandatangani **Surat Akuan Pematuhan DKICT JKR** iaitu **Lampiran C** untuk tidak mendedahkan maklumat-maklumat aset ICT JKR selepas penamatan perkhidmatan di JKR.	Pengurus ICT, Pentadbir Sistem ICT dan Pemilik Sistem

PERKARA 05

KESELAMATAN FIZIKAL

PERKARA 05: KESELAMATAN FIZIKAL

0501 Keselamatan Fizikal

OBJEKTIF:

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

050101 Perimeter Keselamatan Fizikal	
Keselamatan fizikal adalah bertujuan untuk menghalang, mengesan dan mencegah cubaan menceroboh. Langkah-langkah keselamatan fizikal tidak terhad kepada langkah-langkah berikut: a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan sistem 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, Pengurus ICT dan ICTSO

050102 Kawalan Masuk Fizikal	
Pengguna a) Setiap pengguna JKR hendaklah memakai pas keselamatan sepanjang waktu bertugas; b) Semua pas keselamatan pengguna hendaklah diserahkan balik 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;	Pengguna dan Pelawat

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; dan 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" bermaksud 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. 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; c) Mengambil gambar, video, audio adalah dilarang **KECUALI** dengan kebenaran pihak Pengurusan Jabatan, CIO, Pengurus ICT atau ICTSO; dan d) Semua penggunaan peralatan yang melibatkan penghantaran, kemaskini dan penghapusan maklumat rahsia rasmi hendaklah dikawal dan mendapat kebenaran daripada Ketua Jabatan.	Pengguna

050104 Kawasan Terhad	
Kawasan terhad ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada warga JKR yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan terhad adalah seperti bilik *server*, bilik *main distribution frame* (MDF), pusat data, bilik fail dan bilik simpanan aset ICT. Perkara-perkara yang mesti dipatuhi adalah seperti berikut : a) Semua urusan keluar masuk kawasan terhad mesti direkodkan melalui pendaftaran setiap pengguna terlebih dahulu; dan b) Setiap pengguna yang perlu menggunakan aset ICT mestilah diiringi oleh Pentadbir Sistem ICT.	Pengguna

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 sama ada untuk memperoleh, menyewa, ubah suai, pembelian hendaklah dirujuk terlebih dahulu kepada Ketua Pegawai Keselamatan JKR. Bagi menjamin keselamatan persekitaran, langkah-langkah berikut hendaklah diambil: a) Merancang dan menyediakan pelan keseluruhan susun atur dengan teliti (pusat data, bilik cetak, ruang perkakasan komputer, ruang atur pejabat dan sebagainya); 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 keselamatan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan;	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran perkakasan komputer; g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya satu kali setahun atau berdasarkan keperluan; dan h) Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan lanjut sekiranya perlu.	

050202 Bekalan Kuasa

a) Pengagihan bekalan kuasa bagi penggunaan pusat data dan bangunan perlu diasingkan; b) Semua perkakasan ICT hendaklah dilindungi daripada kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada perkakasan ICT; c) Peralatan sokongan seperti *uninterruptable power supply* (UPS) dan sistem penjana kuasa *(generator)* boleh digunakan bagi perkhidmatan kritikal seperti di bilik *server* supaya mendapat bekalan kuasa berterusan; d) Sistem penjana kuasa *(generator)* mestilah disediakan secara khusus untuk pusat data dan berasingan daripada bekalan kepada bangunan / tingkat. Penjaga jentera dipertanggungjawabkan untuk memastikan sistem ini berada di dalam keadaan siap siaga; dan e) Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

050203 Prosedur Kecemasan

a) Setiap pengguna hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada garis panduan keselamatan ICT MAMPU dan CGSO (*Chief Government Security Office*); b) Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Ketua Pegawai Keselamatan JKR 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 (BTM) sekiranya berlaku kerja-kerja pengkabelan baru.	Pentadbir Sistem ICT

0503 Keselamatan Peralatan

Objektif:

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

050301 Perkakasan ICT	
Perkakasan ICT perlu dilindungi kerana boleh menjadi punca keterdedahan maklumat. Langkah-langkah keselamatan yang perlu dipatuhi adalah seperti berikut: a) Pengguna hendaklah menyemak dan memastikan bahawa semua perkakasan 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 untuk menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan; d) Pengguna adalah bertanggungjawab untuk melapor kerosakan atau kehilangan perkakasan ICT di bawah kawalannya;	Pengguna

e) Pengguna perlu memastikan perisian *antivirus* komputer peribadi mereka sentiasa aktif dan dikemaskini di samping melakukan imbasan ke atas media storan yang digunakan; f) Pengguna wajib menetapkan kata laluan untuk akses sistem komputer; g) Semua perkakasan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; h) Semua perkakasan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Perkakasan 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) Perkakasan ICT yang hendak dibawa keluar dari premis JKR, perlulah mendapat kelulusan Pengurus ICT dan direkodkan bagi tujuan pemantauan; k) Perkakasan ICT yang hilang hendaklah dilaporkan kepada Pegawai Aset Alih dan dimaklumkan kepada Penyelaras ICT dengan segera. Penyelaras ICT kemudiannya perlu melaporkan kepada ICTSO; l) Pengendalian perkakasan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; m) Sebarang kerosakan perkakasan ICT hendaklah dilaporkan kepada Pentadbir Sistem ICT untuk di baik pulih; n) Konfigurasi alamat IP asal tidak boleh ditukar tanpa kebenaran; o) Pengguna dilarang mengubah kata laluan 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 bekalan kuasa semua perkakasan komputer, pencetak dan pengimbas dimatikan apabila meninggalkan pejabat; dan r) Sebarang bentuk penyelewengan atau salah guna perkakasan ICT hendaklah dilaporkan kepada ICTSO.	

050302 Penyelenggaraan Peralatan / Perkakasan	
Aset ICT hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan dan integriti: a) Semua aset ICT yang diselenggarakan hendaklah mematuhi spesifikasi pengeluar yang telah ditetapkan; b) Aset ICT hanya boleh diselenggarakan oleh kakitangan atau pihak yang dibenarkan sahaja; dan c) Semua aset ICT hendaklah disemak dan diuji sebelum dan selepas proses penyelenggaraan dilakukan.	Pentadbir Sistem ICT dan Pengguna

050303 Keselamatan Perkakasan untuk Kegunaan di Luar Pejabat / Premis	
Perkakasan yang dipinjam untuk kegunaan di luar pejabat / premis adalah terdedah kepada pelbagai risiko. Langkah-langkah berikut boleh diambil untuk menjamin keselamatan perkakasan: a) Perkakasan, maklumat atau perisian yang dibawa keluar pejabat/ premis mestilah mendapat kelulusan Pegawai Aset Alih Bahagian / cawangan / daerah / negeri dan tertakluk kepada tujuan yang dibenarkan; b) Aktiviti peminjaman dan pemulangan perkakasan mestilah direkodkan dan disahkan oleh Pegawai Aset Alih pejabat; c) Perkakasan perlu dilindungi dan dikawal sepanjang masa; dan d) Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Pengguna

050304 Pelupusan Aset ICT	
Aset ICT yang hendak dilupuskan perlu melalui proses pelupusan seperti termaktub di dalam pekeliling semasa. Pelupusan aset ICT perlu dilakukan secara terkawal dan mengikut prosedur supaya maklumat tidak terlepas dari kawalan JKR: a) Semua kandungan perkakasan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui kaedah *shredding, grinding* atau pembakaran; b) Rujuk Tatacara Pengurusan Aset Alih Kerajaan untuk maklumat lanjut berkaitan proses pelupusan; dan	Pentadbir Sistem ICT dan Pengguna

c) Data dan maklumat di dalam media storan perkakasan ICT yang akan dilupuskan mestilah telah dilupuskan atau dipindah dengan cara yang selamat.	

050305 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat. Media-media storan perlu dipastikan berada di dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan sedia untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; b) Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna yang dibenarkan sahaja; c) Semua media storan perlu dikawal bagi mencegah daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan; d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan pecah, api, air dan medan magnet. e) Akses dan pergerakan media storan seperti *tape backup* hendaklah direkodkan; f) Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; g) Mengadakan salinan penduaan atau *backup* pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h) Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur, selamat dan mengikut prosedur; dan i) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	Pentadbir Sistem ICT dan Pengguna

050306 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Pengguna hanya boleh memasang dan menggunakan perisian dan aplikasi yang mempunyai lesen sah sahaja; b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; c) Lesen perisian (*registration code, serials,* CD-keys) perlu disimpan dan direkodkan dengan betul; d) Kod Sumber (*source code*) sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan; e) Penggunaan media perisian dan aplikasi tidak sah adalah dilarang; dan f) Semua perisian hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala.	Pengguna

PERKARA 06

KESELAMATAN DATA

PERKARA 06: KESELAMATAN DATA

0601 Aliran Data

Objektif:

Memastikan aliran data yang sahih supaya data yang disimpan di dalam pangkalan data selamat daripada dicerobohi dan disalah guna oleh orang lain.

060101 Pengendalian Prosedur	
Aliran data merujuk kepada laluan lengkap data tertentu semasa transaksi. Aliran data dan komunikasi di dalam Jabatan hendaklah dikenal pasti, direkodkan dan dikaji semula secara berkala. Saluran komunikasi termasuk: a) Saluran komunikasi dan aliran data antara sistem-sistem di Jabatan; dan b) Saluran komunikasi dan aliran data ke sistem luar Jabatan. Saluran komunikasi dan aliran data ke ruang storan pengkomputeran awan dianggap sebagai saluran komunikasi luaran. Aliran data bagi Maklumat Rahsia Rasmi hendaklah diasingkan daripada aliran Data Terbuka dan *Personally Identifiable Information* (PII). Selain itu, aliran data bagi empat kategori Maklumat Rahsia Rasmi juga hendaklah diasingkan.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

0602 Teknologi Perlindungan Data

Objektif:

Memastikan teknologi perlindungan data dapat dikenalpasti dan dipatuhi di semua peringkat pemprosesan data dan pada setiap elemen pengkomputeran.

060201 Data-dalam-Simpanan	
Gunakan teknologi yang bersesuaian untuk melindungi data-dalam-simpanan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-simpanan.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

Maklumat Rahsia Rasmi, Maklumat Rasmi dan *Personally Identifiable Information* (PII) perlu dilindungi daripada segi kerahsiaan dan integriti data. Data Terbuka perlu dilindungi daripada segi integriti data.	

060202 Data-dalam-Pergerakan

Gunakan teknologi yang bersesuaian untuk melindungi data-dalam-pergerakan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data-dalam-pergerakan.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

060203 Data-dalam-Penggunaan

Gunakan teknologi yang bersesuaian untuk melindungi data-dalam-penggunaan bagi menghalang capaian data yang tidak dibenarkan dan memelihara integriti data. Di samping itu, teknologi untuk menentukan asal data dan tanpa sangkalan mungkin diperlukan. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk melindungi data dalam penggunaan. Teknologi untuk memastikan asal data dan data / transaksi tanpa-sangkal boleh digunakan oleh Jabatan.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

060204 Perlindungan Ketirisan Data

Teknologi perlindungan ketirisan data bertujuan untuk menghalang pengguna yang sah daripada menyebarkan maklumat tanpa kebenaran. Teknologi dan langkah-langkah perlindungan hendaklah dipilih berdasarkan penilaian risiko untuk menghalang atau mengesan ketirisan data.	Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

PERKARA 07

PENGURUSAN OPERASI DAN KOMUNIKASI

PERKARA 07: PENGURUSAN OPERASI DAN KOMUNIKASI

0701 Pengurusan Prosedur dan Operasi

Objektif:

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

070101 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*, penyelenggaraan perkakasan ICT di dalam Bilik Server/ Pusat Data dan pengurusan pengendalian mel *elektronik* hendaklah direkodkan; Semua prosedur hendaklah direkodkan dan dikemaskini dari masa ke semasa atau mengikut keperluan. Tugas dan tanggungjawab perlu diasingkan bagi mengurangkan risiko kecuaian dan penyalahgunaan aset ICT organisasi. Kemudahan ICT untuk pembangunan, pengujian dan operasi mestilah diasingkan bagi mengurangkan risiko capaian atau pengubahsuaian secara tidak sah kepada sistem yang sedang beroperasi.	Pentadbir Sistem ICT dan Pengguna

070102 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, menyelenggara, 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.	Pentadbir Sistem ICT dan Pengguna

070103 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; d) Menyediakan tindakan pemulihan segera; dan e) Melaporkan kepada pihak pengurusan atasan.	ICTSO dan Pentadbir Sistem ICT

0702 Perancangan dan Penerimaan Sistem

Objektif:

Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

070201 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 perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang. Penggunaan perkakasan mestilah dipantau, ditala (*tuned*) dan perancangan perlu dibuat bagi memastikan prestasi sistem di tahap optimum sepanjang masa.	ICTSO dan Pentadbir Sistem ICT

070202 Penerimaan Sistem dan Keselamatan di dalam Membangunkan Sistem Aplikasi	
Semua sistem baru (termasuklah sistem yang sedang dibangunkan, dikemaskini, dinaiktaraf atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui seperti berikut: a) Pembangunan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujud sebarang *vulnerability* yang boleh mengganggu pemprosesan dan ketepatan maklumat; b) Ujian keselamatan sistem hendaklah dijalankan seperti berikut: i. Semakan pengesahan dan integriti data yang dimasukkan; ii. Menentukan sama ada program berfungsi dengan betul dan sempurna berdasarkan aliran proses dan kerja; dan iii. Memastikan ketepatan (output) maklumat yang dipaparkan. c) Persetujuan kawalan keselamatan; d) Memenuhi kapasiti dan prestasi yang ditetapkan; e) Prosedur *error recovery* dan *restart* termasuk pelan kecemasan;	Pentadbir Sistem ICT dan ICTSO

f) Persediaan dan pengujian berterusan bagi mengenalpasti piawaian dan prosedur; g) Dokumen (manual) prosedur yang berkesan; dan h) Latihan penggunaan sistem baharu.	

0703 Perisian Berbahaya

Objektif:

Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti *virus, trojan* dan sebagainya.

070301 Perlindungan daripada Perisian Berbahaya	
Di dalam proses pengendalian perisian dan maklumat, perkara-perkara berikut perlu diambil perhatian: a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti *antivirus* atau sistem pengesanan pencerobohan (IDS) dan mengikut prosedur penggunaan yang betul dan selamat; b) Memasukkan klausa tanggungan perlindungan daripada perisian berbahaya di dalam kontrak yang ditawarkan kepada pihak ketiga. Klausa ini bertujuan untuk tuntutan baik pulih 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 sebelum menggunakannya; g) Memastikan *anti virus pattern* sentiasa dikemaskini; h) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; dan i) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya.	ICTSO, Pentadbir Sistem ICT dan Pengguna

070302 Perlindungan daripada *Mobile Code*	
Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pentadbir Sistem ICT

0704 *Housekeeping*

Objektif:

Melindungi integriti maklumat dan perkhidmatan komunikasi agar sentiasa tersedia dan bebas risiko kegagalan akses pada bila-bila masa.

070401 Sistem *Backup*	
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali terdapat perubahan konfigurasi. 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 kritikal ICT sekurang-kurangnya satu (1) kali setahun atau berdasarkan keperluan disebabkan perubahan konfigurasi atau mana-mana perubahan terkini yang melibatkan perubahan keseluruhan arkitektur *backup*; b) Membuat *backup* ke atas semua data-data dan maklumat-maklumat kritikal secara berkala iaitu harian, mingguan, bulanan dan tahunan; c) Menyimpan sekurang-kurangnya tiga (3) generasi *backup;* d) Melaksanakan pengujian proses *backup* dan *restore* supaya proses ini dapat berfungsi dengan sempurna di dalam memastikan semua data dan maklumat boleh digunakan, boleh dipercayai, berintegriti dan terjamin selamat apabila diperlukan; dan e) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Pentadbir Sistem ICT

070402 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 baik pulih dengan segera; dan c) Laporkan segera kepada ICTSO sekiranya wujud aktiviti-aktiviti tidak sah seperti kecurian maklumat dan pencerobohan.	ICTSO dan Pentadbir Sistem ICT

070403 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Log audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan forensik dan memantau kawalan capaian; b) Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu diwujudkan dan hasilnya perlu dipantau secara berkala; dan c) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem selain mengambil tindakan baik pulih dengan segera.	Pentadbir Sistem ICT

070404 *Clock Synchronization*	
Semua sistem aplikasi JKR termasuk aset ICT berkaitan perlu diselaraskan di bawah satu piawaian kawalan masa yang sama. Pelarasan waktu ini bertujuan untuk memastikan keseragaman dan ketepatan waktu log audit.	Pentadbir Sistem ICT

0705 Pengurusan Rangkaian

Objektif:

Melindungi maklumat di dalam rangkaian dan infrastruktur ICT Jabatan.

070501 Kawalan Infrastruktur Rangkaian	
Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin berpandukan teknologi terkini bagi mengelakkan ancaman terhadap sistem dan aplikasi termasuk data-dalam-pergerakan dan ketirisan data 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) Perkakasan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh, selamat dan bebas risiko seperti banjir, gegaran dan habuk; c) Capaian kepada perkakasan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; d) Semua peralatan mestilah melalui proses *factory acceptance check* (FAC) semasa pemasangan dan konfigurasi; e) *Firewall* hendaklah dipasang di antara rangkaian dalaman dan sistem yang melibatkan maklumat rahsia rasmi Kerajaan serta dikonfigurasi oleh Pentadbir Sistem ICT; f) Semua trafik data yang 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 Pengurus ICT; 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; j) Sebarang penyambungan rangkaian yang bukan di bawah kawalan JKR hendaklah mendapat kebenaran Pengurus ICT;	Pengurus ICT, ICTSO, Pentadbir Sistem ICT dan Pengguna

k) Memastikan keperluan perlindungan ICT adalah bersesuaian dan mencukupi bagi menyokong perkhidmatan yang lebih optimum; l) Semua pengguna hanya dibenarkan untuk menggunakan rangkaian ICT JKR sahaja. Penggunaan modem persendirian pada aset ICT Jabatan seperti *broadband* adalah dilarang sama sekali; dan m) Memastikan terdapat kawalan keselamatan bagi kemudahan rangkaian tanpa wayar LAN.	

070502 Pengauditan dan Forensik ICT

Semua Pentadbir Sistem ICT mestilah bertanggungjawab untuk merekod dan menganalisis perkara-perkara berikut: a) Sebarang percubaan pencerobohan terhadap sistem ICT JKR; 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 pemasangan dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; g) Aktiviti penyalahgunaan akaun e-mel rasmi Kerajaan; h) Aktiviti penukaran alamat IP selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Sistem ICT; dan i) Laksanakan semakan audit keselamatan perlu dengan merujuk kepada Rangka Kerja Siber Sektor Awam (RAKKSSA).	Pentadbir Sistem ICT

0706 Pengurusan Media

Objektif:

Melindungi media yang mengandungi data dari kerosakan dan gangguan aktiviti perkhidmatan yang tidak dikawal.

070601 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	Pengguna

070602 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 mengelakkan 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.	Pentadbir Sistem ICT dan Pengguna

070603 Keselamatan Sistem Dokumentasi	
Sistem dokumentasi perlu mengambilkira perkara-perkara berikut: a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b) Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c) Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Pentadbir Sistem ICT dan Pengguna

0707 Keselamatan Komunikasi

Objektif:

Melindungi aset ICT melalui sistem komunikasi yang selamat.

070701 Internet	
a) Laman-laman yang boleh dilayari, dilanggan dan diguna adalah berbentuk akademik dan pengetahuan serta untuk urusan kerja harian rasmi. 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*, tv / *radio online* dan *video streaming*; c) Bagi melindungi keselamatan dan kerahsiaan data-dalam-simpanan, penggunaan storan awan komersial yang berada di luar premis Pusat Data Jabatan adalah dilarang. Ini juga disebabkan isu kerahsiaan; d) Melayari Internet tanpa tujuan atau meninggalkan capaian Internet yang *unattended* adalah amat tidak beretika dan tidak digalakkan kerana ianya boleh menyebabkan kesesakan rangkaian JKR; e) CIO, Pengurus ICT, ICTSO atau wakil pengurusan berhak menapis, menghalang dan menegah penggunaan atau capaian mana-mana laman web yang dianggap tidak sesuai; f) Pengguna dilarang mengganggu atau menceroboh laman web mana-mana Jabatan, organisasi atau negara; g) Pengguna dilarang masuk, salin, ciplak, cetak dan sebar maklumat daripada Internet yang menyalahi undang-undang negara; h) Pengguna tidak dibenarkan mencapai atau cuba mencapai sumber elektronik (data, paparan, *keystrokes logging*, 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; i) Penggunaan penganalisis rangkaian (*network analyzer*) atau pengintip (*sniffer*) adalah dilarang sama sekali;	Pentadbir Sistem ICT dan Pengguna

j) Pengguna yang mencapai sesuatu perkhidmatan yang perlu dibayar (contohnya pangkalan data *online* komersial), hendaklah bertanggungjawab ke atas segala bayaran yang dikenakan; k) Sebarang salah laku penggunaan Internet yang telah dikenalpasti akan diambil tindakan berdasarkan budi bicara ICTSO, Pengurus ICT atau Jawatankuasa Keselamatan ICT. Tindakan awal sekatan Internet melalui penutupan *port* atau kaedah lain boleh dibuat oleh Pentadbir Sistem ICT; dan l) Pengecualian akses kepada laman web yang disekat boleh dipertimbangkan jika ia bertujuan untuk urusan kerja rasmi bagi tempoh tertentu atas keizinan ICTSO atau Pengurus ICT. Maklumat lanjut mengenai keselamatan Internet hendaklah merujuk kepada **PKPA Bil. 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan".**	

070702 Media Sosial	
Penggunaan jaringan media sosial tanpa kawalan akan menyebabkan gangguan kepada capaian ke atas perkhidmatan *online* yang disediakan kepada pelanggan. Berikut adalah amalan terbaik di dalam penggunaan jaringan media sosial yang perlu dipatuhi: **Pegawai Bertanggungjawab Mengendalikan Laman Web / Media Sosial Jabatan** a) Memastikan kandungan yang tidak bercanggah dengan dasar Jabatan dan Kerajaan; b) Menjadikan laman web sosial sebagai media mempromosi dan memberi publisiti kepada perkara-perkara yang berkaitan dengan Jabatan dan Kerajaan; c) Memastikan kesesuaian kandungan dan mempunyai kepentingan untuk disampaikan kepada orang awam; d) Memastikan kekerapan pengemaskinian maklumat dan memastikan tahap relevan maklumat; e) Menghapuskan kandungan dan maklumat yang diterima daripada orang awam yang tidak relevan dengan aktiviti Jabatan; f) Memastikan bahawa pautan dan kandungan antara laman web sosial dan laman web rasmi Jabatan adalah jelas dan tidak bertindih;	Pentadbir Sistem ICT dan Pengguna

g) Menggunakan logo rasmi Jabatan di dalam laman web sosial;

h) Menggunakan e-mel rasmi di dalam profil laman web sosial;

i) Menggunakan foto dan / atau video yang dapat memperjelaskan mesej yang hendak disampaikan dalam keadaan yang sesuai;

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 sosial tersebut.

Pengguna

a) Mencapai laman web sosial yang hanya berkaitan dengan urusan rasmi Jabatan pada waktu pejabat;

b) Menggunakan ayat yang lengkap dan jelas maksudnya;

c) Tidak memaparkan isu-isu sensitif seperti agama, politik, perkauman, fitnah atau hasutan;

d) Tidak memaparkan kenyataan-kenyataan yang boleh menjejaskan imej Jabatan dan Kerajaan;

e) Tidak memuat naik maklumat Jabatan dan Kerajaan; dan

f) Tidak menggunakan laman web sosial untuk mengaibkan individu tertentu.

Pentadbir Sistem Rangkaian

a) Memastikan pengurusan *content filtering* sentiasa berfungsi di dalam menapis capaian ke laman web sosial yang tiada kaitan dengan kegunaan rasmi Jabatan dan Kerajaan; dan

b) Memantau serta menganalisis transaksi capaian pengguna ke atas laman web sosial luar agar tidak mengganggu prestasi rangkaian Jabatan.

070703 Mel Elektronik	
Penggunaan mel elektronik tanpa kawalan boleh menyebabkan gangguan kepada perkhidmatan JKR. Berikut adalah amalan terbaik di dalam pengurusan dan penggunaan mel elektronik rasmi yang perlu dipatuhi: a) Akaun mel elektronik JKR atau mel elektronik JKR hanya diperuntukkan kepada pegawai dan kakitangan JKR sahaja bagi tujuan penghantaran dan penerimaan data atau maklumat secara rasmi sahaja; b) Sebarang penyalahgunaan mel elektronik akan di ambil tindakan berdasarkan peraturan-peraturan yang berkuatkuasa; c) Pengguna hanya boleh menggunakan dan mengakses akaun atau alamat emel yang diperuntukkan kepadanya sahaja. Penggunaan akaun milik orang lain adalah dilarang dan tidak dibenarkan; d) Penggunaan emel persendirian bagi tujuan rasmi seperti emel *yahoo, gmail, streamyx* dan sebagainya adalah dilarang dan tidak dibenarkan; e) Sebarang penghantaran data atau maklumat menggunakan emel hendaklah dienkrip atau menggunakan sebarang kaedah keselamatan yang terjamin bagi memastikan data atau maklumat yang dihantar adalah dijamin selamat; f) Pengguna adalah dilarang menggunakan emel untuk penghantaran maklumat-maklumat terperingkat dan sulit tanpa menggunakan kaedah keselamatan yang dibenarkan dan terjamin keselamatannya seperti enkripsi, *digital signature*, *public key infrastructure* (PKI) atau sebarang kawalan keselamatan yang bersesuaian. Perhantaran dokumen dan kata laluan perlu di hantar di dalam emel berasingan; g) Penghantaran sebarang fail kepilan yang berkapasiti tinggi adalah tidak digalakkan dan hanya pada kadar kapasiti yang dibenarkan sahaja iaitu **tidak melebihi 10 MB**. Kaedah pemampatan, penggunaan medium kolaborasi dan *secured file sharing* untuk mengurangkan kapasiti fail kepilan adalah disarankan; h) Pengguna hendaklah memastikan emel yang diterima adalah selamat digunakan dengan mengelak daripada membuka emel, kepilan fail atau *link* daripada *spamming mail* atau penghantar yang tidak diketahui dan diragui kewujudannya; i) Pengguna hendaklah memastikan emel penerima adalah emel yang sah sebelum menghantar dan menerima sebarang transaksi data atau maklumat menerusi emel;	Pengguna dan Pentadbir Sistem ICT

j) Pengguna adalah dilarang menggunakan apa-apa cara sekalipun untuk menyamar dan menggunakan emel orang lain sebagai penghantar emel yang sah. Sebarang penyalahgunaan emel akan di ambil tindakan berdasarkan peraturan-peraturan yang berkuatkuasa; k) Sebarang penyalahgunaan emel yang telah dikenalpasti akan diambil tindakan serta merta dengan dinyahaktifkan penggunaannya sehingga proses pembaikan dan pencegahan dilaksanakan; l) Akaun emel yang tidak aktif sekurang-kurangnya **selama tiga (3) bulan** akan dinyahaktifkan dan seterusnya akaun tersebut serta data akan dihapuskan dalam tempoh tiga (3) bulan berikutnya; m) Bagi pengguna yang tidak lagi menggunakan emel rasmi JKR disebabkan berhenti, bersara, bertukar dan sebagainya akan dinyahaktifkan dalam tempoh **14 hari** atau serta merta mengikut keperluan; n) Pengguna adalah dilarang melibatkan diri di dalam aktiviti mel bom, mel sampah, mel *spam* dan sebarang aktiviti menggunakan emel rasmi JKR bagi tujuan yang tidak dibenarkan, menganggu dan memberikan ancaman kepada Jabatan dan Pengguna emel; o) Pengguna hendaklah bertanggungjawab ke atas akaun emel masing-masing dengan memastikan kerahsiaan dan penukaran berkala kata laluan emel, mematuhi kapasiti emel yang dibenarkan, melaksanakan *housekeeping mailbox* dan sebagainya. Kegagalan melakukan yang sedemikian boleh menyebabkan prestasi dan tahap keselamatan emel dikompromi; dan p) Pengguna yang menggunakan emel *client* seperti *Microsoft Outlook*, *mobile client* emel atau sebarang perisian emel *client* hendaklah memastikan perisian, perkakasan dan peranti mudah alih yang digunakan adalah terjamin keselamatannya daripada sebarang ancaman dan pencerobohan.	

PERKARA 08

KAWALAN CAPAIAN

PERKARA 08: KAWALAN CAPAIAN

0801 Dasar Kawalan Capaian

Objektif:

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

080101 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 ICT

080102 Pendaftaran / Nyah Daftar Pengguna	
Prosedur formal berkaitan pendaftaran / nyah daftar mestilah diwujudkan untuk memberi atau mengambil kembali capaian ke atas semua sistem aplikasi dan perkhidmatan ICT JKR.	Pemilik Sistem, Pentadbir Sistem ICT

080103 Pengurusan Keistimewaan Capaian	
Pemberian hak keistimewaan capaian kepada pengguna tertentu perlulah dihadkan dan dikawal.	Pemilik Sistem, Pengguna dan Pentadbir Sistem ICT

0802 Pengurusan Capaian Pengguna

Objektif:

Mengawal capaian pengguna ke atas aset ICT Jabatan.

080201 Akaun Pengguna	
Pengguna, Pemilik Sistem, Pentadbir Sistem ICT dan Pihak Ketiga adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, beberapa peraturan telah ditetapkan seperti berikut: **Pengguna:** a) Akaun yang diperuntukkan oleh Jabatan sahaja boleh digunakan; b) Akaun pengguna atau ID mestilah unik dan mencerminkan identiti pengguna; c) Akaun pengguna sistem aplikasi yang diwujudkan pertama kali melalui *single sign on* (SSO) akan diberi tahap capaian mengikut peranan dan sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada Pemilik Sistem terlebih dahulu; d) Pemilikan akaun pengguna bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan Jabatan. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; dan e) Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang. **Pentadbir Sistem ICT:** a) Peranan Pentadbir Sistem ICT boleh diberikan kepada pengguna tertentu di dalam sistem. Pentadbir Sistem ICT boleh diberi dan dilucutkan oleh pentadbir lain. Sekurang-kurangnya dua (2) orang pentadbir diperlukan bagi satu-satu sistem; b) Pentadbir Sistem ICT yang dilantik mestilah menggunakan ID sendiri untuk log masuk kepada sistem. Penggunaan ID dengan akaun *admin* atau *root* adalah tidak dibenarkan.	Pemilik Sistem, Pentadbir Sistem ICT, Pengguna dan Pihak Ketiga

c) Akaun Pentadbir Sistem atau ID mestilah unik dan hendaklah mencerminkan identiti pengguna; dan d) Pentadbir Sistem ICT boleh membeku dan menamatkan akaun pengguna atas sebab-sebab berikut; i. Pengguna bercuti panjang atau menghadiri kursus di luar pejabat dalam tempoh waktu melebihi tiga (3) bulan; ii. Melanggar peraturan yang telah ditetapkan dalam DKICT; iii. Bertukar bidang tugas / kerja (untuk sistem aplikasi); iv. Bertukar keluar ke agensi lain (kecuali staf JKR); v. Bersara; vi. Ditamatkan perkhidmatan; atau vii. Pengguna luar yang telah tamat kontrak dan perkhidmatan dengan Jabatan. **Pihak Ketiga:** a) Permohonan penggunaan sistem mestilah diisi melalui borang seperti yang dikuatkuasakan oleh Jabatan dan dengan keizinan Pemilik Sistem; b) Akaun pengguna sistem aplikasi yang diwujudkan pertama kali melalui SSO akan diberi tahap capaian mengikut peranan dan sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada Pemilik Sistem terlebih dahulu; c) Akaun yang diberikan boleh digunakan dalam satu tempoh masa yang tertentu sahaja yang telah ditetapkan oleh Pentadbir Sistem ICT; d) Tidak boleh menyalahgunakan akaun yang telah diberikan untuk kepentingan sendiri kerana akaun yang diberikan adalah hak milik Kerajaan Malaysia; dan e) Akaun pengguna atau ID mestilah unik dan hendaklah mencerminkan identiti pengguna.	

080202 Jejak Audit	
Jejak audit akan merekodkan semua aktiviti sistem yang diguna pakai oleh pengguna. Jejak audit juga adalah penting dan digunakan untuk tujuan penyiasatan sekiranya berlaku kerosakan atau penyalahgunaan sistem. Aktiviti jejak audit mengandungi:	Pentadbir Sistem ICT

a) Maklumat identiti pengguna, sumber yang digunakan, perubahan maklumat yang dibuat, tarikh dan masa aktiviti, rangkaian dan program yang digunakan; b) Aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; dan c) Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak memaparkan ciri-ciri keselamatan. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari masa ke semasa dan menyediakan laporan, jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	

080203 Hak Capaian

Penetapan dan penggunaan hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT

080204 Pengurusan Kata Laluan

Pemilihan, penggunaan dan pengurusan kata laluan sebagai akses utama untuk mencapai maklumat di dalam sistem aplikasi mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh JKR 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 apabila disyaki berlakunya kebocoran atau dikompromi; c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara, angka dan simbol; 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 tidak boleh dipaparkan semasa input, di dalam laporan atau media lain serta tidak boleh dikodkan di dalam program;	Pentadbir Sistem ICT dan Pengguna

g) Kuatkuasakan pertukaran kata laluan semasa log masuk kali pertama atau selepas kata laluan diset semula; h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; i) Tentukan had masa pengesahan dengan maksimum selama lima (5) minit (mengikut kesesuaian sistem aplikasi) dan selepas had itu, sesi perlu ditamatkan; j) Kata laluan perlu ditukar dalam tempoh tiga (3) bulan; dan k) Elakkan penggunaan semula tiga (3) kata laluan yang terkini.	

080205 *Clear Desk* dan *Clear Screen*

Semua maklumat di 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 kata laluan *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

0803 Kawalan Capaian Maklumat dan Aplikasi

Objektif:

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

080301 Capaian Maklumat dan Aplikasi

Capaian sistem dan aplikasi di JKR adalah terhad kepada pengguna dan tujuan yang dibenarkan sahaja. Untuk memastikan kawalan capaian sistem dan aplikasi yang kukuh, langkah-langkah berikut hendaklah dipatuhi:	ICTSO dan Pentadbir Sistem ICT

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 di dalam 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 kata laluan 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. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	

0804 Perkakasan Komputer Mudah Alih

Objektif :

Memastikan keselamatan maklumat apabila menggunakan kemudahan atau perkakasan komputer mudah alih.

080401 Penggunaan Perkakasan Komputer Mudah Alih	
a) Merekodkan aktiviti keluar masuk penggunaan perkakasan 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 c) Semua peralatan mudah alih seperti telefon pintar, *tablet* dan komputer riba dan sebarang *mobile devices* 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*);	Pengguna

ii. Keselamatan peralatan adalah di bawah tanggungjawab pengguna; iii. Memastikan tiada perisian atau *bugs* yang boleh mengganggu gugat keselamatan rangkaian JKR; dan iv. Penggunaan adalah atas urusan rasmi sahaja.	

080402 *Bring Your Own Device* (BYOD)

Bring Your Own Device atau BYOD adalah merupakan perkakasan mudah alih persendirian atau yang dibekalkan oleh Kerajaan seperti telefon pintar, tablet, komputer riba dan sebarang *mobile devices* yang digunakan untuk tujuan rasmi dan semua perkhidmatan ICT JKR. Pengguna hendaklah memastikan keselamatan penggunaan peralatan mudah alih peribadi seperti berikut: **Langkah 1: Kurangkan Risiko dengan menggunakan Pengurusan Peralatan Mudah Alih (*Mobile Device Management*)** a) Semua kawalan terhadap telefon pintar, *tablet*, komputer riba dan sebarang *mobile devices* peribadi adalah menjadi tanggungjawab Pengguna. b) Sebarang pertukaran dan penggantian peralatan mudah alih peribadi adalah hak Pengguna. Walau bagaimanapun data yang direkod, disimpan dan dihantar keluar yang melibatkan data dan maklumat Kerajaan hendaklah dipantau dan diurus dengan selamat. c) Semua Pengguna hendaklah mendaftarkan peralatan mudah alih yang digunakan apabila menggunakan Perkhidmatan ICT JKR untuk mencapai data dan maklumat di JKR. Ini bagi meminimakan potensi ancaman yang besar seperti kehilangan data apabila berlaku insiden seperti kehilangan telefon pintar atau *tablet*. d) Penggunaan tool Pengurusan Peralatan Mudah Alih boleh membantu memudahkan pengurusan berikut: i. Konfigurasi peralatan mudah alih; ii. Agihan dan capaian perisian / aplikasi; iii. Enkripsi dan pengurusan kata laluan; iv. *Backup dan restore;* dan v. *Remote wipe and lock.*	Pengguna

Langkah 2: Kurangkan Risiko Muat Turun Aplikasi Melalui Polisi dan Latihan

a) Aplikasi yang dimuat turun oleh warga JKR melalui Internet ke dalam peralatan mudah alih boleh mendatangkan ancaman dan risiko serta impak yang besar terhadap keselamatan apabila peranti yang sama digunakan untuk mencapai maklumat dan aplikasi rasmi JKR. Pengguna perlu memastikan kawalan terhadap aplikasi yang dimuat turun terutamanya daripada sumber yang tidak diketahui yang berkemungkinan mengandungi ancaman virus atau *malicious code*;

b) Pengguna hendaklah memastikan setiap aplikasi yang dimuat turun tidak mempunyai keupayaan untuk memuat naik maklumat dan fail yang disimpan dalam peranti pintar peribadi secara sulit dan tidak diketahui oleh pemiliknya; dan

c) Pengguna hendaklah memastikan supaya sebarang muat turun aplikasi menggunakan peralatan mudah alih yang dibenarkan perlu dibuat melalui sumber yang dipercayai seperti *trusted AppStore*.

Langkah 3: Membangunkan Aplikasi Secara Dalaman

a) Pembangunan aplikasi mudah alih (*mobile apps*) secara dalaman adalah digalakkan dengan mematuhi metodologi pembangunan sistem yang selamat;

b) Setiap aplikasi yang dibangunkan ini hendaklah menyediakan kaedah *authentication* sebelum capaian ke atas data dan maklumat dibenarkan; dan

c) Pembangunan aplikasi secara dalaman ini merupakan salah satu langkah terbaik membenarkan warga JKR memuat turun aplikasi daripada sumber yang dipercayai.

Langkah 4: Melaksanakan Audit Keselamatan Terhadap Peralatan, Infrastruktur dan Aplikasi Mudah Alih

a) Keselamatan peralatan mudah alih perlu mengambil kira keseluruhan arkitektur keselamatan peralatan, infrastruktur dan aplikasi mudah alih yang dilaksanakan serta mematuhi DKICT JKR.

b) Pelaksanaan audit keselamatan perlu meliputi aspek berikut:

   i. Membuat penilaian terhadap infrastruktur ICT mudah alih;

   ii. Melaksanakan ujian penembusan (*penetration test*) terhadap peralatan mudah alih dan *server* yang terlibat;

iii. Membuat penilaian terhadap keselamatan aplikasi bagi menentukan jika terdapat kemungkinan berlaku kebocoran maklumat; dan iv. Menilai jurang antara polisi dan prosedur yang dikuatkuasakan dengan amalan terbaik.	

080403 Capaian Jarak Jauh (*Teleworking*)

a) Capaian jarak jauh yang dimaksudkan merangkumi: i. Capaian daripada sistem rangkaian dalaman; dan ii. Capaian daripada sistem rangkaian luaran bagi lokasi luar pejabat untuk tujuan *telecommuting*. b) Pengguna JKR boleh diberi capaian berdasarkan fungsi kerja mereka untuk memastikan kerahsiaan dan integriti data yang dihantar pada rangkaian tersebut; c) Penghantaran maklumat yang menggunakan capaian jarak jauh mestilah menggunakan kaedah enkripsi; d) Lokasi bagi akses ke sistem ICT JKR hendaklah dipastikan selamat; dan e) Penggunaan perkhidmatan ini hendaklah mendapat kebenaran daripada Pengurus ICT. Pengguna yang diberi hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	Pentadbir Sistem ICT, Pengguna

0805 Kawalan Capaian Sistem Pengoperasian

Objektif:

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

080501 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.	Pentadbir Sistem ICT

Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a) Mengesahkan pengguna yang dibenarkan; b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi 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.	

080502 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 09

PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

PERKARA 09: PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

0901 Keselamatan di dalam Membangunkan Sistem dan Aplikasi

Objektif:

Memahami dan mematuhi keperluan keselamatan dalam membangun dan menyelenggara sistem aplikasi Jabatan.

090101 Keperluan Keselamatan

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. 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) Persekitaran pembangunan sistem mestilah selamat secara fizikal dan logikal; d) 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; e) Semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu dengan *Load, Stress* dan *Penetration Test* bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan; f) Aplikasi perlu mengandungi semakan pengesahan (*validation and verification*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; g) 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; h) *Outsourced* hosting tidak dibenarkan menggunakan domain jkr.gov.my atau jkr.my;	Pengurus ICT, Pentadbir Sistem ICT, Pemilik Sistem dan ICTSO

i) Aspek keselamatan hendaklah dimasukkan ke dalam semua fasa kitar hayat pembangunan sistem termasuk penetapan konsep, perisian, pengumpulan keperluan, reka bentuk, pelaksanaan, ujian, penerimaan, pasang atur, penyelenggaraan dan pelupusan. Perancangan bagi Pelan Pengurusan Keselamatan Maklumat disarankan mengikut peringkat yang diterangkan dalam kebanyakan model Kitar Hayat Sistem ICT; dan j) Sistem aplikasi perlu dikaji semula sekiranya terdapat keperluan, untuk memastikan pematuhan kepada maklumat dan keperluan Jabatan yang terkini.	

0902 Kriptografi

Objektif:

Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui teknologi kriptografi.

090201 Enkripsi	
Pastikan semua maklumat sensitif atau maklumat rahsia rasmi menggunakan kaedah enkripsi atau penyulitan dan dekripsi atau penyah sulitan pada setiap kali penghantaran dan penerimaan data atau maklumat dilaksanakan.	Pengurus ICT, Pentadbir Sistem ICT, Pemilik Sistem dan Pengguna

090202 Tandatangan Digital	
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pengurus ICT, Pentadbir Sistem ICT, Pemilik Sistem dan Pengguna

090203 Pengurusan Infrastruktur Kunci Awam (PKI)	
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci (*public* dan *private key*) berkenaan daripada diubah, dimusnah atau didedahkan sepanjang tempoh sah kunci tersebut.	Pengurus ICT, Pentadbir Sistem ICT, Pemilik Sistem dan Pengguna

0903 Fail Sistem

Objektif:

Memastikan supaya fail sistem dikawal dan dikendalikan dengan baik dan selamat.

090301 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 di dalam *development*, *testing* atau *staging environment*; c) Capaian ke atas kod atau aturcara program perlu dikawal bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; dan d) Aktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT dan Pemilik Sistem

0904 Keselamatan di dalam Proses Pembangunan dan Sokongan

Objektif:

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

090401 Kawalan Perubahan

a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkod 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 disengajakan; dan c) Prosedur kawalan perubahan konfigurasi hendaklah diwujud dan dilaksanakan bagi perubahan kepada sistem, termasuk tampalan perisian, pakej perkhidmatan, konfigurasi rangkaian dan pengemaskinian sistem pengoperasian.	Pentadbir Sistem ICT dan Pemilik Sistem

090402 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 Kerajaan. Pihak ketiga tidak dibenarkan menggunakan semula kod sumber yang sama untuk pembangunan sistem yang lain tanpa kebenaran Jabatan. Perolehan produk tempatan atau yang dibangun menggunakan teknologi tempatan hendaklah diberi keutamaan dalam pembangunan dan keseluruhan kitar hayat sistem. Kakitangan dan sumber berkaitan sistem hendaklah dipilih untuk mengurangkan kebergantungan kepada sumber luaran, kepakaran dan teknologi asing.	Pentadbir Sistem ICT, Pemilik Sistem dan Pihak ketiga

0905 Kawalan Teknikal Keterdedahan (*Vulnerability*)

Objektif:

Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

090501 Kawalan daripada Ancaman Teknikal	
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti: a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; c) Mewujud dan melaksanakan jaminan kualiti ke atas semua sistem aplikasi yang dibangunkan; dan d) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT dan ICTSO

PERKARA 10

RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

PERKARA 10: RISIKO DAN PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

1001 Risiko

OBJEKTIF:
Memastikan setiap risiko berkaitan aset ICT dapat dikenalpasti, dinilai dan diambil tindakan bagi meminimumkan insiden keselamatan.

100101 Tafsiran Risiko	
Risiko adalah keberangkalian aset tidak mencapai objektifnya. Risiko yang berkaitan dengan aset perlulah dikenal pasti. Penilaian risiko hendaklah dilaksanakan bagi menilai risiko terjejasnya kerahsiaan, integriti dan ketersediaan maklumat dalam aset ICT Jabatan. Penilaian risiko hendaklah dilaksanakan sekurang-kurangnya sekali setahun atau sekiranya berlaku sebarang perubahan kepada persekitaran. Pengolahan risiko hendaklah dikenal pasti dan dilaksanakan. **Kerentanan** Kerentanan adalah kelemahan atau kecacatan aset yang mungkin dieksploitasikan dan mengakibatkan pelanggaran keselamatan. Kerentanan setiap aset hendaklah dikenal pasti sebagai sebahagian daripada proses pengurusan risiko. **Ancaman** Kedua-dua ancaman yang disengajakan atau tidak disengajakan yang mungkin mengeksploitasi sebarang kelemahan mestilah dikenalpasti. **Impak** Impak insiden yang mungkin terjadi mestilah dikenalpastikan. Impak boleh dikategorikan kepada impak teknikal dan impak fungsi Jabatan. Impak teknikal melibatkan perkara-perkara yang menjejaskan kerahsiaan, integriti, ketersediaan dan akauntabiliti manakala impak fungsi Jabatan melibatkan perkara-perkara dari segi kewangan, reputasi, ketidakpatuhan dan perlanggaran privasi.	Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pemilik Sistem dan Pengguna

100102 Tahap Risiko	
Tahap risiko ditentukan daripada ancaman, kebarangkalian dan impak risiko. Kaedah penentuan tahap risiko hendaklah mengikut polisi penilaian atau pengurusan risiko yang sedang berkuat kuasa.	Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pemilik Sistem dan Pengguna

100103 Pengolahan Risiko	
Pengolahan risiko merangkumi elemen proses, teknologi dan manusia hendaklah dikenal pasti dan dilaksana berdasarkan hasil penilaian risiko. Pengolahan risiko hendaklah dikenal pasti untuk menentukan sama ada perlu dielakkan, dikurangkan, diterima atau dipindahkan dengan mengambil kira kos/faedahnya. Baki risiko adalah risiko yang tinggal atau berbaki selepas pengolahan risiko dilaksanakan. Ancaman berkaitan baki risiko dan risiko yang diterima hendaklah dipantau secara berkala. **a) Teknologi** Teknologi hendaklah dikenal pasti untuk mengelak atau mengurangkan risiko. Sebagai contoh, *firewall* digunakan untuk menghadkan capaian logikal kepada sistem tertentu. **b) Proses** Pengolahan risiko, membangunkan atau mengemaskini perekayasaan proses (*process re-engineering*), Prosedur Operasi Piawaian (*standard operating procedure*) dan polisi perlulah dilaksanakan. **c) Manusia** Sumber manusia berkelayakan dan kompeten mestilah dikenalpastikan. Ia perlu mencukupi serta memastikan pengurusan sumber manusia dilaksanakan sebagai pengolahan risiko yang berkesan.	Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pemilik Sistem dan Pengguna

100104 Pengurusan Risiko	
Pengurusan risiko perlu dilaksanakan untuk: a) Mengenal pasti kerentanan; b) Mengenal pasti ancaman; c) Menilai risiko; d) Menentukan pengolahan risiko; e) Memantau keberkesanan pengolahan risiko; dan f) Memantau ancaman yang berkaitan dengan baki risiko dan risiko yang diterima.	

1002 Mekanisme Pelaporan Insiden Keselamatan ICT

Objektif:

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

100201 Mekanisme Pelaporan	
Insiden keselamatan ICT bermaksud musibah yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar DKICT 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 disyaki 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, disyaki dicuri atau disyaki 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.	Pemilik Sistem, Pentadbir Sistem ICT dan Pengguna

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.	

1003 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:

Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.

100301 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT

Semua maklumat berkaitan insiden keselamatan ICT perlu direkod, disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan, pembetulan dan pembelajaran bagi mengawal kekerapan, kerosakan, kos bagi insiden yang akan berlaku dan meminimumkan kesan serta impak kepada Jabatan. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah direkod, disimpan dan diselenggara. 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 kontigensi 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 ICT

PERKARA 11

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

PERKARA 11: PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1101 Dasar Kesinambungan Perkhidmatan

Objektif:

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

110101 Pengurusan Kesinambungan Perkhidmatan	
Pengurusan Kesinambungan Perkhidmatan (*Business Continuity Management - BCM*) hendaklah disediakan 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, pihak berkuasa tempatan dan lain-lain; iii. *Fallback procedure* – menyediakan lokasi sementara jika perkhidmatan tidak dapat diperolehi dengan segera (contoh: *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 membangun dan memastikan Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan* – BCP) dipatuhi; d) Mendokumentasikan proses dan prosedur yang telah dipersetujui untuk mengelakkan risiko yang akan menjejaskan kesinambungan perkhidmatan; e) Mengadakan program kesedaran dan latihan tentang proses dan prosedur kesinambungan perkhidmatan secara berterusan dan efektif;	CIO, Pengurus ICT, ICTSO dan Pentadbir Sistem ICT

f) Membuat jadual pengujian dan mengemaskini (menambahbaik) pelan BCP sekurang-kurangnya setahun sekali atau sekiranya terdapat keperluan; g) Membuat *backup;* h) Membuat ujian storan semula data (*full data restoration*) untuk pastikan data tersebut masih boleh diguna pakai atau tidak dengan kekerapan sekurang-kurangnya setahun sekali atau mengikut keperluan pengguna atau arahan dari pihak atasan; dan i) Salinan pelan BCM perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama.	

PERKARA 12

PEMATUHAN

PERKARA 12: PEMATUHAN

1201 Pematuhan dan Keperluan Perundangan

Objektif:

Meningkatkan tahap keselamatan ICT bagi mengelak pelanggaran DKICT JKR.

120101 Pematuhan Dasar	
Setiap pengguna di JKR hendaklah membaca, memahami dan mematuhi Dasar 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 hak milik Kerajaan dan Ketua Jabatan berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain daripada tujuan yang telah ditetapkan. Penggunaan dan pengendalian data digital perlu mematuhi prosedur-prosedur yang telah ditetapkan.	Pengguna

120102 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) *Malaysia Management Information System* (MyMIS);	Pengguna

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 Wayar 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;

o) Arahan Teknologi Maklumat 2007 (MAMPU); dan

p) Dasar, Peraturan dan Pekeliling-pekeliling yang sedang berkuatkuasa.

Hukuman bagi pelanggaran keselamatan perlu dikenalpasti dan dikuatkuasakan oleh KPKR mengikut perintah Am Bab D dan pekeliling berkuatkuasa. Semua kesalahan jenayah hendaklah dikuatkuasakan oleh PDRM (jika berkenaan) manakala SKMM merupakan agensi berkaitan untuk menguatkuasakan Akta Komunikasi dan Multimedia 1998 (Akta 588) termasuk Akta Tandatangan Digital 1997 (Akta 562).

SENARAI LAMPIRAN

LAMPIRAN A

SURAT AKUAN PEMATUHAN
DASAR KESELAMATAN ICT (DKICT) JKR

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Unit/Bahagian/Cawangan/ Daerah/Negeri atau Nama Agensi Kerajaan atau Nama Syarikat : .....

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:

1. Saya telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT (DKICT) JKR; dan
2. Sekiranya saya ingkar atau melanggar dasar dan peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

Tandatangan : .....

Tarikh : .....

Pengesahan Pegawai Keselamatan ICT (ICTSO) JKR:

.....

(Pegawai Keselamatan ICT JKR)

b.p. Ketua Pengarah JKR Malaysia

Tarikh: .....

LAMPIRAN B

SURAT AKUAN

AKTA RAHSIA RASMI 1972

(MENGGUNAKAN PERKHIDMATAN KERAJAAN)

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 di 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 akuan selanjutnya bagi maksud ini apabila meninggalkan Perkhidmatan Awam.

Tandatangan : .....

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Unit/Bahagian/Cawangan/Daerah/Negeri/ Nama Agensi Kerajaan atau Nama Syarikat : .....

No Telefon : .....

Tarikh : .....

Cop :

Disaksikan Oleh : .....

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Unit/Bahagian/Cawangan/Daerah/Negeri/ Nama Agensi Kerajaan atau Nama Syarikat : .....

No Telefon : .....

Tarikh : .....

Cop :

LAMPIRAN C

SURAT AKUAN

AKTA RAHSIA RASMI 1972

(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, isyarat timbal atau kata jodoh 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 (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Unit/Bahagian/Cawangan/Daerah/Negeri/ Nama Agensi Kerajaan atau Nama Syarikat : .....

No Telefon : .....

Tarikh : .....

Cop :

Disaksikan Oleh : .....

Nama (Huruf Besar) : .....

No. Kad Pengenalan : .....

Jawatan : .....

Unit/Bahagian/Cawangan/Daerah/Negeri/ Nama Agensi Kerajaan atau Nama Syarikat : .....

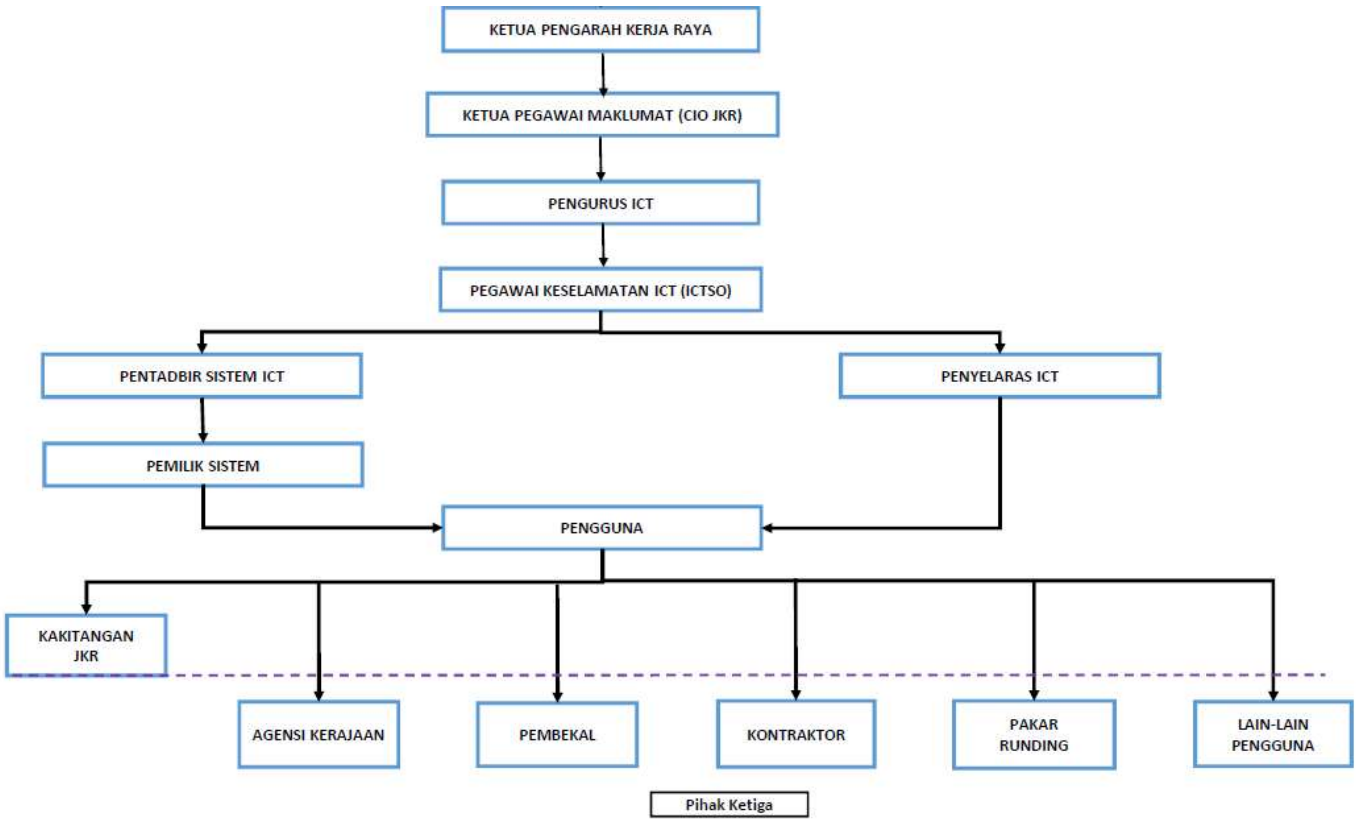
No Telefon : .....

Tarikh : .....

Cop :

LAMPIRAN D

STRUKTUR TADBIR URUS KESELAMATAN ICT JKR



LAMPIRAN E

JADUAL PINDAAN DASAR KESELAMATAN ICT (DKICT) JKR

VERSI ASAL (3.0)			HASIL PINDAAN BAHARU (VERSI 4.0)	MUKA SURAT
PERKARA	**BIL. PINDAAN**	**TOPIK DIPINDA**		
01 Dasar dan Garis Panduan Keselamatan ICT	1	Tajuk	01 Dasar Keselamatan ICT	5
	2	010103	Tambahan ayat "perubahan piawaian antarabangsa ISO/IEC"	6
02 Organisasi Keselamatan ICT	3	020102	Kemaskini ayat "c) ...dan menguatkuasakan pelaksanaan DKICT di Jabatan"	10
	4	020103	Semua para petikan dibuang.	-
	5		Tambahan skop tugas Pengurus ICT dengan para (d), (e) dan (f).	10
	6	020104	Kemaskini ayat pada para (f) "Memaklumkan insiden keselamatan ICT kepada Pengurus ICT"	11
	7		Tambahan skop tugas ICTSO dengan para (i), (j)	11
	8	020105	Tambahan para (f)	12
	9	0201	Tambahan sub perkara baharu "020106 Pemilik Sistem"	12
	10	020106	Kemaskini ayat para (c) "Menyimpan dan menyelenggara rekod aset ICT dan melaporkan kepada pegawai Aset alih di bawah kawalannya;"	13
	11		Tambahan para baharu (e)	
	12	0201	Tambahan sub perkara baharu "020110 Jawatankuasa Tindak balas Insiden Keselamatan ICT (CERT) JKR"	15
03 Pengurusan Aset ICT	13	030101	Tambahan para "Pengguna dan pihak ketiga hendaklah memulangkan semua aset ... sehingga ... *intellectual property* oleh pengguna dan pihak ketiga yang ditamatkan."	19
	14	030102	Semua para petikan dibuang.	-

	15	030201	Tambahan para "Semua maklumat yang dijana… sehingga …Rasmi boleh juga mengandungi Data Terbuka.	20
	16	030202	Tambahan para "Jabatan hendaklah mengenalpasti … kawasan terperingkat"	20
04 Keselamatan Sumber Manusia	Tiada pindaan			
05 Keselamatan Fizikal	17	050301	Kemaskini ayat pada para (q)	32
	18	050306	Kemaskini ayat pada para (f)	35
-	19	-	Tambahan perkara baharu "06 Keselamatan Data" berdasarkan RAKKSSA	36-38
06 Pengurusan Operasi dan Komunikasi	20	Tajuk	Perubahan tajuk perkara kepada "07 Pengurusan Operasi dan Komunikasi"	39
	21	060401	Kemaskini ayat pada para (a)	44
	22	0604	Tambahan sub perkara baharu "070404 *Clock Synchronisation*"	45
	23	0605	Kemaskini ayat pada "070501 Kawalan Infrastruktur Rangkaian"	46
	24		Tambahan para (m)	47
	25	060701	Tambahan para (c), (j) dan (k)	49-50
	26	060703	Kemaskini ayat pada para (m)	53
07 Kawalan Capaian	27	Tajuk	Perubahan tajuk perkara kepada "08 Kawalan Capaian"	55
	28	0701	Tambahan sub perkara baharu "080102 Pendaftaran / Nyah Daftar Pengguna"	55
	29		Tambahan sub perkara baharu "080103 Pengurusan Keistimewaan Capaian"	55
	30	070201	Kemaskini keseluruhan ayat sub perkara.	56
	31	0704	Tambahan sub perkara baharu "080403 Capaian Jarak Jauh (*Teleworking*)"	63
08 Pembangunan dan Penyelenggaraan Sistem	32	Tajuk	Perubahan tajuk perkara kepada "09 Pembangunan dan Penyelenggaraan Sistem"	66
	33	080101	Tambahan para (i) dan (j)	67
	34	080402	Tambahan ayat "Perolehan produk tempatan … hingga …. kepakaran dan teknologi asing."	69

09 Risiko dan Pengurusan Pengendalian Insiden Keselamatan ICT	35	Tajuk	Perubahan tajuk perkara kepada "10 Risiko dan Pengurusan Pengendalian Insiden Keselamatan ICT"	71
	36	-	Tambahan sub perkara baharu "1001 Risiko"	71-73
10 Pengurusan Kesinambungan Perkhidmatan	37	Tajuk	Perubahan tajuk perkara kepada "11 Pengurusan Kesinambungan Perkhidmatan"	76
	38	100101	Tambahan para (j)	77
11 Pematuhan	39	Tajuk	Perubahan tajuk perkara kepada "12 Pematuhan"	79

- DOKUMEN TAMAT -

Bahagian Teknologi Maklumat (BTM)
Cawangan Dasar dan Pengurusan Korporat (CDPK)
Jabatan Kerja Raya (JKR) Malaysia
2017