KEMENTERIAN KERJA RAYA

DASAR KESELAMATAN ICT

KEMENTERIAN KERJA RAYA (KKR)

VERSI 4.1

OKTOBER 2022

www.kkr.gov.my

SEJARAH DOKUMEN

TARIKH	VERSI	KELULUSAN	TARIKH KUATKUASA
2007	1.0		2007
8 Mei 2009	2.0	-	8 Mei 2009
23 Ogos 2017	3.0	22 Nov 2017	11 Dis 2017
26 Feb 2019	3.1	26 Feb 2019	26 Feb 2019
28 Mac 2022	4.0	28 Mac 2022	28 Mac 2022
21 Okt 2022	4.1	21 Okt 2022	21 Okt 2022

JADUAL PINDAAN

TARIKH	VERSI	BUTIRAN PINDAAN
23 Ogos 2017	3.0	1. Pindaan ini juga adalah bagi memenuhi keperluan Standard ISO/IEC 27001 : 2013 *Information Security Management System* (ISMS).
26 Feb 2019	3.1	120101 Mekanisme Pelaporan Insiden m/s 65; • Memasukkan 'PK-KKR-31 (Prosedur Pengurusan Insiden Keselamatan ICT' sebagai perkara 'c' • Menggantikan GCERT MAMPU kepada NACSA
		Singkatan m/s 8; Memasukkan perkara berikut: • NACSA – National Cyber Security Agency • MKN – Majlis Keselamatan Negara
		Lampiran 1 - Surat Akuan Pematuhan DKICT KKR m/s82; • Dikosongkan ruang nama pegawai ICTSO, bagi membolehkan Surat Akuan Pematuhan DKICT KKR boleh disahkan dan ditandatangani oleh Pegawai ICTSO semasa yang dilantik.
		Lampiran 2 - Proses Kerja Pelaporan InsidenKeselamatan ICT (CERT) KKR m/s 83-86
		• Dipinda bagi mematuhi Carta Aliran Proses Kerja Pelaporan Insiden Keselamatan Siber oleh pihak Majlis Keselamatan Negara (MKN) rujukan nombor surat MKN(S0.10.700-8/12/3(20) bertarikh 28 Januari 2019

28 Mac 2022	**4.0**	050303 Capaian Rangkaian Dalaman melalui VPN m/s 35 • Memasukkan prosedur kawalan capaian perkhidmatan rangkaian bagi mengakses sistem-sistem yang diletakkan di dalam *Server Farm* dan sistem intranet. 050304 Penggunaan *Video Conferencing* m/s 35 • Memasukkan prosedur kawalan Penggunaan Video Conferencing dikalangan warga KKR 050305 Simpanan Data dalam Awan (*cloud storage*) m/s 36 • Memasukkan prosedur kawalan Simpanan Data dalam Awan dikalangan warga KKR
21 Okt 2022	**4.1**	7.0 Singkatan m/s 8 • Penggantian terma **CERT** (Computer Emergency Response Team) kepada **CSIRT** (Computer Security Incident Response Team) 020108 Pegawai Keselamatan ICT (ICTSO) m/s 17 • (f) Melaporkan insiden keselamatan ICT kepada **Pasukan Tindak Balas Insiden Keselamatan ICT (CERT)** KKR, CIO dan Pengurus ICT. kepada (f) Melaporkan insiden keselamatan ICT kepada **Pasukan Tindak Balas Insiden Keselamatan Siber (CSIRT)** KKR, CIO dan Pengurus ICT. 020109 Pasukan Tindak Balas Insiden Keselamatan ICT (CERT) KKR m/s 17 0502 Pengurusan Capaian Pengguna 050203 Pindah "Pengurusan Kata Laluan" ke 050502 "Kawalan Capaian Aplikasi dan Maklumat" 050203 Pengurusan Hak Akses Istimewa Tukar tajuk kepada "Penggunaan Maklumat Pengesahan Rahsia (Use of Secret Authentication Information) m/s 33 050205 Pengurusan Maklumat Pengesahan Rahsia Pengguna 050206 Kajian Semula Hak Akses Pengguna

		0502 Pengurusan Capaian Pengguna (penambahan sub-tajuk) 050204 Pengurusan Hak Akses Istimewa m/s 36 050205 Pengurusan Maklumat Pengesahan Rahsia Pengguna m/s 36 050206 Kajian Semula Hak Akses Pengguna m/s 36 050203 Pindah "Pengurusan Kata Laluan" ke 0505 "Kawalan Capaian Aplikasi dan Maklumat" m/s 36 050401 Capaian Sistem Pengoperasian m/s 40 c) Mewujudkan akaun pendua bagi kegunaan pihak ketiga (kakitangan teknikal KKR/Vendor) bagi tujuan menghalang akses kepada dokumen-dokumen terperingkat pemilik komputer/laptop d) Menetapkan akaun pengguna pada level limited bagi mengelakkan pemasangan dan konfigurasi aplikasi/perisian yang tidak dibenarkan. 0506 Peralatan Mudah Alih dan Kerja Jarak Jauh m/s 25 dipindahkan ke Bidang 02 : Organisasi Keselamatan 0203 Peralatan Mudah Alih dan Kerja Jarak Jauh 020301 Peralatan Mudah Alih m/s 25 020302 Kerja Jarak Jauh m/s 25 070104 Kawasan Terhad m/s 46 f) Semua perubahan peralatan/aksesori di Pusat Data hendaklah mendapat kelulusan bertulis dan rekod perubahan hendaklah diselenggara. g) Kerja-kerja pemasangan/pengujian bagi peralatan/peranti/aksesori tambahan hendaklah dilaksanakan di luar Pusat Data (Staging Area) h) Semua aktiviti cetakan adalah TIDAK DIBENARKAN di dalam Pusat Data.

		080102 Kawalan Perubahan m/s 52 • Perkataan menghapus kepada melupus. 080302 Perlindungan daripada Mobile Code m/s 54 • Tambah ayat: Memastikan mobil code yang digunakan adalah daripada sumber yang dipercayai. 080401 Backup dan Restore m/s 54 • Pindaan ayat : asal (a) Melaksanakan backup keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; • Kepada: (a) Melaksanakan backup keselamatan ke atas semua sistem perisian dan aplikasi mengikut Prosedur Backup dan Restore atau setelah mendapat versi terbaru; 0805 Pemantauan m/s 55 • Kemaskini ayat : Objektif : Memastikan aktiviti pemprosesan maklumat yang tidak dibenarkan DAPAT dikesan. 080502 Jejak Audit m/s 55 • Tambah ayat : (a) Setiap sistem dan perkakasan ICT mestilah mempunyai jejak audit; • Buang perkataan : e) Semakan ~~catatan~~ jejak audit hendaklah dilakukan dari semasa ke semasa bagi membantu mengesan aktiviti yang luar biasa dengan lebih awal; 090201 Pengurusan E-mel m/s 58 • Kemaskini ayat : (a) Menggunakan akaun e-mel yang disediakan oleh KKR sahaja; • Tambah ayat : (f) Memastikan e-mel yang diterima adalah dari sumber yang dipercayai dan selamat. 100102 Pengesahan Data Input dan Output m/s 61 • Tambah : Pentadbir Sistem ICT dan Pemilik Sistem

		100206 Prosedur Pembangunan Laman Web dan Aplikasi Web m/s 66 • Tukar tanggungjawab : Pentadbir Sistem ICT, Pentadbir Web dan Ketua Bahagian 100209 Ujian Keselamatan Sistem m/s 67 • Tambah tangungjawab : Pentadbir Pusat Data dan Rangkaian ICT 120101 Mekanisme Pelaporan Insiden m/s 70 • Pindaan dari CERT KKR, GCERT kepada CSIRT • Tanggungjawab : CIO, ICTSO, CSIRT KKR, Pengguna 2. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CSIRT KKR dengan kadar segera apabila: 3. Tindakan terhadap insiden keselamatan siber yang berlaku hendaklah dibuat berasaskan kepada keseriusan sesuatu insiden. Tahap keutamaan tindakan terhadap insiden keselamatan siber akan ditentukan seperti yang berikut: (i) **Keutamaan 1** - insiden keselamatan siber yang memberi impak tinggi terhadap pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan Kerajaan untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu. (ii) **Keutamaan 2 -** insiden keselamatan siber yang tidak memberi impak seperti mana yang dinyatakan dalam Keutamaan 1. Sekiranya berstatus **Keutamaan 1,** agensi hendaklah melaporkan insiden kepada NC4 bagi tujuan penyelarasan dan memaklumkan kepada agensi yang menyelianya dalam tempoh 24 jam selepas insiden dikesan serta mengaktifkan Pelan Kesinambungan Perkhidmatan (Business Continuity Plan, BCP) dan Pelan Pemulihan Bencana (Disaster Recovery Plan, DRP) sekiranya perlu. Bagi **Keutamaan 2**, agensi hendaklah melaksanakan pengendalian insiden secara kendiri dan seterusnya memaklumkan kepada NC4 dan agensi yang menyelianya setelah proses pengendalian insiden dan pemulihan pada peringkat agensi selesai. Dengan berkuat kuasanya Pekeliling Am ini, pekeliling/ surat pekeliling/ surat arahan berikut adalah dibatalkan :

		a) Pekeliling Am Bilangan 1 Tahun 2001 Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); b) Surat Pekeliling Am Bilangan 4 Tahun 2006 Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; dan c) Surat Arahan Ketua Pengarah MAMPU bertarikh 23 Mac 2009 Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-Agensi Kerajaan. Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan kepada Jawatankuasa CERT KKR untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. Apabila berlakunya insiden keselamatan siber, pengarah CSIRT Agensi hendaklah menggerakkan ahli CSIRT Agensi untuk mengambil tindakan seperti yang berikut: (i) Mengurus dan mengambil tindakan terhadap insiden yang berlaku sehingga keadaan pulih. (ii) Mengaktifkan BCP dan/atau DRP jika perlu. (iii) Melapor dan memaklumkan insiden keselamatan siber kepada NC4 serta agensi yang menyelianya. (iv) Menentukan sama ada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang. (v) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti; 120201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT m/s 71 • Pindaan dari CERT KKR, GCERT kepada CSIRT • Tanggungjawab : CIO, ICTSO, CSIRT KKR 130104 Pelan Pengurusan Pemulihan Bencana (Pindaan ayat) m/s 75 (a) Senarai pegawai KKR dan pembekal beserta nombor yang boleh dihubungi (Contohnya: faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel yang tidak dapat hadir untuk

		menangani insiden; (b) Mengenalpasti pejabat alternatif dan/atau pusat pemulihan bencana (Disaster Recovery Centre – DRC) yang berbeza dari lokasi asal bagi meneruskan perkhidmatan apabila lokasi asal menghadapi gangguan/bencana. (c) Mengenalpasti peranan dan tanggungjawab Pasukan Pemulihan Bencana serta pembekal berkaitan; (d) Mengenalpasti system/aplikasi yang memerlukan backup; (e) Menyediakan infrastruktur bagi memastikan pemulihan boleh dilaksanakan; 140107 Pelanggaran Dasar m/s 77 Mengambil tindakan undang-undang dan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan perlanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan akta lain yang berkaitan. SUB (PM) atau ICTSO adalah berhak untuk mengambil tindakan sebagaimana berikut:- .

ISI KANDUNGAN

1.0 PENGENALAN

Dasar Keselamatan ICT (DKICT) Kementerian Kerja Raya (KKR) mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset ICT. Peraturan-peraturan ini perlu difahami dan dipatuhi oleh semua pengguna di KKR. Dasar ini juga menerangkan kepada semua pengguna mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KKR.

2.0 OBJEKTIF

DKICT KKR diwujudkan untuk menjamin kesinambungan urusan KKR dengan meminimumkan kesan insiden keselamatan ICT.

Objektif utama Keselamatan ICT KKR ialah seperti berikut :

(a) Memastikan kelancaran operasi KKR dan meminimumkan kerosakan atau kemusnahan;
(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan daripada segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi;
(c) Meminimumkan kos penyelenggaraan ICT akibat ancaman dan penyalahgunaan; dan
(d) Memperkemaskan pengurusan keselamatan ICT KKR.

3.0 PERNYATAAN DASAR

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

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

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

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

(a) Kerahsiaan – Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;
(b) Integriti – Data dan maklumat hendaklah tepat, lengkap dan kemaskini. Ia hanya boleh diubah dengan cara yang dibenarkan;
(c) Tidak Boleh Disangkal – Punca data dan maklumat hendaklah daripunca yang sah dan tidak boleh disangkal;
(d) Kesahihan – Data dan maklumat hendaklah dijamin kesahihannya; dan
(e) Ketersediaan – Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

4.0 SKOP

Aset ICT KKT terdiri daripada perkakasan, perisian, perkhidmatan, data dan maklumat serta manusia. DKICT KKR menetapkan keperluan-keperluan asas berikut:

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

(b) Data dan maklumat hendaklah dijaga kerahsiaannya dan dikendalikan sebaik mungkin pada setiap masa bagi memastikan integriti dan kesahihan maklumat serta untuk melindungi kepentingan Kerajaan, perkhidmatan dan masyarakat.

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

(a) Perkakasan
Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan KKR. Contohnya: komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian

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

(c) Perkhidmatan

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

i. Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;
ii. Sistem halangan akses seperti sistem kad akses; dan
iii. Perkhidmatan sokongan seperti kemudahan elektrik, penghawadingin, sistem pencegah kebakaran dan lain-lain.

(d) Data dan Maklumat

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

(e) Manusia

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

(f) Premis Komputer dan Komunikasi

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

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

5.0 PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada DKICT KKR dan perlu dipatuhi adalah seperti berikut;

(a) Akses atas Dasar Perlu Mengetahui

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

Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam dokumen Arahan Keselamatan perenggan 53, muka surat 15;

(b) Hak Akses Minimum

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

(c) Akauntabiliti

Semua pengguna adalah dipertanggungjawabkan ke atas semua tindakannya terhadap aset ICT. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk membolehkan pertanggungjawaban ini dilaksanakan, sistem ICT hendaklah mampu menyokong kemudahan mengesan dan mengesahkan penggunaan sistem ICT.

Akauntibiliti atau tanggungjawab pengguna termasuklah:

i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
ii. Memeriksa data dan maklumat serta menentukan ianya tepat dan lengkap dari semasa ke semasa;
iii. Menentukan data dan maklumat sedia untuk digunakan;
iv. Menjaga kerahsiaan kata laluan;
v. Mematuhi standard prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
vi. Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
vii. Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.

(d) Pengasingan

Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada

kesilapan, kebocoran maklumat terperingkat atau dimanipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan system dan operasi;

(e) Pengauditan

Pengauditan ialah tindakan untuk mengenal pasti insiden berkaitankeselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, aset ICT seperti komputer, pelayan, *router*; *firewall*, rangkaian dan lain-lain hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

(f) Pematuhan

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

(g) Pemulihan

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

(h) Saling Bergantungan

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

6.0 PENILAIAN RISIKO KESELAMATAN ICT

KKR hendaklah mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko asset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT. KKR hendaklah melaksanakan penilaian risiko keselamatan ICT secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT. Seterusnya adalah mengambil tindakan susulan dan/atau langkah-langkah bersesuaian untuk mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat KKR termasuk aplikasi, perisian, pelayan, rangkaian, dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi maklumat termasuklah pusat data, bilik penyelenggaraan, kemudahan utiliti dan sistem-sistem sokongan lain. KKR bertanggungjawab melaksanakan dan menguruskan risiko keselamatan ICT selaras dengan keperluan Surat Pekeliling AmBilangan 6 Tahun 2005. Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam.

KKR hendaklah mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

(a) mengurangkan risiko dengan melaksanakan kawalan yang bersesuaian;
(b) menerima dan/atau bersedia berhadapan dengan risiko yang akan terjadi selagi ia memenuhi kriteria yang telah ditetapkan oleh pengurusan atasan;
(c) mengelak dan/atau mencegah risiko daripada terjadi dengan mengambil tindakan yang dapat mengelak dan/atau mencegah berlakunya risiko; dan
(d) memindahkan risiko kepada pihak lain seperti pembekal, pakarrunding dan pihak-pihak lain yang berkepentingan.

7.0 SINGKATAN

Berikut ialah jadual singkatan bagi perkataan yang digunakan dalamkeseluruhan dokumen ini.

Jadual 1 : Singkatan

BIL.	SINGKATAN	KETERANGAN
1.	API	Application Programming Interface
2.	AVR	Auto Voltage Regulator
3.	BYOD	Bring Your Own Device
4.	CSIRT	**CSIRT** (Computer Security Incident Response Team) Pasukan Tindak Balas Insiden Keselamatan ICT
5.	CIO	Chief Information Officer Ketua Pegawai Maklumat
6.	DDSA	Data Dictionnary Sektor Awam
7.	DKICT	Dasar Keselamatan ICT
8.	E-mel	Elektronik mel
.	GAMMA	Gallery of Malaysia Government MobileApplication
10.	GCERT	Government Computer Emergency ResponseTeam Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan
11.	ICT	Information and Communication TechnologyTeknologi Maklumat dan Komunikasi
12.	ICTSO	ICT Security Officer Pegawai Keselamatan ICT
13.	IDS	Intrusion Detection System
14.	IP	Internet Protocol
15.	IPS	Intrusion Prevention Syste,
16.	ISMS	Information Security Management System Sistem Maklumat Pengurusan Keselamatan
17.	ISP	Internet Service Provider
18.	JTICT	Jawatankuasa Teknikal ICT
19.	JPA	Jabatan Perkhidmatan Awam
20.	JPICT	Jawatankuasa Pemandu ICT
21.	JPM	Jabatan Perdana Menteri
22.	KPDNKK	Kementerian Perdagangan Dalam Negeri, Koperasi dan Kepenggunaan
23.	KPK	Ketua Pegawai Keselamatan

BIL.	SINGKATAN	KETERANGAN
24.	KKR	Kementerian Kerja Raya
25.	KSU	Ketua Setiausaha
26.	LAN	Local Area Network
27.	MAMPU	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia
28.	MKN	Majlis Keselamatan Negara
29.	MYCERT	Malaysia Computer Emergency Response TeamPasukan Tindak Balas Insiden Keselamatan ICT Malaysia
30.	NACSA	National Cyber Security Agency
31.	PICT	Pengurus ICT
32.	PKI	Public Key Infrastructure Infrastruktur Kunci Awam
33.	PKP	Pengurusan Kesinambungan PerkhidmatanBusiness Continuity Management
34.	SKMM	Suruhanjaya Komunikasi dan Multimedia Malaysia
35.	SLA	Service Level Agreement Perjanjian Tahap Perkhidmatan
36.	SoA	Statement of Applicability
37.	SPPA	Sistem Pemantauan Pengurusan Aset
38.	SUB	Setiausaha Bahagian
39.	SUB(PM)	Setiausaha Bahagian Pengurusan Maklumat
40.	UC	Unified Communication
41.	UPS	Uninterruptible Power Supply
42.	WAN	Wide Area Network

BIDANG 01 : DASAR KESELAMATAN

0101 Dasar Keselamatan ICT KKR **Objektif** : Menerangkan hala tuju dan sokongan pengurusan terhadap keselamatan maklumat selaras dengan keperluan KKR dan perundangan yang berkaitan.	
010101 Pelaksanaan Dasar	**Tanggungjawab**
Pelaksanaan dasar ini akan dijalankan oleh KSU selakuPengerusi JPICT KKR dengan dibantu oleh Ketua Pegawai Maklumat (CIO), Pengurus ICT, Pegawai Keselamatan ICT (ICTSO) dan lain-lain pegawai yang dilantik.	KSU
010102 Penyebaran Dasar	**Tanggungjawab**
DKICT ini perlu disebarkan kepada semua pengguna danpihak ketiga yang menggunakan aset ICT KKR	Pengurus ICT
010103 Penyelenggaraan Dasar	**Tanggungjawab**
DKICT KKR adalah tertakluk kepada semakan dan pindaan daripada semasa ke semasa termasuk kawalan keselamatan, prosedur dan proses selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Berikut adalah prosedur penyelenggaraan DKICT KKR: (a) Kenal pasti dan tentukan perubahan yang diperlukan; (b) Kemukakan cadangan pindaan secara bertulis kepada CIO KKR bagi tujuan kelulusan; (c) Pembentangan dan persetujuan penguatkuasaanpada Mesyuarat JPICT KKR; dan (d) Memaklumkan perubahan dasar yang telah dipersetujui kepada semua pengguna. DKICT hendaklah dikaji semula mengikut keperluan semasa.	CIO dan Pengurus ICT
010104 Pemakaian dan Pengecualian Dasar	**Tanggungjawab**
DKICT KKR adalah terpakai kepada semua pengguna dan pihak ketiga yang menggunakan aset ICT KKR dan tiada pengecualian diberikan.	Pengguna dan pihak ketiga.

BIDANG 02 : ORGANISASI KESELAMATAN

0201 Infrastruktur Organisasi Dalaman

Objektif : Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif DKICT KKR.

020101 Ketua Setiausaha KKR	Tanggungjawab
KSU KKR adalah berperanan dan bertanggungjawabdalam pelaksanaan dan pematuhan DKICT KKR.	KSU

020102 Ketua Pegawai Maklumat (CIO) KKR	Tanggungjawab
CIO KKR ialah Timbalan Ketua Setiausaha (Pengurusan). Peranan dan tanggungjawab CIO KKR adalah seperti berikut: (a) Menentukan keperluan keselamatan ICT; (b) Menyelaras pembangunan dan pelaksanaan pelan tindakan dan program kesedaran keselamatan ICT seperti penyediaan DKICT KKR serta pengurusan risiko dan pengauditan. (c) Memastikan semua keperluan organisasi (sumber kewangan, sumber manusia dan perlindungan keselamatan) adalah mencukupi; (d) Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam DKICT KKR; (e) Memastikan pelaksanaan semakan semula DKICT KKR dilaksanakan bergantung kepada perubahan polisi yang ditetapkan di KKR dan sektor awam; dan (f) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT KKR .	CIO

020103 Ketua Pegawai Keselamatan (KPK) KKR	Tanggungjawab
KPK KKR ialah Timbalan Ketua Setiausaha (Pengurusan). Peranan dan tanggungjawab KPK KKR adalah seperti berikut: (a) Bertanggungjawab ke atas semua aspek keselamatan dokumendan maklumat rasmi KKR, bangunan dan harta benda Kerajaan daripada sebarang ancaman, kecurian, kebakaran dan sebagainya dengan mengambil kira langkah-langkah melindungi	KPK KKR

	selaras dengan peraturan-peraturan yangditetapkan oleh Kerajaan;	
(b)	Mengemukakan perakuan kepada KSU KKR akancadangan untuk meningkatkan keselamatan perlindungan dari semasa ke semasa mengikut kesesuaian;	
(c)	Menubuhkan jawatankuasa keselamatan di KKR yang dipengerusikan oleh Pegawai Keselamatan KKR yang berperanan untuk menyelaraskan pelaksanaan kawalan Keselamatan Perlindungan serta menyelesaikan isu-isu yang berkaitan dalam melaksanakan kawalan keselamatan perlindungan di KKR;	
(d)	Mewakili KKR dalam menghadiri mesyuarat mengenai keselamatan dari semasa ke semasa dan sekiranya diperlukan dan hendaklah membentangkan laporan keselamatan KKR serta isu-isu yang tidak dapat diselesaikan di peringkat KKR;	
(e)	Menubuhkan jawatankuasa yang akan dipengerusikan oleh KSU KKR yang akanbermesyuarat dengan serta merta jika berlaku sebarang kejadian kecemasan yang melibatkan keselamatan dokumen dan kebocoran maklumat serta harta benda Kerajaan termasuk ancaman keselamatan, pencerobohan, kebakaran, kecurian dan sebagainya. Selanjutnya menyediakan laporan hasil mesyuarat jawatankuasa berkenaan untuk dikemukakan kepada pihak berkuasa berkaitan;	
(f)	Mengadakan pemeriksaan dari semasa ke semasa ke atas bangunan, sistem pendawaian elektrik, bilik komputer, bilik dokumen dan peralatan, kawasan pejabat dan semua perkara di bawah tanggungjawabnya bagi memastikan ia dalam keadaan yang selamat dan tidak terdedah kepadaancaman risiko;	
(g)	Menganjurkan kursus dan taklimat kesedaran keselamatan perlindungan dengan kerjasama Pejabat Ketua Pegawai Keselamatan Kerajaan, JPM bagi memastikan setiap anggota di KKR memahami	

langkah-langkah serta peraturan-peraturan keselamatan perlindungan; (h) Bekerjasama rapat dengan Pegawai Keselamatan Kerajaan untuk mendapat khidmat nasihat mengenai langkah-langkah meningkatkan sistem kawalan keselamatan perlindungan di KKR; (i) Menyelaras langkah-langkah keselamatan (*coordinate security measures*) dan mengadakan hubungan dengan Pegawai Keselamatan Kerajaan, Pegawai Bomba, Pegawai Polis serta pihak-pihak lain; dan (j) Melaksanakan tugas-tugas lain yang ditetapkan dalam peraturan-peraturan keselamatan Kerajaan yang sedang berkuat kuasa dan yang akan dipinda dari semasa ke semasa.	
020104 Jawatankuasa Pemandu ICT (JPICT) KKR	**Tanggungjawab**
Keahlian JPICT KKR adalah terdiri daripada: Pengerusi: KSU KKR atau Pegawai yang diturunkan kuasa. Ahli-ahli: i. Ketua-Ketua Jabatan, Badan Berkanun dan Bahagian di bawah KKR; ii. CIO; iii. Pengurus ICT; iv. ICTSO; dan v. Lain-lain ahli yang berkaitan. Urus setia: Bahagian Pengurusan Maklumat (BPM) KKR. Peranan dan tanggungjawab JPICT KKR adalah sepertiberikut: a) Menetapkan arah tuju dan strategi untuk pembangunan dan pelaksanaan ICT Kementerian; b) Merancang, mengenal pasti dan mencadangkansumber seperti kepakaran, tenaga kerja dan kewangan yang diperlukan bagi melaksanakan arah	JPICT KKR

tuju/strategi ICT Kementerian dan semua agensi di bawahnya; c) Merancang dan menyelaras pembangunan program/projek ICT Kementerian dan semua agensi di bawahnya supaya selaras dengan pelan strategik organisasi dan pelan strategik ICT; d) Menyelaras dan menyeragamkan pembangunan dan pelaksanaan ICT antara Kementerian dan semua agensi di bawahnya dengan pelan strategik organisasi dan pelan strategik ICT Sektor Awam; e) Mempromosi dan menggalakkan perkongsianpintar projek ICT antara Kementerian dan semua agensi di bawahnya; f) Merancang dan menentukan langkah-langkah keselamatan ICT; g) Mengikuti dan memantau perkembangan program ICT Kementerian dan semua agensi di bawahnya, serta memahami keperluan, masalah dan isu-isu yang dihadapi dalam pembangunan dan pelaksanaan ICT; h) Menilai dan meluluskan semua perolehan ICT Kementerian dan semua agensi di bawahnya berdasarkan kepada keperluan sebenar dan dengan perbelanjaan yang berhemah serta mematuhi peraturan-peraturan semasa yang berkaitan; i) Menyelaras dan mengemukakan kertas cadangan perolehan ICT bagi Kementerian dan semua agensi di bawahnya kepada JTISA untuk kelulusan teknikal; j) Mengemukakan laporan projek ICT yang diluluskan di peringkat JPICT Kementerian dan dibuat perolehan kepada JTISA; dan k) Mengemukakan laporan kemajuan projek ICT bagi Kementerian dan semua agensi di bawahnya yang telah diluluskan oleh JTISA kepada JTISA mengikut tempoh yang telah ditetapkan.	

020105	Jawatankuasa Pensijilan Sistem Pengurusan Keselamatan Maklumat (ISMS) KKR	Tanggungjawab
	Keahlian Jawatankuasa ISMS KKR adalah terdiri daripada: Pengerusi: KSU KKR atau Pegawai yang diturunkan kuasa. Ahli-ahli: i. Ketua Bahagian Kementerian yang terlibat dibawah skop ISMS; dan ii. Lain-lain ahli yang berkaitan. Urus setia: Bahagian / Pegawai yang dilantik. Peranan dan tanggungjawab Jawatankuasa ISMS adalahseperti berikut: (a) Merancang dan menyelaras pensijilan ISMS seperti: i. Merancang struktur organisasi ISMS; ii. Merancang kursus kesedaran ISMS; iii. Merancang skop, objektif dan strategi ISMS; iv. Melaksanakan analisis jurang; v. Merancang jadual perbatuan (milestone) ISMS; vi. Membantu Pelaksana ISMS menyediakan pernyataan dasar ISMS, SoA, Penilaian Risiko, Risk Treatment Plan, kaedah pengukuran kawalan dan prosedur-prosedur ISMS; dan vii. Permohonan pensijilan. (b) Memantau pelaksanaan ISMS; dan (c) Mengukur keberkesanan kawalan dan pelaksanaan ISMS.	Jawatankuasa ISMS KKR

020106 Koordinator Pengurusan Kesinambungan Perkhidmatan (PKP) KKR	Tanggungjawab
Koordinator PKP KKR terdiri daripada pegawai yang dilantik iaitu KPK KKR. Manakala Koordinator PKP Bahagian ialah pegawai yang dilantik oleh Ketua Bahagian. Peranan dan tanggungjawab Koordinator PKP adalah seperti berikut: (a) Bertindak sebagai pegawai perhubungan (*single point of contact*) bagi aktiviti pemulihan bencana dan mengetuai pelaksanaan aktiviti pemulihanbencana; (b) Memastikan ujian simulasi pemulihan bencanadijalankan mengikut jadual atau mengikut perancangan yang telah dipersetujui; dan (c) Mengurus penyediaan laporan ujian (*post-mortem*) dan melaksanakan penambahbaikan dokumenPKP.	Koordinator PKP

020107 Pengurus ICT	Tanggungjawab
Pengurus ICT merujuk kepada SUB (PM). Peranan dan tanggungjawab Pengurus ICT adalah sepertiberikut: (a) Mengurus keseluruhan program keselamatan ICT KKR; (b) Menguatkusakan pelaksanaan DKICT KKR; (c) Memberi penerangan dan pendedahan berkenaan DKICT KKR kepada semua pengguna; (d) Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan DKICT KKR; (e) Menjalankan pengurusan risiko; (f) Menjalankan audit ke atas isu-isu keselamatan ICT, mengkaji, menyediakan laporan mengenainya; dan (g) Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti ancaman serangan siber dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian kepada semua pengguna.	Pengurus ICT

020108 Pegawai Keselamatan ICT (ICTSO)	Tanggungjawab
ICTSO bagi KKR ialah Pegawai Teknologi Maklumat yang dilantik. Peranan dan tanggungjawab ICTSO adalah seperti berikut: (a) Mengkaji dan melaksanakan kawalan keselamatanICT selaras dengan keperluan KKR; (b) Menentukan kawalan akses pengguna terhadapaset ICT; (c) Melaporkan sebarang insiden atau penemuan mengenai keselamatan ICT kepada Pengurus ICT; (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT; (e) Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; dan (f) Melaporkan insiden keselamatan ICT kepada **Pasukan Tindak Balas Insiden Keselamatan Siber (CSIRT)** KKR, CIO dan Pengurus ICT.	ICTSO

020109 Pasukan Tindak Balas Insiden Keselamatan Siber (CSIRT) KKR	Tanggungjawab
Penubuhan CSIRT KKR: Kementerian hendaklah menubuhkan CSIRT KKR dan menyelaras penubuhan CSIRT Agensi di bawah seliaannya mengikut keperluan. Bagi agensi yang tiada keperluan untuk menubuhkan CSIRT, agensi tersebut hendaklah melaporkan terus kepada CSIRT Agensi yang menyelianya. Sebagai langkah mengukuhkan pengurusan dan pengendalian keselamatan siber sektor awam serta memastikan insiden ditangani dengan berkesan, setiap agensi hendaklah: (i) Menubuhkan CSIRT atau yang setara dengannya bagi menangani insiden keselamatan siber. (ii) CSIRT KKR bertindak sebagai first level support kepada NC4 dalam mengendali insiden keselamatan siber, mengawasi dan memberi khidmat nasihat berkaitan keselamatan siber kepada agensi di bawah seliaannya.	CSIRT KKR

(iii) bertanggungjawab melaporkan insiden keselamatan siber kepada Ketua Pegawai Digital (Chief Digital Officer, CDO) atau yang setara dan bersesuaian dengan struktur agensi masing-masing.

Model struktur pewujudan CSIRT KKR adalah seperti yang berikut:

(i) CSIRT ditubuhkan pada peringkat Kementerian dan juga agensi di bawahnya. CSIRT Agensi di bawahnya bertanggungjawab atas insiden masing-masing dan perlu diselaraskan pada peringkat Kementerian

Peranan	Pegawai Bertanggungjawab	Tugas dan Tanggungjawab
Pengarah CSIRT	Ketua Pegawai Digital (Chief Digital Officer, CDO)/Pengurus ICT atau yang setara	Menguruskan tindakan insiden yang berlaku sehingga keadaan pulih. Mengaktifkan BCP/DRP jika perlu. Menentukan sama ada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang/keselamatan.
Pengurus CSIRT	Pegawai Keselamatan ICT (ICTSO) atau yang setara	Menentukan tahap keutamaan insiden. Melaporkan insiden kepada Pengarah CSIRT. Mengambil langkah pemulihan awal.
Ahli CSIRT	Pegawai Teknologi Maklumat/Penolong Pegawai Teknologi Maklumat	Mengendalikan insiden berdasarkan panduan yang telah ditetapkan.

Jadual 1: Keahlian dan Tanggungjawab CSIRT KKR

Keahlian CSIRT KKR boleh dilantik daripada kalangan pegawai sedia ada yang mengendalikan keselamatan maklumat, rangkaian, operasi sistem atau mempunyai kelayakan akademik dalam bidang berkaitan atau sijil profesional keselamatan siber.

020110 Pentadbir Sistem ICT	Tanggungjawab
Pentadbir Sistem ICT ialah pegawai yang dipertanggungjawabkan berdasarkan skop tugasan masing-masing seperti menyelenggara sistem aplikasi, laman web dan aplikasi *mobile*. Peranan dan tanggungjawab Pentadbir Sistem ICT adalah seperti berikut: (a) Mengambil tindakan segera mengikut proses yang ditetapkan apabila dimaklumkan mengenai pengguna ICT yang berhenti, bertukar, bercuti dan berkursus panjang atau berlaku perubahan dalam bidang kuasa; (b) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di DKICT KKR; (c) Memantau aktiviti capaian harian sistem aplikasi pengguna; (d) Mengenal pasti aktiviti-aktiviti tidak normal seperti pengubahsuaian data tanpa kebenaran serta membatalkan atau memberhentikannya dengan serta-merta dan melaporkannya kepada Pengurus ICT; dan (e) Menganalisis dan menyimpan rekod jejak audit.	Pentadbir Sistem ICT

020111 Pentadbir Web	Tanggungjawab
Peranan dan tanggungjawab Pentadbir Web adalahseperti berikut: (a) Memastikan kandungan portal rasmi sentiasa sahih dan terkini; (b) Memantau prestasi capaian dan menjalankan penilaian prestasi untuk memastikan akses yang lancar; (c) Memantau dan menganalisis log untuk mengesan sebarang capaian yang tidak sah atau cubaan menggodam, menceroboh dan mengubahsuai muka laman; (d) Menghadkan capaian Pentadbir Laman Web bahagian ke *web server*; (e) Mengasingkan kandungan dan aplikasi atas talian untuk capaian secara Intranet dan Internet ke portal KKR; (f) Memastikan data-data SULIT tidak boleh disalin atau dicetak oleh orang yang tidak berhak; (g) Memastikan reka bentuk web dibangunkan dengan ciri-ciri keselamatan supaya tidak dicerobohi; (h) Melaksanakan *housekeeping* keselamatan terhadapsystem pengoperasian dan perisian-perisian lain di *web server*; (i) Melaksanakan proses *backup* dan *restoration* secaraberkala; dan (j) Melaporkan sebarang pelanggaran keselamatanportal rasmi kepada ICTSO.	Pentadbir Web
020112 Pentadbir Pusat Data dan Rangkaian ICT	**Tanggungjawab**
Pentadbir Pusat Data dan Rangkaian ICT ialah pegawai yang dipertanggungjawabkan berdasarkan skop tugasan masing-masing seperti melaksanakan dan menyelenggara rangkaian ICT dan komunikasi serta Pusat Data. Peranan dan tanggungjawab Pentadbir Pusat Data dan Rangkaian ICT adalah seperti berikut: (a) Memastikan kerahsiaan akaun pentadbir;	Pentadbir Pusat Data dan Rangkaian ICT

(b) Merangka , melaksana dan menguatkuasakan polisi keselamatan ICT seperti perlindungan dan perkongsian data; (c) Merancang dan melaksana polisi ancaman keselamatan ICT; (d) Merancang dan melaksana polisi capaian rangkaian; (e) Memastikan semua aset di Pusat Data berfungsi dan beroperasi dengan sempurna; (f) Menyelia dan membuat proses *backup* dan *restore*;dan (g) Memantau keadaan rangkaian dan mengawal penggunaan sumber.	
020113 Pegawai Aset	**Tanggungjawab**
Pegawai Aset KKR ialah Ketua Penolong Setiausaha Bahagian Kewangan dan Pegawai Aset Bahagian ialah pegawai yang dilantik oleh Pegawai Pengawal; Peranan dan tanggungjawab Pegawai Aset adalah seperti berikut: (a) Mengetuai Unit Pengurusan Aset Alih KKR / Bahagian bagi memastikan pengurusan aset alih Kerajaan dijalankan selaras dengan peraturan yang ditetapkan; (b) Memastikan penerimaan aset alih Kerajaan dilaksanakan oleh pegawai yang dilantik secara bertulis oleh Ketua Bahagian; (c) Memastikan semua aset alih Kerajaan yang diterima, didaftarkan dalam tempoh dua (2) minggu dari tarikh pengesahan penerimaan aset; (d) Memastikan semua aset alih Kerajaan yang dipinjam, direkodkan ke dalam Rekod Pergerakan Aset. Aset tidak dibenarkan dibawa keluar dari pejabat kecuali dengan kelulusan bertulis daripada Ketua Bahagian; (e) Memastikan Daftar Aset Alih dikemas kini apabila berlaku penambahan / penggantian / penaiktarafan aset termasuk selepas pemeriksaan aset, pelupusan dan hapus kira;	Pegawai Aset

(f) Memastikan semua aset alih Kerajaan diberi tanda pengenalan dengan cara melabel / mengecat / "emboss" tanda Hak Kerajaan Malaysia dan nama KKR / Bahagian berkenaan di tempat yang mudah dilihat dan sesuai pada aset berkenaan; (g) Memastikan semua aset alih Kerajaan ditandakan dengan Nombor Siri Pendaftaran mengikut susunan yang ditetapkan; (h) Memastikan senarai daftar induk aset alih Kerajaan disediakan; (i) Memastikan senarai aset alih Kerajaan disediakan mengikut lokasi dan format Senarai Aset Alih Kerajaan dalam dua (2) salinan. Satu (1) senarai berkenaan perlu disimpan oleh Pegawai Aset dan satu (1) Salinan perlu dipaparkan oleh pegawai yang bertanggungjawab di lokasi; (j) Memastikan setiap kerosakan aset alih Kerajaan dilaporkan; (k) Bertanggungjawab untuk menyedia, merancang, melaksana, memantau dan merekodkan penyelenggaraan aset alih Kerajaan; (l) Merancang, memantau dan memastikan pemeriksaan aset alih Kerajaan dilaksanakan ke atas keseluruhan aset alih Kerajaan sekurang-kurangnya sekali setahun; dan (m) Memastikan setiap kes kehilangan aset alih Kerajaan dilaporkan dan diuruskan dengan teratur.	
020114 Pengguna	**Tanggungjawab**
Pengguna ialah semua warga KKR meliputi pegawai dan kakitangan yang menggunakan peralatan, perisian dan perkhidmatan ICT KKR. Pengguna mempunyai peranan dan tanggungjawabseperti berikut: (a) Membaca, memahami, dan mematuhi DKICT KKR; (b) Mengetahui dan memahami implikasi keselamatan ICT akibat daripada tindakannya;	Pengguna

(c) Menjalani tapisan keselamatan seperti yang diarahkan (sekiranya berkaitan); (d) Melaksanakan dan mematuhi prinsip-prinsip DKICT KKR serta menjaga kerahsiaan maklumat KKR; (e) Melaporkan sebarang aktiviti yang mengancamkeselamatan ICT kepada ICTSO dengan segera; (f) Menghadiri program-program kesedaran mengenai keselamatan ICT; dan (g) Menandatangani Surat Akuan Pematuhan DKICT KKR sebagaimana **Lampiran 1**.	
020115 Pengasingan Tugas dan Tanggungjawab	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanupulasi; dan (c) Aset ICT digunakan bagi tugas membangun, mengemas kini, menyelenggara dan menguji aplikasi hendaklah diasingkan daripada aset ICT yang digunakan sebagai persekitaran sebenar (*production*). Pengasingan juga meragkumi tindakan memisahkan antara kumpulan sistem dan operasi.	Pengurus ICT dan ICTSO
0202 *Bring Your Own Device* (BYOD) **Objektif** : Memastikan keselamatan maklumat semasa menggunakan peralatan BYOD di dalam KKR.	
020201 Keperluan dan Kawalan Penggunaan BYOD	**Tanggungjawab**
Penggunaan BYOD yang disambungkan kepada rangkaian KKR sama ada menyimpan atau mengakses data rasmi Kerajaan adalah tertakluk kepada perkara-perkara yang perlu dipatuhi seperti berikut:	Pengguna

(a) Pengguna perlu mengetahui risiko dan kesan penggunaan BYOD terhadap keselamatan maklumat; (b) Pengguna perlu mengetahui peraturan-peraturanyang telah ditetapkan apabila menggunakan BYOD; dan (c) Pengguna bertanggungjawab sepenuhnya ke atas sebarang insiden keselamatan yang berpunca daripada pengguna BYOD.	
0203 Peralatan Mudah Alih dan Kerja Jarak Jauh **Objektif : Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh.**	
020301 Peralatan Mudah Alih	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan pendaftaran ke atas peralatan mudah alih; (b) Memastikan keperluan ke atas perlindungan secara fizikal; (c) Memastikan kawalan ke atas pemasangan perisian peralatan mudah alih; (d) Memastikan kawalan ke atas versi dan *patches* perisian; (e) Memastikan sekatan ke atas perkhidmatan maklumat secara dalam talian; (f) Memastikan kawalan perkhidmatan maklumat secara kawalan akses dan teknik kriptografi; dan (g) Memastikan peralatan mudah alih disimpan di tempat yang selamat apabila tidak digunakan.	Pengguna
020302 Kerja Jarak Jauh	**Tanggungjawab**
Memastikan dasar dan langkah – langkah keselamatan sokongan hendaklah dilaksanakan bagi melindungi maklumat yang diakses, diproses atau disimpan di lokasi kerja jarak jauh.	Pengguna

BIDANG 03 : KESELAMATAN SUMBER MANUSIA

0301 Keselamatan Sumber Manusia dalam Tugas Harian

Objektif : Memastikan pengguna dan pihak ketiga yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Pengguna dan pihak ketiga hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

030101 Sebelum Perkhidmatan	Tanggungjawab
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Menyatakan dengan lengkap dan jelas peranan dan tanggungjawab dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; (b) Menjamin tapisan keselamatan berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (c) Mematuhi semua terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan penjanjian yang telah ditetapkan. (d) Menandatangani Surat Akuan Pematuhan DKICT KKR sebagaimana di **Lampiran 1**.	Pengguna dan pihak ketiga

030102 Dalam Perkhidmatan	Tanggungjawab
Perkara-perkara yang mesti dipatuhi termasuk yangberikut: (a) Memastikan keselamatan aset ICT diurus berdasarkan perundangan dan peraturan yang ditetapkan oleh KKR; (b) Memastikan program kesedaran yang berkaitan mengenai pengurusan keselamatan aset ICT dihadiri secara berterusan; (c) Tindakan disiplin dan/atau undang-undang akan dikenakan sekiranya berlaku pelanggaran dengan perundangan dan peraturan ditetapkan oleh KKR;dan (d) Menghadiri kursus dan latihan teknikal yang berkaitan bagi memantapkan pengetahuan serta memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT.	Pengguna dan pihak ketiga

030103 Bertukar atau Tamat Perkhidmatan	Tanggungjawab
Perara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Memastikan semua aset ICT dikembalikan kepada KKR mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; (b) Kebenaran capaian ke atas maklumat dankemudahan proses maklumat akan dibatalkan atau ditarik balik dengan serta merta mengikut peraturan yang ditetapkan oleh KKR; dan (c) Melupuskan semua maklumat terperingkat yang tidak lagi diperlukan secara selamat.	Pengguna dan pihak ketiga

BIDANG 04 : PENGURUSAN ASET

0401 Akauntabiliti Aset

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

040101 Inventori Aset ICT	Tanggungjawab
Ini bertujuan memastikan semua aset ICT diberi kawalan dan perlindungan yang sesuai oleh pemilik atau pemegang amanah masing-masing. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua aset ICT dikenal pasti dan maklumat aset direkodkan ke dalam Sistem Pengurusan Aset (SPA); (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 KKR; (d) Peraturan bagi pengendalian aset ICT hendaklah dipatuhi dan dilaksanakan; (e) Setiap pengguna adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan (f) Memastikan semua aset ICT diagihkan kepada pengguna mengikut piawaian dan garis panduan yang ditetapkan.	Pegawai Aset KKR / Bahagian dan pengguna

0402 Pengelasan, Pengendalian dan Keselamatan Maklumat

Objektif: Memastikan setiap maklumat atau aset ICT diberikan tahapperlindungan yang bersesuaian.

040201 Pengelasan Maklumat	Tanggungjawab
Maklumat hendaklah dikelaskan atau dilabelkan sewajarnya oleh pegawai yang diberi kuasa mengikut dokumen Arahan Keselamatan Kerajaan. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan dalam dokumen Arahan Keselamatan Kerajaan seperti berikut: (a) Rahsia Besar; (b) Rahsia;	Pengguna

(c) Sulit; atau (d) Terhad.	
040202 Pengendalian Maklumat	**Tanggungjawab**
Aktiviti pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengikut standard, prosedur, garis panduan dan langkah keselamatan yang ditetapkan mengikut jenis-jenis pemperosesan berikut: (a) Penyalinan; (b) Muat naik (*upload*) dan muat turun (*download*); (c) Penyimpanan dalam media storan; (d) Penghantaran melalui pos, faks, e-mel dan media baharu seperti *Facebook*, *WhatsApp*, *Twitter*, *Youtube* dan *Instagram*; (e) Penghantaran melalui percakapan termasuk melalui telefon, mel suara, mesin menjawab telefon dan *VoIP*, dan (f) Pemusnahan. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut: (g) Menghalang pendedahan maklumat kepada pihakyang tidak dibenarkan; (h) Memeriksa maklumat dan menentukan ia tepat danlengkap dari semasa ke semasa; (i) Menentukan maklumat sedia untuk digunakan; (j) Menjaga kerahsiaan kata laluan; (k) Mematuhi standard, prosedur, langkah dan garispanduan keselamatan ditetapkan; (l) Memberi perhatian terutama semasa aktiviti pengendalian maklumat terperingkat; dan (m) Menjaga kerahsiaan langkah-langkah keselamatan ICT daripada diketahui umum.	ICTSO dan Pengguna

040203 Keselamatan Maklumat	Tanggungjawab
Perkara-perkara yang mesti dipatuhi termasuk yang berikut: (a) Maklumat terperingkat hanya boleh dilakukan penduaan dan penyalinan pada media storan oleh pegawai yang dibenarkan sahaja; (b) Menggunakan enkripsi dan lain-lain kaedah keselamatan yang bersesuaian ke atas maklumat terperingkat yang disediakan dan dihantar secara elektronik; dan (c) Semua maklumat terperingkat hendaklah dihapuskan mengikut prosedur pelupusan semasa.	ICTSO dan Pengguna
0403 ICT Hijau (*Green* ICT) **Objektif**: Memastikan aset ICT mempunyai ciri-ciri ICT Hijau.	
040301 Pengurusan Aset ICT	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan perolehan aset ICT mempunyai spesifikasi ciri-ciri ICT Hijau; (b) Memastikan kerja-kerja seharian mengguna pakai prinsip pengurangan (*reduce*), penggunaan semula (*reuse*) dan kitar semula (*recycle*); (c) Memastikan system pengurusan kuasa (*power management*) aset ICT diaktifkan; dan (d) Memastikan peralatan ICT dilupuskan dan penggunaan semula alat ganti mengikut tatacara yang mengambil kira pemuliharaan alam sekitar.	Pengurus ICT dan Pengguna.
0404 Pengurusan Media **Objektif** : Melindungi aset ICT daripada sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
040401 Penghantaran dan Pemindahan	**Tanggungjawab**
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran terlebih dahulu.	Pengguna
040402 Prosedur Pengendalian Media	**Tanggungjawab**
Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut:	Pentadbir Pusat Data dan Rangkaian ICT.

(a) Semua media hendaklah dilabel mengikut kesesuaian; (b) Menghadkan dan menentukan capaian media kepada pengguna yang dibenarkan sahaja; (c) Menghadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; (d) Mengawal dan merekodkan aktiviti pengurusan media bagi mengelak daripada sebarang kerosakan dan pendedahan yang tidak dibenarkan; dan (e) Menyimpan semua media di tempat yang selamat.	
040403 Media Storan	**Tanggungjawab**
Media storan perlu dipastikan berada dalam keadaan yang baik, selamat, terjamin kerahsiaan, integriti dan kebolehsediaan untuk digunakan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Media storan hendaklah disimpan di ruang penyimpanan yang baik dan mempunyai ciri-ciri keselamatan; (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. Langkah-langkah pencegahan hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan adalah terjamin dan selamat; (d) Semua media storan yang mengandungi data kritikal hendaklah disimpan di tempat yang mempunyai ciri-ciri keselamatan dan mengikut prosedur yang telah ditetapkan; (e) Mematuhi prosedur media storan yang telah dikenal pasti termasuk akses, inventori, pergerakan, pelabelan serta *backup* dan *restore*; (f) Perkakasan backup hendaklah diletakkan di tempat yang terkawal;	Pengguna

(g) Mengadakan salinan atau *backup* pada media storan kedua bagi tujuan keselamatan dan mengelakkan kehilangan data. Media storan kedua hendaklah disimpan ditempat yang selamat; dan (h) Semua maklumat dalam media storan yang hendak dilupuskan mestilah dihapuskan terlebih dahulu. Proses pelupusan hendaklah dilakukan dengan teratur dan selamat mengikut prosedur pelupusan.	
040404 Media Perisian	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah sepertiberikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi penggunaan KKR; dan (b) Lesen perisian (*registrationcode*, *serials* dan *CD-keys*) perlu disimpan dengan selamat bagi mengelakkandari berlakunya kecurian atau cetak rompak.	Pengguna
040405 Media Tandatangan Digital	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan; (b) Media ini tidak boleh dipindah milik atau dipinjamkan; dan (c) Sebarang kehilangan media tandatangan digital yangberlaku hendaklah dilaporkan mengikut peraturan semasa yang ditetapkan.	Pengguna
0405 Keselamatan Dokumen **Objektif** : Melindungi maklumat KKR daripada sebarang bentuk ancamanpersekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian, pencerobohan, kemalangan atau kecurian.	
040501 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut:	Pengurus ICT, ICTSO, Pentadbir Sistem ICT,

(a) Menyediakan sistem penyampaian dokumentasimempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan keselamatan sisem dokumentasi; dan (c) Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Pentadbir Pusat Data dan Rangkaian ICT
040502 Dokumen	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah sepertiberikut: (a) Setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; (b) Pergerakan fail dan dokumen hendaklah dikawal dan direkodkan serta perlulah mengikut prosedurkeselamatan; (c) Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan Kerajaan; (d) Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa; dan (e) Penyimpanan maklumat rahsia di storan dalam talian umum (Contohnya: *Amazon* dan *Dropbox*) tidak dibenarkan sama sekali.	Pengguna

BIDANG 05 : KAWALAN CAPAIAN

0501 Dasar Kawalan Capaian

Objektif :Peraturan kawalan capaian hendaklah mengambil kira faktor had capaian dan hak capaian (*authorization*) ke atas maklumat/data dan proses capaian maklumat.

050101 Keperluan Kawalan Capaian	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melaksanakan kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan perananpengguna; (b) Melaksanakan kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Melaksanakan keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan (d) Melaksanakan kawalan ke atas kemudahan pemprosesan maklumat.	ICTSO, Pentadbir Sistem ICT, PentadbirPusat Data dan Rangkaian ICT.

0502 Pengurusan Capaian Pengguna

Objektif : Mengawal capaian pengguna ke atas aset ICT KKR.

050201 Akaun Pengguna	Tanggungjawab
Setiap pengguna adalah bertanggungjawab ke atas aset ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan sahaja boleh digunakan; (b) Akaun pengguna mestilah unik; (c) Pengguna bertanggungjawab sepenuhnya ke atas segala kegunaan melalui akaun dan kata laluannya; dan (d) Akaun pengguna akan dibeku atau ditamatkan atas sebab-sebab berikut: i. Pengguna yang bercuti panjang dalam tempoh waktu melebihi empat (4) minggu; ii. Bertukar ke agensi lain; iii. Bersara; atau iv. Ditamatkan perkhidmatan.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT serta pengguna.

050202 Hak Capaian	Tanggungjawab
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Pusat Data dan Rangkaian ICT

050203 Penggunaan Maklumat Pengesahan Rahsia	Tanggungjawab
Peranan dan tanggungjawab pengguna adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT KKR; (b) Mengetahui dan memahami implikasi keselamatan siber kesan dari tindakannya; (c) Melaksanakan prinsip-prinsip dan menjaga kerahsiaan maklumat KKR; dan (d) Melaksanakan langkah-langkah perlindungan seperti yang berikut: i. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; ii. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari masa ke semasa; iii. Menentukan maklumat sedia untuk digunakan; iv. Menjaga kerahsiaan kata laluan; v. Mematuhi standart, prosuder, langkah dan garis panduan keselamatan yang ditetapkan; vi. Memberikan perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan vii. Menjaga kerahsiaan langkah-langkah keselamatan siber daripada diketahui umum. (e) Melaporkan sebarang aktiviti yang mengancam keselamatan siber kepada ICTSO dengan segera; dan (f) Menghadiri program-program kesedaran mengenai keselamatan siber.	Pengguna

050204 Pengurusan Hak Akses Istimewa	Tanggungjawab
Peruntukan dan penggunaan hak akses istimewa hendaklah dihadkan dan dikawal. Penetapan dan penggunaan ke atas hak akses perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas merujuk kepada **Prosedur Pendaftaran dan Penamatan Pengguna**	Pentadbir Sistem ICT
050205 Pengurusan Maklumat Pengesahan Rahsia Pengguna	**Tanggungjawab**
Peruntukan maklumat pengesahan rahsia bagi pengguna hendaklah dikawal melalui proses pengurusan formal. Peruntukan maklumat pengesahan rahsia bagi pengguna perlu diberikan kawalan dan penyeliaan yang ketat berdasarkan keperluan.	Pentadbir Sistem ICT, ICTSO
050206 Kajian Semula Hak Akses Pengguna	**Tanggungjawab**
Pemilik aset hendaklah menyemak hak akses pengguna pada sela masa yang ditetapkan. Pentadbir Sistem ICT perlu mewujudkan Prosedur Pendaftaran dan Penamatan Pengguna sistem masing-masing sebagai rujukan semakan ke atas hak akses pengguna pada sela masa yang ditetapkan.	Pentadbir Sistem ICT, ICTSO

0503 Kawalan Capaian Rangkaian **Objektif** : Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
050301 Capaian Rangkaian	**Tanggungjawab**
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat melalui langkah-langkah berikut: (a) Menempatkan atau memasang antara muka yang bersesuaian antara rangkaian KKR, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan dan peralatan yang menepati kesesuaian penggunanya; (c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan (d) Capaian fizikal dan logikal ke atas perkakasan rangkaian bagi tujuan mengubah konfigurasi perlulah dikawal.	Pentadbir Pusat Data dan Rangkaian ICT
050302 Capaian Internet	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pemantauan secara berterusan dilakukan bagi memastikan penggunaannya hanya untuk capaian yang dibenarkan sahaja; (b) Penguatkuasaan *Content Filtering* hendaklah dilaksanakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (c) Pengawalan penggunaan *bandwidth* hendaklah dilaksanakan bagi penggunaan *bandwidth* yang maksimum dan lebih berkesan; (d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja; (e) Pengguna hanya dibenarkan memuat turun perisian yang sah dan berdaftar; dan (f) Perolehan / pembelian dan penggunaan broadband bergantung kepada justifikasi atau keperluan dan perlu mendapat kelulusan Pengurusan KKR.	Pengurus ICT, Pentadbir Pusat Data dan Rangkaian ICT

050303 Capaian Rangkaian Dalaman melalui VPN	Tanggungjawab
Kawalan capaian perkhidmatan rangkaian bagi mengakses sistem-sistem yang diletakkan di *Server Farm* dan sistem intranet hendaklah dijamin selamat dengan : (a) Memastikan hanya sistem-sistem yang yang diminta untuk diakses sahaja dibenarkan dengan sekatan dibuat berdasarkan kepada ID pemohon dengan tempoh masa sah selama 3 bulan sahaja; (b) Memastikan sistem log dilaksanakan bagi setiap aktiviti capaian sistem; (c) Memastikan setiap server yang menempatkan sistem-sistem ini mempunyai *Firewall Rules* bagi menghalang pengaksesan diantara server-server lain secara *Remote Desktop Protocol*; (d) Memasang antara muka yang bersesuaian dengan Rangkaian KKR bagi tujuan capaian daripada luar rangkaian KKR secara VPN; (e) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT; dan (f) Warga KKR perlu mendapat kelulusan Pengurus ICT untuk permohonan VPN	Pengurus ICT, Pentadir Pusat Data dan Rangkaian ICT

050304 Penggunaan *Video Conferencing*	Tanggungjawab
Penggunaan *video conference* serta kawalan dan perhatian yang perlu dipatuhi oleh warga KKR: (a) Mematuhi terma dan syarat yang terkandung dalam Peraturan Pegawai Awan (Kelakuan dan Tatatertib) 1993 dan arahan-arahan yang berkaitan yang menjadi teras kepada keperibadian atau tatakelakuan anggota perkhidmatan awam; (b) Membuat pemakluman terlebih dahulu untuk tujuan merakam atau mengedar rakaman sepanjang komunikasi berlangsung; (c) Sebarang komen mengenai isu-isu yang melibatkan agensi atau yang berbentuk serangan peribadi hendaklah dielakkan; (d) Memastikan perkongsian dan penggunaan maklumat yang berkaitan dengan hak cipta dan harta intelek telah mendapat kebenaran daripada pihak yang berkenaan; (e) Bahan-bahan rasmi yang hendak dimuat naik atau dikongsi hendaklah disemak dan mendapat pengesahan/kelulusan daripada pihak yang berkenaan	Pengguna

dahulu; (f) Dilarang menggunakan akaun milik orang lain, berkongsi akaun, memberikan akaun kepada orang lain, menggunakan identiti palsu atau menyamar sebagai orang lain; (g) Dilarang membuat sebarang pernyataan yang menyentuh perkara yang boleh menjejaskan imej dan dasar Kerajaan, sensitiviti agama, maklumat berbentuk hasutan dan lucah atau cuba memprovokasikan sesuatu isu yang menyalahi peraturan dan undang-undang; (h) Tidak meninggalkan sidang video (PC / Notebook) tanpa *screen lock* apabila perlu meninggalkan sidang video semasa sesi berlangsung; (i) Rakaman sidang video yang mempunyai maklumat terperingkat adalah tidak dibenarkan; dan (j) Penggunaan *Wifi* Awam hanya dibenarkan melalui Akaun VPN yang diwujudkan untuk melaksanakan sesi VC di luar daripada rangkaian KKR	
050305 Simpanan Data dalam Awan (*Cloud Storage*)	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen rasmi hanya dibenarkan disimpan di cloud yang disediakan oleh kerajaan; (b) Dokumen terperingkat tidak dibenarkan disimpan di public cloud storage; (c) Setiap dokumen yang disimpan di atas talian perlu ditetapkan kata laluan untuk membuka dokumen; dan (d) Warga KKR perlu mendapat kelulusan BPM untuk mencapai kemudahan *cloud storage* yang disediakan oleh KKR.	ICTSO

0504 Kawalan Capaian Sistem Pengoperasian **Objektif** : Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
050401 Capaian Sistem Pengoperasian	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan mekanisme log masuk yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unikuntuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja; (c) Mewujudkan akaun pendua bagi kegunaan pihak ketiga (kakitangan teknikal KKR/Vendor) bagi tujuan menghalang akses kepada dokumen-dokumen terperingkat pemilik komputer/laptop; dan (d) Menetapkan akaun pengguna pada level *limited* bagi mengelakkan pemasangan dan konfigurasi aplikasi/perisian yang tidak dibenarkan.	Pentadbir Sistem ICT, Pentadir Pusat Data dan Rangkaian ICT
0505 Kawalan Capaian Aplikasi dan Maklumat **Objektif** : Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat dalam sistem aplikasi.	
050501 Capaian Aplikasi dan Maklumat	**Tanggungjawab**
Perkara-perkara berikut hendaklah dipatuhi: (a) Penggunaan sistem maklumat dan aplikasi yang dibenarkan adalah mengikut tahap capaian dankeselamatan maklumat yang telah ditentukan; (b) Memastikan sistem log dilaksanakan bagi setiap aktiviti capaian sistem maklumat dan aplikasi; (c) Mengehadkan capaian sistem dan aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun pengguna akan disekat; dan (d) Memastikan kawalan keselamatan sistem adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah.	Pentadbir Sistem ICT

050502 Pengurusan Kata Laluan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Kata laluan hendaklah ditukar apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Kata laluan hendaklah sekurang-kurangnya dua belas (12) aksara dengan gabungan aksara, angka dan aksara khusus; (d) Kata laluan hendaklah diingat dan **TIDAK BOLEH** dicatat, disimpan atau didedahkan dengan apa cara sekalipun; (e) Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak bolehdikodkan di dalam program; (f) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; dan (g) Kata laluan hendaklah ditukar dalam tempoh yang ditetapkan.	Pengguna

BIDANG 06 : KRIPTOGRAFI

0601 Kawalan Kriptografi

Objektif : Melindungi kerahsiaan, integriti dan kesahihan maklumat melaluikawalan kriptografi.

060101 Enkripsi	Tanggungjawab
Setiap transaksi sistem aplikasi yang melibatkan maklumat rahsia rasmi hendaklah dienkripsi. Keperluan kawalan kriptografi mestilah dinyatakan dalam semua perolehan dan pembangunan ICT baharuyang melibatkan maklumat terperingkat. Kaedah, kod sumber dan produk kriptogafi yang digunakan mestilah boleh diakses oleh Kerajaan bagi tujuan kawalan, penilaian dan penganalisaan keselamatan.	Pentadbir Sistem ICT
060102 Pengurusan Kunci	**Tanggungjawab**
Semua kunci kriptografi yang dihasilkan bagi melindungi maklumat terperingkat adalah milik Kerajaan. Kunci kriptogafi mestilah dilindungi dengan menggunakan kaedah yang ditetapkan dan hendaklah dirahsiakan. Semua kunci mestilah dilindungi daripada pengubahsuaian, pemusnahan dan sebaran tanpa kebenaran sepanjang kitaran hayat kunci tersebut.	Pentadbir Sistem ICT dan Pengguna.
060103 Tandatangan Digital	**Tanggungjawab**
Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik bagi tujuan perlindungan kesahihan dan integriti.	Pentadbir Sistem ICT dan Pengguna.

060104 Pengurusan Infrastruktur Kunci Awam (PKI)	Tanggungjawab
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan daripada diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan sijil digital hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; (b) Sijil digital hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian ataudigunakan oleh pihak lain; (c) Perkongsian sijil digital untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali; dan (d) Sebarang kehilangan, kerosakan dan / atau kata laluan disekat perlu dimaklumkan kepada pegawai yang bertanggungjawab.	Pentadbir Sistem ICT dan Pengguna.

BIDANG 07 : KESELAMATAN FIZIKAL DAN PERSEKITARAN

0701 Keselamatan Kawasan dan Persekitaran

Objektif : Melindungi premis dan aset ICT daripada sebarang bentuk pencerobohan, kerosakan, ancaman, gangguan persekitaran yang disebabkan oleh bencana alam, kesilapan, kecurian, atau kemalangan serta akses yang tidak dibenarkan.

070101 Kawalan Kawasan	Tanggungjawab
Bertujuan menghalang akses, kerosakan dan gangguan secara fizikal terhadap premis dan maklumat agensi. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: (a) Kawasan keselamatan fizikal hendaklah dikenal pasti dengan jelas. Lokasi dan keteguhan keselamatan fizikal hendaklah bergantung kepada keperluan untuk melindungi aset dan hasil penilaian risiko; (b) Menggunakan keselamatan perimeter (halangan seperti dinding, pagar kawalan, pengawak keselamatan dan lain-lain) untuk melindungi kawasan yang mengandungi maklumat dankemudahan pemprosesan maklumat; (c) Melindungi kawasan terhad melalui kawalan- kawalan tertentu seperti memasang alat penggera atau kamera litar tertutup sekiranya berkaitan; (d) Menghadkan jalan keluar masuk; (e) Mengadakan kaunter kawalan; (f) Menyediakan ruang untuk pihak luar; (g) Mewujudkan perkhidmatan kawalan keselamatan; (h) Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (i) Merekabentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik dan kemudahan yang disediakan; (j) Merekabentuk dan melaksanakan perlindungan fizikal daripada kebakaran, banjir, letupan, kacau bilau dan bencana; (k) Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan (l) Memastikan kawasan-kawasan penghantaran dan pemuggahan serta tempat-tempat lain dikawal daripada pihak yang tidak diberi kebenaran memasukinya.	KPK KKR

070102 Kawalan Persekitaran	Tanggungjawab
Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: (a) Memastikan susun atur semua aset di Pusat Data adalah teratur; (b) Semua ruang pejabat khususnya kawasan yangmempunyai kemudahan ICT hendaklah dilengkapi dengan peralatan perlindungan keselamatan yang bersesuaian dan dibenarkan seperti alat pengesan kebakaran, alat pencegah kebakaran dan pintu kecemasan; (c) Semua bahan mudah terbakar, cecair, bahan atau peralatan lain yang boleh merosakkan peralatan ICT, hendaklah diletakkan di tempat yang bersesuaian dan berjauhan daripada aset ICT; (d) Dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran aset ICT; (e) Memastikan akses kepada saluran riser sentiasa dikunci; (f) Memastikan peralatan rangkaian seperti switch, router dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; dan (g) Memastikan pegawai yang bertanggungjawab menyimpan kunci, dapat dihubungi apabila keadaan memerlukan berbuat demikian.	ICTSO, Pentadbir Pusat Data dan Rangkaian ICT sertaPengguna
070103 Kawalan Masuk Fizikal	**Tanggungjawab**
Perara-perkara yang mesti dipatuhi termasuk yangberikut: (a) Pas keselamatan hendaklah dipakai sepanjang waktu bertugas; (b) Semua pas keselamatan hendaklah diserahkan semula kepada KKR apabila pengguna berpindah keluar, berhenti atau bersara. Pihak ketiga juga hendaklah berbuat demikian apabila urusan selesai atau tamat kontrak; (c) Pas pelawat hendaklah diambil di kaunter masuk. Pas ini hendaklah dikembalikan semula selepas tamat lawatan; dan (d) Kehilangan pas mestilah dilaporkan dengan segera.	Pengguna dan pihak ketiga.

070104 Kawasan Terhad	Tanggungjawab
Kawasan terhad ditakrifkan sebagai kawasan yang dihadkan kemasukannya kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan terhad ICT di KKR adalah Pusat Data. Perkara-perkara berikut hendaklah dipatuhi: (a) Akses kepada kawasan terhad hanyalah kepada pegawai-pegawai yang dibenarkan sahaja. Tanda kawasan terhad hendaklah dipamerkan; (b) Buku log keluar/masuk Pusat Data sentiasa dipantau dan diselenggara; (c) Pihak ketiga dilarang sama sekali untuk memasuki kawasan terhad kecuali bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal; (d) Pihak ketiga hendaklah diiringi dan dipantau sepanjang masa oleh pegawai yang diberi kebenaran untuk mengakses Pusat Data sehingga tugas di kawasan berkenaan selesai; dan (e) Peralatan rakaman/penyimpanan seperti kamera, video, perakam suara dan storan mudah alih adalah tidak dibenarkan dibawa masuk ke dalam pusat data kecuali dengan kebenaran Pentadbir Pusat Datadan Rangkaian ICT. (f) Semua perubahan peralatan/aksesori di Pusat Data hendaklah mendapat kelulusan bertulis dan rekod perubahan hendaklah diselenggara; (g) Kerja-kerja pemasangan/pengujian bagi peralatan/peranti/aksesori tambahan hendaklah dilaksanakan di luar Pusat Data (Staging Area); (h) Semua aktiviti cetakan adalah TIDAK DIBENARKAN di dalam Pusat Data.	Pentadbir Pusat Data dan Rangkaian ICT

070105 Bekalan Kuasa	Tanggungjawab
Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada aset ICT. Perkara-perkara yang perlu dipatuhi adalah sepert berikut: (a) Semua peralatan ICT hendaklah dilindungi daripada kegagalan bekalan kuasa; (b) Peralatan sokongan seperti UPS dan penjana kuasa (generator) digalakkan untuk digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan (c) Semua peralatan sokongan bekalan kuasahendaklah diperiksa, diuji dan diselenggara secara berjadual	Pentadbir Pusat Data dan Rangkaian ICT

070106 Kabel	Tanggungjawab
Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan 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 megelakkan ancaman kerosakan dan *wire tapping*; dan (d) Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pentadbir Pusat Data dan Rangkaian ICT

070107 Prosedur Kecemasan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah sepertiberikut: (a) Memastikan setiap pengguna memahami dan mematuhi prosedur kecemasan; (b) Insiden kecemasan persekitaran mesti dilaporkan; dan (c) Merancang dan menyertai latihan kecemasan bencana yang diadakan di KKR.	KPK KKR dan pengguna

0702 Keselamatan Peralatan Objektif : Melindungi peralatan ICT KKR daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
070201 Peralatan ICT	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna. Sebarang kerosakan peralatan ICT hendaklah dilaporkan melalui saluran yang ditetapkan; (b) Bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran dan perubahan konfigurasiyang telah ditetapkan; (c) Dilarang sama sekali menambah, mengganti atau mengeluarkan sebarang perkakasan ICT yang telah ditetapkan; (d) Dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran; (e) Bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (f) Memastikan perisian antivirus yang dibekalkan oleh KKR di komputer peribadi (*desktop*) / komputer riba sentiasa aktif (*activated*) dan di kemas kini di samping melakukan imbasan ke atas media storan yang digunakan; (g) Penggunaan kata laluan untuk akses ke sistemkomputer adalah diwajibkan; (h) Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (i) Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan; (j) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; dan (k) Peralatan ICT yang hendak dibawa keluar dari premis KKR, hendaklah mematuhi peraturan yang ditetapkan;	Pengguna

(l) Peralatan ICT yang hilang hendaklah dilaporkan kepada Pengurus ICT dan Pegawai Aset KKR/ Bahagian dengan segera; (m) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yangberkuatkuasa; (n) Pengguna tidak dibenarkan mengubah lokasi penempatan peralatan ICT dari tempat asal ia ditempatkan tanpa kebenaran Pegawai Aset KKR/ Bahagian. Perpindahan peralatan ICT hendaklah mematuhi peraturan yang telah ditetapkan; (o) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (p) Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; (q) Bertanggunjawab terhadap peralatan ICT di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; (r) Memastikan semua peralatan ICT yang digunakan dalam keadaan tutup (*off*) apabila meninggalkan pejabat; dan (s) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Pengurus ICT.	
070202 Penyelenggaraan Peralatan ICT	**Tanggungjawab**
Peralatan ICT hendaklah diselenggara dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang dipatuhi adalah seperti berikut: (a) Semua peralatan ICT yang diselenggara hendaklah mengikut spesifikasi yang telah ditetapkan; (b) Memastikan peralatan ICT hanya bolehdiselenggara oleh kakitangan atau pihak ketiga yang dibenarkan sahaja; (c) Bertanggungjawab terhadap setiap peralatan ICT bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan; (d) Menyemak dan menguji semua peralatan ICT sebelum dan selepas proses penyelenggaraan; dan (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan.	Pegawai Aset

070203 Peralatan ICT di Luar Premis	Tanggungjawab
Peralatan ICT yang dibawa keluar dari premis KKR adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan ICT termasuk perisian dan maklumat perlu dilindungi dan dikawal sepanjang masa; (b) Penyimpanan atau penempatan peralatan ICT mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian; dan (c) Kehilangan peralatan ICT perlu dilaporkan mengikut peraturan semasa yang ditetapkan.	Pengguna

070204 Pelupusan Peralatan ICT	Tanggungjawab
Pelupusan melibatkan semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan. Peralatan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas daripada kawalan. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan ICT yang hendak dilupuskan perlulah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut; (b) Pegawai Aset bertanggungjawab merekodkan butir- butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT; (c) Pelupusan peralatan ICT hendaklah dilakukan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan	Pegawai Aset dan Pengguna

(d) Pengguna adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan ICT yang hendak dilupuskan untuk milik peribadi. Contohnya: CPU, RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, *speaker* dan mana-mana peralatan yang berkaitan ke mana- mana bahagian; dan iii. Memindah keluar dari lokasi mana-mana peralatan ICT yang hendak dilupuskan.	
070205 *Clear Desk* dan *Clear Screen*	**Tanggungjawab**
Clear Desk dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Menggunakan kemudahan *password screen saver* atau *log out* apabila meninggalkan komputer; (b) Menyimpan bahan-bahan sensitif di dalam laci atau kabinet fail yang berkunci; dan (c) Memastikan semua dokumen diambil segera daripada pencetak, pengimbas, mesin faksimili dan mesin fotostat.	Pengguna

BIDANG 08 : PENGURUSAN OPERASI

0801 Pengurusan Prosedur Operasi

Objektif : Memastikan pengurusan operasi berfungsi dengan betul dan selamatdaripada sebarang ancaman dan gangguan.

080101 Pengendalian Prosedur	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur pengurusan operasi yang diwujudkan, dikenal pasti dan diguna pakai hendaklah didokumenkan, disimpan dan dikawal; (b) Setiap prosedur mestilah mengandungi arahan- arahan yang jelas, teratur dan lengkap seperti keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian output, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; dan (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa atau mengikut keperluan.	Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT

080102 Kawalan Perubahan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah mendapat kebenaran daripada pegawai yang diberi kuasa terlebih dahulu; (b) Aktiviti-aktiviti seperti memasang, menyelenggara, melupus dan mengemas kini mana-mana perkakasan ICT hendaklah dikendalikan oleh pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian aset ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT

0802 Perancangan dan Penerimaan Sistem **Objektif** : Meminimumkan risiko yang menyebabkan gangguan atau kegagalansistem.	
080201 Perancangan Kapasiti	**Tanggungjawab**
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, kegunaan dan operasi sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT
080202 Penerimaan Sistem	**Tanggungjawab**
Semua sistem baharu (termasuklah sistem yang dikemas kini atau diubah suai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pengurus ICT, Pentadbir Sistem ICT,Pentadbir Pusat Data dan Rangkaian ICT serta Pemilik Sistem
0803 Perisian Berbahaya **Objektif** : Melindungi integriti perisian dan maklumat daripada pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *malware* dan sebagainya.	
080301 Perlindungan dari Perisian Berbahaya	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti antivirus, IDS dan IPS serta memastikan prosedur penggunaan yang betul dan selamat diikuti; (b) Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana- mana undang-undang bertulis yang berkuat kuasa; (c) Mengimbas peralatan ICT dengan antivirus sebelum digunakan; (d) Mengemas kini antivirus dengan paten antivirus yang terkini; dan (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT serta Pengguna

diingini seperti kehilangan dan kerosakan maklumat; (f) Melaksanakan program kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; dan (g) Memberi amaran mengenai ancaman keselamatan ICT seperti serangan virus.	
080302 Perlindungan daripada *Mobile Code*	**Tanggungjawab**
Penggunaan *mobilecode* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan. Memastikan *mobil code* yang digunakan adalah daripada sumber yang dipercayai.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT dan pengguna
0804 *Housekeeping* **Objektif** : Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
080401 *Backup* dan *Restore*	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Melaksanakan backup keselamatan ke atas semua sistem perisian dan aplikasi mengikut Prosedur *Backup* dan *Restore* atau setelah mendapat versi terbaru; (b) Melaksanakan *backup* ke atas semua data dan maklumat mengikut keperluan. Kekerapan *backup* bergantung pada tahap kritikal maklumat; (c) *Backup* hendaklah dilakukan di dalam media yang bersesuaian; (d) Menguji secara berkala *backup* dan *restore* bagi memastikan ia dapat berfungsi dengan sempurna,boleh dipercayai dan berkesan apabila perludigunakan; (e) Melaksanakan generasi *backup* pada sistem danmaklumat; dan (f) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT

0805 Pemantauan **Objektif** : Memastikan aktiviti pemprosesan maklumat yang tidak dibenarkan dapat dikesan.	
080501 Pengauditan dan Forensik ICT	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi dalam memastikan pelaksanaan pengauditan dan forensik ICT ialah: (a) Memastikan jadual pelaksanaan disediakan; (b) Memastikan laporan dapatan dilaksanakan; dan (c) Memastikan tindakan pembetulan dilaksanakan.	ICTSO
080502 Jejak Audit	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah sepertiberikut: (a) Setiap sistem dan perkakasan ICT mestilah mempunyai jejak audit; (b) Merekod setiap aktiviti transaksi; (c) Memastikan maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (d) Memastikan aktiviti capaian pengguna ke atas sistem ICT sama ada secara sah atau sebaliknya; (e) Semakan jejak audit hendaklah dilakukan dari semasa ke semasa bagi membantu mengesan aktiviti yang luar biasa dengan lebih awal; (f) Menganalisa maklumat aktiviti sistem yang luar biasa atau aktiviti yang tidak mempunyai ciri-ciri keselamatan; (g) Jejak audit hendaklah disimpan untuk tempoh masa yang ditetapkan; dan (h) Jejak audit hendaklah dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT
080503 Sistem dan Pemantauan Log	**Tanggungjawab**
Perkara-perkara berikut hendaklah dilaksanakan: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, aktiviti ini hendaklah dilaporkan kepada ICTSO dan Pengurus ICT.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT

0806 Kawalan Teknikal Keterdedahan (*Vulnerability*)	
Objektif : Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
080601 Kawalan daripada Ancaman Teknikal	**Tanggungjawab**
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan keterdedahan ancaman maklumat teknikal diperolehi daripada pihak berkaitan; (b) Menilai tahap keterdedahan bagi mengenal pastitahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT
080602 Pematuhan Keperluan Audit	**Tanggungjawab**
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT serta Pengguna

BIDANG 09 : PENGURUSAN KOMUNIKASI

0901 Pengurusan Keselamatan Rangkaian **Objektif** : Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
090101 Kawalan Infrastruktur Rangkaian	**Tanggungjawab**
Infrastruktur rangkaian mestilah dikawal dan diuruskan sebaik mungkin demi melindungi sistem dan aplikasi dalam rangkaian daripada ancaman. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yangtidak dibenarkan; (b) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas daripada risiko seperti banjir, gegaran dan habuk; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Peralatan keselamatan seperti *firewall* hendaklahdipasang bagi memastikan hak capaian ke atas sistem ICT dapat dilaksanakan; (e) Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan; (f) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran; (g) Memasang perisian IPS bagi mengesan sebarang cubaan pencerobohan dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat KKR; dan (h) Sebarang penyambungan rangkaian yang bukan di bawah kawalan KKR adalah tidak dibenarkan;	ICTSO, Pentadbir Pusat Data dan Rangkaian ICT

090102 Keselamatan Perkhidmatan Rangkaian	Tanggungjawab
Perkhidmatan rangkaian hendaklah dipastikan sentiasa selamat bagi memastikan kerahsiaan, integriti danketersediaan maklumat terjamin. Perkara-perkara yang perlu dipatuhi adalah: (a) Mekanisme keselamatan, tahap ketersediaan perkhidmatan dan keperluan pengurusan perkhidmatan rangkaian hendaklah dikenal pasti dan dinyatakan dalam perjanjian perkhidmatan rangkaian, sama ada perkhidmatan disediakan secara *in-house* ataupun *outsourced*; (b) Semua trafik keluar dan masuk hendaklah ditapis oleh peralatan keselamatan di bawah kawalanKKR; dan (c) Sebarang aktiviti yang dilarang seperti yang termaktub di dalam Pekeliling Kemajuan Pentadbiran Awam (PKPA) yang berkuat kuasa perlu disekat melalui penggunaan *Web Content Filtering*.	ICTSO, Pentadbir Pusat Data dan Rangkaian ICT

090103 Pengasingan Rangkaian	Tanggungjawab
Pengasingan perkhidmatan rangkaian bertujuan meminimumkan risiko capaian tidak sah dan pengubahsuaian yang tidak dibenarkan. Perkara-perkara yang perlu dipatuhi adalah: (a) Mengenal pasti fungsi dan tanggungjawabpengguna; (b) Mengkonfigurasi hak capaian pengguna mengikut segmen rangkaian berdasarkan keperluan; (c) Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna yang dibenarkan sahaja; (d) Mengemaskinikan hak capaian pengguna dari masa ke semasa mengikut keperluan; dan (e) Operasi rangkaian hendaklah diasingkan untuk meminimumkan risiko capaian dan pengubahsuaian yang tidak dibenarkan.	ICTSO, Pentadbir Pusat Data dan Rangkaian ICT

0902 Pengurusan Pertukaran Maklumat

Objektif : Memastikan keselamatan pertukaran maklumat dan perisian antara KKR dan agensi luar terjamin.

090201 Pengurusan E-mel	Tanggungjawab
Perkara-perkara yang perlu dipatuhi dalam penggunaane-mel adalah seperti berikut: (a) Menggunakan akaun e-mel yang disediakan oleh KKR sahaja;	Pengguna

(b) Memastikan pengemaskinian peti e-mel (*mailbox*) dilaksanakan supaya kapasiti e-mel tidak melebihi kuota yang telah ditetapkan. (c) Menggunakan akaun e-mel rasmi untuk tujuantugas rasmi sahaja; (d) Mengambil tindakan dan memberi maklum balas terhadap e-mel dengan cepat dan mengambil tindakan segera; dan (e) Memastikan e-mel rasmi yang dihantar atau diterima disimpan mengikut tatacara pengurusan sistem fail elektronik yang telah ditetapkan. (f) Memastikan e-mel yang diterima adalah dari sumber yang dipercayai dan selamat.	
090202 Pengurusan Komunikasi Bersepadu (UC)	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah sepertiberikut: (a) Memastikan setiap komunikasi yang dibuat untuk tujuan rasmi sahaja; (b) Melindungi maklumat rahsia rasmi dan maklumatrasmi Kerajaan; (c) Memastikan maklumat yang dihantar mengikut etika keselamatan yang ditetapkan; dan (d) Akaun yang diperuntukkan oleh KKR sahaja yangboleh digunakan.	Pengguna
0903 Pengurusan Media Sosial **Objektif** : Memastikan keselamatan dan kawalan penyebaran maklumat melalui media sosial.	
090301 Media Sosial	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi di dalam memastikan keselamatan dan kawalan penyebaran maklumat yang dikongsi dan disebarkan melalui media sosial adalah seperti berikut: (a) Tidak menjejaskan kepentingan perkhidmatan awam dan kedaulatan negara; (b) Tidak melibatkan penyebaran maklumat dan dokumen terperingkat; (c) Tidak memaparkan kenyataan yang boleh menjejaskan imej Kerajaan; (d) Tidak menyentuh isu sensitif seperti agama, politik dan perkauman; dan (e) Tidak memaparkan kenyataan yang berunsur fitnah atau hasutan.	Pengguna

090302 Keselamatan Media Sosial	Tanggungjawab
Pegawai yang bertanggungjawab mengendalikan laman web media sosial rasmi perlulah memastikan keselamatan media sosial dengan melaporkan masalah *spam* kepada penyedia perkhidmatan media sosial (Contohnya: *Facebook, Twitter, Instagram*).	ICTSO
0904 Data Terbuka **Objektif** : Data Terbuka Sektor Awam adalah untuk meningkatkan kualiti ketelusan penyampaian perkhidmatan serta meningkatkan produktiviti negara melalui pemanfaatan data terbuka.	
090401 Pengurusan Data Terbuka	**Tanggungjawab**
Pelaksanaan data terbuka KKR perlulah berasaskan tadbir urus dan aktiviti yang telah dipersetujui oleh KSU atau Ketua Bahagian. Perkara-perkara yang perlu dilaksanakan adalah seperti berikut: (a) Menubuhkan struktur tadbir urus atau tadbir urus sedia ada untuk melaksanakan tugas dan aktiviti berkaitan data terbuka KKR; (b) Mengenal pasti set data Bahagian yang boleh dimuatnaik atau dipaut ke Portal Data Terbuka Sektor Awam; dan (c) Membuat semakan semula pelaksanaan data terbuka dan menilai tahap penggunaannya.	CIO dan PengurusICT

BIDANG 10 : PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM

1001 Keselamatan dalam Membangunkan Sistem dan Aplikasi

Objektif : Memastikan sistem yang dibangunkan sendiri atau pihak ketigamempunyai ciri-ciri keselamatan ICT yang bersesuaian.

100101 Keperluan Keselamatan Sistem Maklumat	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pembangunan, penambahbaikan dan penyelenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tiada sebarang ralat yang boleh mengganggu pemprosesan dan ketetapan maklumat; (b) Mewujudkan dan melindungi persekitaran bagi pembangunan yang merangkumi keseluruhan kitar hayat pembangunan sistem; (c) Ujian keselamatan hendaklah dijalankan ke atas sistem input untuk menyemak pengesahan dan integriti data yang dimasukkan, sistempemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna serta sistem output untuk memastikan data yang telahdiproses adalah tepat; (d) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (e) Dokumentasi sistem hendaklah disediakan bagi semua sistem yang dibangunkan sama ada secara dalaman atau sebaliknya.	Pentadbir Sistem ICT dan Pemilik Sistem

100102 Pengesahan Data Input dan Output	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a) Data input bagi aplikasi perlu disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b) Data output daripada aplikasi perlu disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pentadbir Sistem ICT dan Pemilk Sistem

100103 Kawalan Prosesan	Tanggungjawab
Kawalan proses perlu ada dalam aplikasi bagi tujuan mengesan sebarang pengubahsuaian ke atas maklumat yang berkemungkinan terhasil daripada masalah semasa prosesan.	Pentadbir Sistem ICT

100104 Keselamatan Aplikasi di Rangkaian Umum	Tanggungjawab
Maklumat aplikasi yang melalui rangkaian umum (*public networks*) hendaklah dilindungi daripada aktiviti penipuan dan pendedahan maklumat yang tidak dibenarkan. Perkara yang perlu dipertimbangkan adalah seperti berikut: a) Tahap kerahsiaan bagi mengenal pasti identiti masing-masing, misalnya melalui pengesahan (authentication); b) Proses berkaitan dengan pihak yang berhak untuk meluluskan kandungan, penerbitan atau menandatangani dokumen transaksi; c) Memastikan pihak ketiga dimaklumkan sepenuhnya mengenai kebenaran penggunaanperkhidmatan ICT; dan d) Memastikan pihak ketiga memahami keperluan kerahsiaan, integriti, bukti penghantaran serta penerimaan dokumen dan kontrak.	ICTSO, Pentadbir Pusat Data dan Rangkaian ICT, Pentadbir Sistem ICT

100105 Melindungi Transaksi Aplikasi	Tanggungjawab
Maklumat yang terlibat dalam perkhidmatan transaksi hendaklah dilindungi daripada penghantaran yang tidak lengkap, *miss-routing*, pengubahan mesej yang tidak dibenarkan, pendedahan yang tidak dibenarkan danduplikasi mesej. Perkara yang perlu dipertimbangkan adalah seperti berikut: (a) Memastikan semua aspek transaksi dipatuhi: i) Maklumat pengesahan pengguna adalah sahdigunakan dan telah disahkan; ii) Mengekalkan kerahsiaan maklumat; iii) Mengekalkan privasi pihak yang terlibat; iv) Komunikasi antara semua pihak yang terlibat dirahsiakan; dan v) Protokol yang digunakan untuk berkomunikasi antara semua pihak dilindungi.	Pusat Data dan Rangkaian ICT, Pentadbir Sistem ICT

100106 Kawalan Fail Sistem	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian fail sistem hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; (b) Kod sumber sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; (c) Mengawal capaian ke atas kod sumber sistem bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati,dilindungi dan dikawal; dan (e) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT
1002 Keselamatan dalam Proses Pembangunan dan Sokongan **Objektif** : Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.	
100201 Dasar Keselamatan Dalam Pembangunan Sistem	Tanggungjawab
Peraturan untuk pembangunan sistem hendaklah diwujudkan dan digunakan untuk perkembangan dalam organisasi. Perkara yang perlu dipertimbangkan adalah seperti berikut: a) Keselamatan persekitaran pembangunan; b) Panduan keselamatan dalam kitar hayat pembangunan (*development lifecycle*) perisian; c) Keselamatan dalam fasa reka bentuk; d) Pemeriksaan keselamatan dalam perkembangan projek; e) Keselamatan repositori; f) Keselamatan dalam kawalan versi; g) Keperluan pengetahuan keselamatan dalam pembangunan perisian; h) Kebolehan pembekal untuk mengenalpasti kelemahan; dan i) Mencadangkan penambahbaikan dalam pembangunan sistem.	Pentadbir Sistem ICT

100202 Prosedur Kawalan Perubahan	Tanggungjawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diujiapabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Pegawai yang bertanggungjawab perlu memantau penambahbaikan dan pembetulan yang dilakukan oleh pembekal; (c) Mengawal perubahan dan/atau pindaan ke atas pakej perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (d) Akses kepada kod sumber sistem perlu dihadkan kepada pengguna yang dibenarkan sahaja; dan (e) Menghalang sebarang peluang kebocoran maklumat.	Pengurus ICT, Pentadbir Sistem ICTserta Pentadbir Pusat Data dan Rangkaian ICT
100203 Prosedur Pembangunan Sistem Aplikasi	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Permohonan secara rasmi hendaklah dikemukakan kepada urus setia JPICT Kementerian untukkelulusan; (b) Permohonan hendaklah lengkap meliputi spesifikasi teknikal, anggaran kos yang terlibat, guna tenaga dan juga skop perluasan sistem aplikasi tersebut; (c) Pembangunan sistem aplikasi hendaklah mengambil kira sistem aplikasi sedia ada di KKR dan agensi lain bagi mengelakkan pertindihan pembangunan sistem aplikasi yang sama; (d) Sebarang pembangunan sistem aplikasi mestilah menggunakan kod-kod piawai di bawah DDSA; dan (e) Sesuatu pembangunan sistem aplikasi perlu mempunyai Pemilik Sistem kepada sistem aplikasi tersebut;	Pentadbir Sistem ICT dan Pemilik Sistem

(f) Pemilik Sistem aplikasi bertanggungjawabmempromosi dan memastikan kelancaran pelaksanaan sistem; (g) Pemilik Sistem aplikasi hendaklah membaca dan memahami dokumentasi serta mematuhi prosedur yang berkaitan; (h) Pemilik Sistem aplikasi perlu melaporkan kepada JPICT secara berkala bagi kemajuan pelaksanaan sistem; (i) Memastikan pembangunan sistem menggunakan teknik *secure coding*; (j) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagihkan kepada pihak lain kecuali dengan kebenaran Pengurus ICT; dan (k) Kod sumber sistem hendaklah disimpan dengan teratur dan sebarang pindaan hendaklah direkodkan.	
100204 Kawalan Kod Sumber dan Dokumentasi Sistem Aplikasi	**Tanggungjawab**
Kawalan kod sumber dan dokumentasi sistem aplikasihendaklah dilaksanakan ke atas sistem yangdibangunkan secara *outsource* dan *in-house*. Ini bagi memastikan kesinambungan sistem aplikasi itu dapat berjalan dengan lancar sama ada selepas pertukaran pegawai atau penyerahan sistem kepada Pemilik Sistem Aplikasi. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan kod sumber dan dokumentasi bagi setiap sistem yang dibangunkan disediakan sama ada secara *hardcopy* dan/atau *softcopy*; (b) Dokumentasi bagi konfigurasi integrasi antara sistem induk dan aplikasi *mobile* disediakan; (c) Semua dokumentasi diletakkan secara berpusat, dikawal dan direkodkan; dan (d) Memastikan kod sumber sistem dan dokumentasi ialah hak milik Kerajaan.	Pentadbir Sistem ICT

100205 Penamatan Penggunaan Sistem Aplikasi	Tanggungjawab
Memaklumkan dan mencadangkan penamatan sistem aplikasi secara bertulis kepada urus setia JPICT sekiranya tidak lagi digunakan/diperlukan.	Pengurus ICT, Pentadbir Sistem ICT dan Pemilik Sistem
100206 Prosedur Pembangunan Laman Web dan Aplikasi Web	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua maklumat yang hendak dimuatkan ke dalam laman web mestilah mendapat kelulusan Ketua Bahagian; (b) Maklumat yang terkandung dalam laman web adalah di bawah tanggungjawab Ketua Bahagian masing-masing; (c) Maklumat di laman web hendaklah dikemas kinidari semasa ke semasa; (d) Laman web agensi luar yang memerlukan pautan ke Laman Web KKR atau sebaliknya mestilah mendapat kebenaran Ketua Bahagian; dan (e) Pembangunan laman web dan aplikasi web hendaklah mempunyai ciri-ciri keselamatan bagi mengelak diceroboh dan digodam.	Pentadbir Sistem ICT, Pentadbir Web dan Ketua Bahagian
100207 Prosedur Pembangunan Aplikasi *Mobile*	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pembangunan aplikasi mobile mestilah menggunakan API sebagai antara muka hubungan dengan sistem induk; dan (b) Sistem aplikasi *mobile* yang dibangunkan perlu melalui akaun langganan GAMMA untuk dimuat naik ke *Apps Market Place*. (Contohnya : *Apple App Store, Google Play*)	Pentadbir Sistem ICT
100208 Pembangunan Perisian Secara *Outsource*	**Tanggungjawab**
Pembangunan perisian aplikasi secara *outsource* perlu dipantau oleh pemilik sistem. *Source code* adalah menjadi hak milik KKR.	Pentadbir Sistem ICT

100209 Ujian Keselamatan Sistem	Tanggungjawab
Ujian keselamatan sistem hendaklah dijalankan ke atastiga (3) peringkat pemprosesan maklumat iaitu peringkat kemasukan data (*input*), peringkat pemprosesan data (proses) dan peringkat penjanaan laporan (*output*). Perkara-perkara yang perlu dipatuhi oleh pentadbir sistem adalah: (a) Merancang dan melaksanakan penilaian risiko mengikut keperluan bagi mengenal pasti dan melaksana kawalan yang sesuai bagi pengesahan dan perlindungan integriti data dalam aplikasi; (b) Merancang dan melaksana *Security Posture Assessment* (SPA) bagi mengenal pasti kelemahan sistem; dan (c) Membuat semakan pengesahan sistem aplikasiuntuk mengenal pasti sebarang pencemaran maklumat sama ada disebabkan oleh kesilapan atau disengajakan.	Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT
100210 Pengujian Penerimaan Sistem	**Tanggungjawab**
Program Pengujian Penerimaan Sistem (Ujian Penerimaan Pengguna dan Ujian Penerimaan Akhir) hendaklah dilaksanakan berdasarkan kriteria yang telah ditetapkan sebelum sistem diguna pakai.	Pentadbir Sistem ICT, Pihak Ketiga dan Pemilik Sistem
1003 Data Ujian **Objektif :** Memastikan keselamatan data yang digunakan	
100301 Perlindungan Data Ujian	**Tanggungjawab**
Perkara-perkara yang perlu dipatuhi adalah sepertiberikut: a) Data dan atur cara yang hendak diuji perlu dipilih, dilindungi dan dikawal; b) Pengujian hendaklah dibuat ke atas aturcara yang terkini; dan c) Mengaktifkan audit log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT

BIDANG 11 : HUBUNGAN DENGAN PEMBEKAL/PIHAK KETIGA

1101 Pihak Ketiga

Objektif : Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga. Contohnya: Pembekal dan Pakar Runding.

110101 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	Tanggungjawab
Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketigadikawal. Perkara yang perlu dipatuhi termasuk yang berikut; (a) Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; (b) Mengenal pasti keperluan keselamatan sebelummemberi kebenaran capaian atau kepenggunaan kepada pihak ketiga; (c) Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dilaksanakan dan dipatuhi: i. Tapisan Keselamatan (jika perlu); dan ii. Perakuan Akta Rahsia Rasmi 1972; (d) Akses kepada asset ICT KKR perlu pengawasan oleh Pegawai berkenaan;	CIO, Pengurus ICT, ICTSO, Pentadbir Sistem ICT, PentadbirPusat Data dan Rangkaian ICT serta Pihak ketiga

110102 Kawalan Keselamatan Maklumat Melalui Perjanjian Dengan Pembekal	Tanggungjawab
Semua keperluan keselamatan maklumat hendaklah relevan dan dipersetujui dengan setiap pembekal bagi mengakses, memproses, menyimpan, berkomunikasi, atau menyediakan komponen infrastruktur, maklumat Kementerian. Perkara-perkara yang perlu dipatuhi adalah:- a) Penerangan maklumat keselamatan; b) Mematuhi klasifikasi keselamatan maklumat; c) Keperluan undang-undang dan peraturan; d) Obligasi setiap pihak bagi kawalan akses,pemantauan, pelaporan dan pengauditan;	CIO, Pengurus ICT, ICTSO, Pentadbir Sistem ICT, PentadbirPusat Data dan Rangkaian ICT serta Pihak ketiga

e) Penerimaan peraturan penggunaan maklumat oleh pembekal; f) Hak untuk mengaudit pembekal; dan g) Kewajipan pembekal mematuhi keperluan keselamatan maklumat.	
1102 Pengurusan Penyampaian Perkhidmatan Pembekal **Objektif :** Memastikan pembekal memberi perkhidmatan terbaik dan sebarangperubahan yang berlaku dipihak pembekal tidak menjejaskan kementerian.	
110201 Pemantauan dan Kajian Perkhidmatan Pembekal	**Tanggungjawab**
KKR hendaklah sentiasa memantau, mengkaji semula dan mengaudit perkhidmatan pembekal/pihak ketiga. Perkara yang perlu dipatuhi adalah: a) Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b) Memantau tahap prestasi perkhidmatan untuk mengesahkan pembekal mematuhi perjanjian perkhidmatan; dan c) Mengkaji semula laporan perkhidmatan yang dihasilkan oleh pembekal dan mengemukakan status kemajuan.	CIO, Pengurus ICT, ICTSO serta Pihak Ketiga
110202 Pengurusan Perubahan Perkhidmatan Pembekal	**Tanggungjawab**
Perkara yang perlu diambil kira adalah: a) Perubahan dalam perjanjian dengan pembekal; b) Perubahan yang dilakukan oleh KKR bagi meningkatkan perkhidmatan selaras dengan penambahbaikan sistem, pengubahsuaian dasar dan prosedur; dan c) Perubahan dalam perkhidmatan pembekal selaras dengan perubahan rangkaian, teknologi baru, produk-produk baru, perkakasan baru, perubahan lokasi, pertukaran kakitangan pembekal dan perubahan sub- kontraktor pembekal.	CIO, Pengurus ICT, ICTSO serta Pihak Ketiga

BIDANG 12 : PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN SIBER SEKTOR AWAM

1201 Mekanisme Pelaporan Insiden Keselamatan ICT

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

120101 Mekanisme Pelaporan Insiden	Tanggungjawab
Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CSIRT KKR dengan kadar segera apabila: (a) Maklumat disyaki/didapati hilang atau terdedah kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat disyaki atau digunakan tanpa kebenaran; (c) Kata laluan atau mekanisme kawalan akses hilang, dicuri atau didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Ringkasan bagi semua proses kerja yang terlibat dalam pelaporan insiden keselamatan ICT di KKR seperti di **Lampiran 2**. Tindakan terhadap insiden keselamatan siber yang berlaku hendaklah dibuat berasaskan kepada keseriusan sesuatu insiden. Tahap keutamaan tindakan terhadap insiden keselamatan siber akan ditentukan seperti yang berikut: (i) **Keutamaan 1** - insiden keselamatan siber yang memberi impak tinggi terhadap pertahanan dan keselamatan negara, kestabilan ekonomi negara, imej negara, keupayaan Kerajaan untuk berfungsi, kesihatan dan keselamatan awam serta privasi individu. (ii) **Keutamaan 2 -** insiden keselamatan siber yang tidak memberi impak seperti mana yang dinyatakan dalam Keutamaan 1. Sekiranya berstatus **Keutamaan 1,** agensi hendaklah melaporkan insiden kepada NC4 bagi tujuan penyelarasan dan memaklumkan kepada agensi yang menyelianya dalam tempoh 24 jam selepas insiden dikesan serta mengaktifkan Pelan Kesinambungan Perkhidmatan (Business Continuity Plan, BCP) dan Pelan Pemulihan Bencana (Disaster Recovery Plan, DRP) sekiranya perlu.	CIO, ICTSO, CSIRT KKR, Pengguna

Bagi **Keutamaan 2**, agensi hendaklah melaksanakan pengendalian insiden secara kendiri dan seterusnya memaklumkan kepada NC4 dan agensi yang menyelianya setelah proses pengendalian insiden dan pemulihan pada peringkat agensi selesai.

Dengan berkuat kuasanya Pekeliling Am ini, pekeliling/ surat pekeliling/ surat arahan berikut adalah dibatalkan :

a) Pekeliling Am Bilangan 1 Tahun 2001 Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT);

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

c) Surat Arahan Ketua Pengarah MAMPU bertarikh 23 Mac 2009 Pengaktifan Fail Log Server Bagi Tujuan Pengurusan Pengendalian Insiden Keselamatan ICT di Agensi-Agensi Kerajaan.

Semua insiden keselamatan ICT yang berlaku mesti dilaporkan kepada ICTSO dan kepada Jawatankuasa CSIRT KKR untuk pengendalian dan pengumpulan statistik insiden keselamatan ICT Kerajaan. Semua maklumat adalah SULIT dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan.

Apabila berlakunya insiden keselamatan siber, pengarah CSIRT Agensi hendaklah menggerakkan ahli CSIRT Agensi untuk mengambil tindakan seperti yang berikut:

(i) Mengurus dan mengambil tindakan terhadap insiden yang berlaku sehingga keadaan pulih.
(ii) Mengaktifkan BCP dan/atau DRP jika perlu.
(iii) Melapor dan memaklumkan insiden keselamatan siber kepada NC4 serta agensi yang menyelianya.
(iv) Menentukan sama ada insiden ini perlu dilaporkan kepada agensi penguatkuasaan undang-undang.
(v) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti.

1202 Pengurusan Maklumat Insiden Keselamatan ICT **Objektif** : Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
120201 Prosedur Pengurusan Maklumat Insiden Keselamatan ICT	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Menyimpan jejak audit, backup secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (c) Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan (jika perlu); dan (d) Memastikan pemulihan dilaksanakan dengan segera.	CIO, ICTSO, CSIRT KKR

BIDANG 13 : ASPEK KESELAMATAN MAKLUMAT & PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1301	Dasar Kesinambungan Perkhidmatan	
Objektif : Menjamin operasi perkhidmatan agar tidak tergendala dan penyampaian perkhidmatan yang berterusan kepada pelanggan.		
130101	Perancangan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	Tanggungjawab
Aspek keselamatan maklumat hendaklah menjadi elemen penting dalam pembangunan Pelan Pengurusan Kesinambungan Perkhidmatan (PKP) KKR bagi memastikan perkhidmatan KKR tidak terganggu semasa krisis atau bencana.		Koordinator PKP
130102	Pelaksanaan Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	Tanggungjawab
Pelan Pengurusan Kesinambungan Perkhidmatan (PKP) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Perkara yang perlu diberi perhatian: (a) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes, impak gangguan yang mungkin berlaku dan kesannya terhadap keselamatan ICT serta tindakan bagi meminimumkan impak gangguan tersebut; (b) Melaksanakan prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (c) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (d) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (e) Membuat backup; dan (f) Menguji dan mengemaskini pelan sekurang-kurangnya setahun sekali.		Koordinator PKP

Pelan PKP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai pegawai KKR dan pembekal besertanombor yang boleh dihubungi (Contohnya: faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel yang tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan. Salinan pelan PKP perlu disimpan di lokasi berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama.	
130103 Pengujian Keselamatan Maklumat Dalam Kesinambungan Perkhidmatan	**Tanggungjawab**
Pelan PKP hendaklah diuji sekurang-kurangnya setahun sekali atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian pelan PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan.	Koordinator PKP

130104 Pelan Pengurusan Pemulihan Bencana	Tanggungjawab
Pelan Pemulihan Bencana (*Disaster Recovery Plan*) direkabentuk untuk membantu agensi mengembalikan semula proses perkhidmatan dalam tempoh ditetapkan untuk pemulihan bencana. Ia merujuk kepada dokumen pelan yang menetapkan sumber tindakan, tanggungjawab dan data yang diperlukan untuk mengurus proses pemulihan selepas berlaku gangguan dalam perkhidmatan agensi. Pelan ini mestilah diluluskan oleh pengurusan atasan BPM dan perkara-perkara berikut perlu diberi perhatian : a) Senarai pegawai KKR dan pembekal beserta nombor yang boleh dihubungi (Contohnya: faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel yang tidak dapat hadir untuk menangani insiden; b) Mengenalpasti pejabat alternatif dan/atau pusat pemulihan bencana (Disaster Recovery Centre – DRC) yang berbeza dari lokasi asal bagi meneruskan perkhidmatan apabila lokasi asal menghadapi gangguan/bencana. c) Mengenalpasti peranan dan tanggungjawab Pasukan Pemulihan Bencana serta pembekal berkaitan; d) Mengenalpasti system/aplikasi yang memerlukan backup; e) Menyediakan infrastruktur bagi memastikan pemulihan boleh dilaksanakan; f) Mendokumentasikan proses dan prosedur yang digunapakai untuk pemulihan maklumat dan kemudahan yang berkaitan; g) Melaksanakan pengujian dan latihan kepada kaktangan terlibat; dan h) Mengemaskini pelan apabila perlu.	Pengurus ICT, ICTSO, Pentadbir Sistem ICT, Pentadbir Pusat Data dan Rangkaian ICT
1302 *Redundancy* **Objektif :** Memastikan ketersediaan fasiliti pemprosesan maklumat	
130201 Ketersediaan Kemudahan Pemprosesan Maklumat	Tanggungjawab
Kemudahan pemprosesan maklumat perlu mempunyai *redundancy* yang mencukupi untuk memenuhi keperluan ketersediaan. Kemudahan *redundancy* perlu diuji (*failover test*) keberkesanannya dari masa ke semasa.	ICTSO

BIDANG 14 : PEMATUHAN

1401 Pematuhan dan Keperluan Perundangan **Objektif** :Meningkatkan tahap keselamatan ICT bagi mengelak daripada pelanggaran DKICT KKR.	
140101 Pematuhan Dasar	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna KKR hendaklah membaca,memahami dan mematuhi DKICT KKR dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa; (b) Semua aset ICT KKR termasuk data dan maklumat yang disimpan di dalamnya ialah hak milik Kerajaan. ICTSO berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain daripada tujuan yang telah ditetapkan; dan (c) Sebarang penggunaan aset ICT KKR selain daripada maksud dan tujuan yang telah ditetapkan juga merupakan satu penyalahgunaan sumber KKR.	Pengguna
140102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	**Tanggungjawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap pengguna hendaklah memastikan bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal yang ditetapkan (jika ada); dan (b) Sistem maklumat perlu diperiksa dan dipantau secara berkala bagi mematuhi piawaian pelaksanaan keselamatan ICT.	Pengurus ICT, ICTSO dan Pengguna
140103 Mengenal Pasti Undang-Undang dan Perjanjian Kontrak	**Tanggungjawab**
Senarai perundangan dan peraturan yang perlu dipatuhi oleh pengguna aset ICT KKR adalah seperti di Lampiran 3. Pengguna juga perlu mematuhi perundangan dan peraturan semasa yang berkuat kuasa.	Pengguna dan Pihak Ketiga

140104 Perlindungan Rekod	Tanggungjawab
Rekod hendaklah dilindungi daripada kehilangan, kemusnahan, pemalsuan, capaian dan pengeluaran yang tidak sah mengikut undang-undang, peraturan, kontrakdan keperluan KKR.	Pengguna dan Pihak Ketiga
140105 Privasi dan Perlindungan Maklumat Peribadi	**Tanggungjawab**
Maklumat peribadi dan privasi pengguna hendaklah dilindungi seperti yang tertakluk dalam undang-undang kerajaan Malaysia dan peraturan-peraturan yang berkaitan.	Pengguna dan Pihak Ketiga
140106 Peraturan Kawalan Kriptogafi	**Tanggungjawab**
Kawalan kriptografi hendaklah dilaksanakan berdasarkan kepada perjanjian kontrak, undang-undang dan peraturan-peraturan berkaitan.	ICTSO
140107 Pelanggaran Dasar	**Tanggungjawab**
Mengambil tindakan undang-undang dan tatatertib ke atas sesiapa yang terlibat di dalam semua perbuatan kecuaian, kelalaian dan perlanggaran keselamatan yang membahayakan perkara-perkara terperingkat di bawah Akta Rahsia Rasmi 1972 dan akta lain yang berkaitan. SUB (PM) atau ICTSO adalah berhak untuk mengambil tindakan sebagaimana berikut:- (a) Membuat teguran pertama melalui e-mel, sistem pemantauan atau mana-mana medium komunikasi secara atas talian; (b) ICTSO akan memberi e-mel/surat teguran kepada pelaku dan satu salinan emel akan turut diberi kepada Ketua Bahagian/pegawai pelaku; dan (c) Pelaku hendaklah memberi surat tunjuk sebab dalam tempoh tiga (3) hari bekerja dari tarikh e-mel/surat diterima; dan (d) SUB (PM) atau ICTSO berhak mengambil tindakan berupa menarik balik kemudahan capaian internet/ peralatan ICT/ komputer (sementara/kekal) bergantung kepada jenis dan tahap kesalahan.	Pengurus ICT, ICTSO, Pengguna dan Pihak Ketiga

1402 Pemantauan ke atas Pematuhan Dasar **Objektif :** Memastikan pemantauan ke atas pematuhan dasar dilaksanakan secara menyeluruh di Kementerian	
140201 Audit Pemahaman dan Pematuhan ICT	**Tanggungjawab**
Audit pemahaman dan pematuhan ICT perlu dilaksanakan sekurang-kurangnya sekali setahun bagi warga Kementerian bertujuan mengurangkan kebarangkalian wujudnya insiden keselamatan ICT di KKR.	ICTSO

8.0 GLOSARI

Berikut ialah jadual glosari bagi perkataan yang digunakan dalamkeseluruhan dokumen ini.

BIL.	GLOSARI	KETERANGAN GLOSARI
1.	Antivirus	Perisian yang digunakan untuk mengesan, mengasingkan, memadamkan dan melaporkan virus atau kad perosak dalamsistem komputer.
2.	API *Mobile*	Satu teknik pengaturcaraan yang menghubungkan antara sistem induk dan aplikasi *mobile*.
3.	Aset ICT	Peralatan ICT termasuk perkakasan, perisian, data, maklumat, perkhidmatan dan manusia.
4.	*Backup*	Aktiviti menyediakan sandaran atau penduaan sesuatu fail, data, maklumat atau sistem maklumat bagi membolehkan ia terpelihara dan dapat digunakan apabilasumber utama tidak berfungsi atau terhapus.
5.	*Bandwidth*	Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi dalam jangka masa yang ditetapkan. Contohnya: *video streaming* dan *teleconference*.
6.	*Broadband*	Teknologi yang menyediakan capaian Internet melalui rangkaian luas.
7.	BYOD	Peralatan mudah alih persendirian seperti telefon pintar, *tablet*, komputer riba danmedia storan yang digunakan untuk tujuan rasmi.

BIL.	GLOSARI	KETERANGAN GLOSARI
8.	CERT	Organisasi yang ditubuhkan untukmembantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing- masing dan agensi di bawah kawalannya.
9.	CIO	Pegawai yang dilantik untuk menjadi peneraju dalam merancang, melaksana dan memantau program Kerajaan berasaskan ICT bagi memudahkan pelanggan berurusan dengan agensi Kerajaan. Beliaujuga merupakan agen transformasi menerusi inovasi, kreativiti dan inisiatif pembaharuan yang berterusan.
10.	*Clear Desk dan Clear Screen*	Tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin apabila pengguna tidak berada di tempatnya.
11.	*Cloud Computing*	Proses menyimpan dan mengurus maklumat di Internet melalui aktiviti memuat turun dan memuat naik maklumatdi dalam storan yang dikongsi di Internet. Maklumat ini boleh dicapai melalui pelbagai peralatan seperti computer, *tablet*, telefon pintar dan sebagainya.
12.	Dokumen ICT	Dokumen fizikal dan dokumen digital.
13.	E-Dagang	Urusan jual beli secara dalam talian yang melibatkan jualan produk dan mendapatkan keuntungan daripada jualan tersebut.
14.	Enkripsi (Encyption)	Penukaran data sensitif kepada bentuk kod sulit untuk membolehkan data dikirim dengan selamat tanpa difahami pihak lain.

BIL.	GLOSARI	KETERANGAN GLOSARI
15.	ICT	Penggabungan teknologi maklumat dan teknologi komunikasi dalam perolehan, penyimpanan, pemprosesan dan pengagihan maklumat secara elektronik.
16.	ICTSO	Pegawai yang dilantik dan tanggungjawabterhadap keselamatan ICT.
17.	ICT Hijau	Amalan daripada segi pengeluaran, penggunaan dan pelupusan komputer, pelayan (*server*) serta alat-alat aksesori seperti monitor, tetikus, pencetak dan peralatan rangkaian secara berkesan dan efektif dengan memberi kesan yang minima atau tiada kesan terhadap alam sekitar.
18.	IDS	Sistem yang menyiasat semua aktiviti rangkaian dan mengenal pasti pola yang disyaki untuk menunjukkan bahawa rangkaian atau sistem diceroboh. Terdapat dua bentuk IDS yang lazim, iaitu pegesanan salah guna dan pengesanan anomali. Dalam pengesanan salah guna, IDS menganalisis maklumat yang dikumpul dan membandingkannya dengan pangkalan data tandatangan serangan yang besar. Secara khusus IDS mencari serangan tertentu yang telah didokumenkan. Seperti sistem pengesan virus, keberkesanan perisian pengesan salah guna ini hanyalahbergantung kepada sebaik mana pangkalan data tandatangan serangan yang ada untuk membandingkan maklumat yang dikumpul.
19.	Internet	Sistem perangkaian antarabangsa yang membolehkan pengguna di seluruh dunia berhubung antara satu sama lain dan mencapai maklumat di seluruh dunia.

BIL.	GLOSARI	KETERANGAN GLOSARI
20.	Insiden keselamatan ICT	Musibah (advise event) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin satu perbuatan yang melanggar DKICT sama ada yang ditetapkan secara tersurat atau tersirat.
21.	IPS	Perkakasan keselamatan komputer yang memantau rangkaian dan / atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindak balasmenyekat atau menghalang aktiviti serangan seperti *malicious code*. Contohnya: *Network-based* IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
22.	Jejak Audit (*audit trail*)	Log yang merekod aktiviti-aktiviti yang berlaku dalam sistem secara kronologi bagi membenarkan pemeriksaan dan pembinaan semual dilakukan bagi susunan danperubahan dalam sesuatu acara.
23.	Kriptografi	Penulisan kod rahsia yang membolehkan penghantaran dan storan data dalam bentuk yang hanya difahami oleh pihak tertentu sahaja.
24.	LAN	Rangkaian komputer yang berkongsi data dan sumber dalam sesuatu kawasan yang terhad seperti sebuah bangunan dan sebuah pejabat.
25.	Lesen perisian	Maklumat yang berkaitan pendaftaran, pengesahan lesen bagi membolehkan perisian digunakan secara sah seperti *registration code*, *serials* dan *CD-keys*.

BIL.	GLOSARI	KETERANGAN GLOSARI
26.	*Log out*	Tindakan menarik diri secara rasmi daripada log sistem komputer sebelum berhenti secara muktamad daripada menggunakan sistem.
27.	*Malicious Code*	Sebahagian atau keseluruhan kod atur cara terkompil, skrip, atau jujukan arahan sistem pengendalian atau perisian yang boleh menyebabkan sistem bertindak dengan cara yang tidak diingini oleh Pemilik Sistem dan pengguna. Ia mampu menyebabkan kemudaratan kepada data, pengguna, sumber atau aset sistem komputer yang disasarkan.
28.	Media Sosial	Saluran komunikasi dalam talian yangberasaskan Internet yang membolehkan penggunanya berhubung, bertukar-tukar maklumat, berkongsi idea, bekerjasama dan membina komuniti.
29.	Media Storan	Peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti cakera padat, pita magnetic, *optical disk*, *flash disk*, CDROM, *thumb drive* dan media storan lain.
30.	*Mobile code*	Kod program yang boleh disebarkan dari komputer ke komputer dan di execute secara automatik. Contohnya: JavaScript, VBScript, applet Java, ActiveX, Flash, Shockwave dan *macro embedded* bagidokumen Microsoft Office.
31.	Muat turun	Tindakan memindahkan fail atau data daripada sumber tertentu ke komputer pengguna melalui talian rangkaian.

BIL.	GLOSARI	KETERANGAN GLOSARI
32.	*Outsource*	Menggunakan perkhidmatan luar atau pihak ketiga untuk melaksanakan fungsi- fungsi tertentu ICT bagi suatu tempoh berdasarkan dokumen perjanjian dengan bayaran yang telah dipersetujui.
33.	Pegawai Pengawal	KSU/Ketua Jabatan.
34.	Pemilik Sistem	Pemilik bisnes (*business owner*) bagi sistemyang dibangun atau yang paling banyak memiliki data.
35.	Pengguna	Warga KPKT di Bahagian / Jabatan / Agensi termasuk pegawai yang berkhidmat secarakontrak atau pegawai khidmat singkat yang menggunakan aset ICT secara langsung atau tidak langsung.
36.	Pentadbir SistemICT	Pentadbir yang melaksanakan dan menyelenggarakan sistem aplikasi, lamanweb dan aplikasi *mobile*.
37.	Pentadbir Pusat Data dan Rangkaian ICT	Pentadbir yang melaksanakan dan menyelenggarakan rangkaian ICT dan komunikasi ICT serta Pusat Data.
38.	Peralatan ICT	Merujuk kepada semua perkakasan danperisian ICT.
39.	Perkakasan ICT	Merujuk kepada komponen dalaman peralatan ICT.

BIL.	GLOSARI	KETERANGAN GLOSARI
40.	Perisian	Set atur cara komputer yang menjalankan sesuatu tugas pada sistem komputer. Terdapat tiga (3) jenis perisian atau sistem pengendali (contohnya: Linux dan Windows), sistem utiliti (contohnya: *Disk Cleanup* dan *Disk Defregmenter) dan* perisian aplikasi (contohnya: Microsoft Office dan Google Chrome).
41.	Pihak Ketiga	Pembekal, pakar runding dan individu yang dilantik untuk melaksanakan tugas di KKR dalam jangka masa yang tertentu.
42.	PKI	Sistem enkripsi lengkap khusus untukmencipta dan mengurus kekunci awam semasa proses penyulitan data dan pertukaran kekunci dalam kalangan pengguna. Ia merupakan satu kombinasi perisian, teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
43.	*Restore*	Proses penarikan semula data.
44.	*Router*	Peranti yang digunakan untuk menghantar data antara dua (2) rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya capaian Internet.
45.	*Screen Saver*	Imej yang akan diaktifkan pada komputer setelah ia tidak digunakan dalam jangka masa tertentu.
46.	*Server*	Unit dalam rangkaian yang membekalkan data dan maklumat kepada komputer lainyang mempunyai hubungan rangkaian dengannya.

BIL.	GLOSARI	KETERANGAN GLOSARI
47.	*Switch*	Alat yang boleh menapis (*filter*) dan memajukan (*forward*) isyarat paket data antara segmen rangkaian LAN.
48.	UC	Saluran-saluran komunikasi elektronik selain e-mel yang disepadukan dan antaramuka yang sama dalam satu rangkaian.

9.0 LAMPIRAN

Berikut ialah lampiran-lampiran yang berkaitan sebagai panduan.

i. Lampiran 1: Surat Akuan Pematuhan Dasar Keselamatan ICT KKR;
ii. Lampiran 2: Proses Kerja Pelaporan Insiden Keselamatan ICT (CERT) KKR; dan
iii. Lampiran 3: Senarai Perundangan dan Peraturan.

LAMPIRAN 1
Pindaan 1/2019

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT

KEMENTERIAN KERJA RAYA

Nama :

No. Kad Pengenalan :

Jawatan :

Bahagian :

Kementerian :

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa:-

1. Saya telah mengikuti Taklimat Dasar Keselamatan ICT (DKICT);
2. Saya juga telah membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam Dasar Keselamatan ICT ; dan
3. Jika saya ingkar kepada peruntukan-peruntukan yang ditetapkan, maka tindakan sewajarnya boleh diambil ke atas diri saya.

.....

( )

Tarikh :

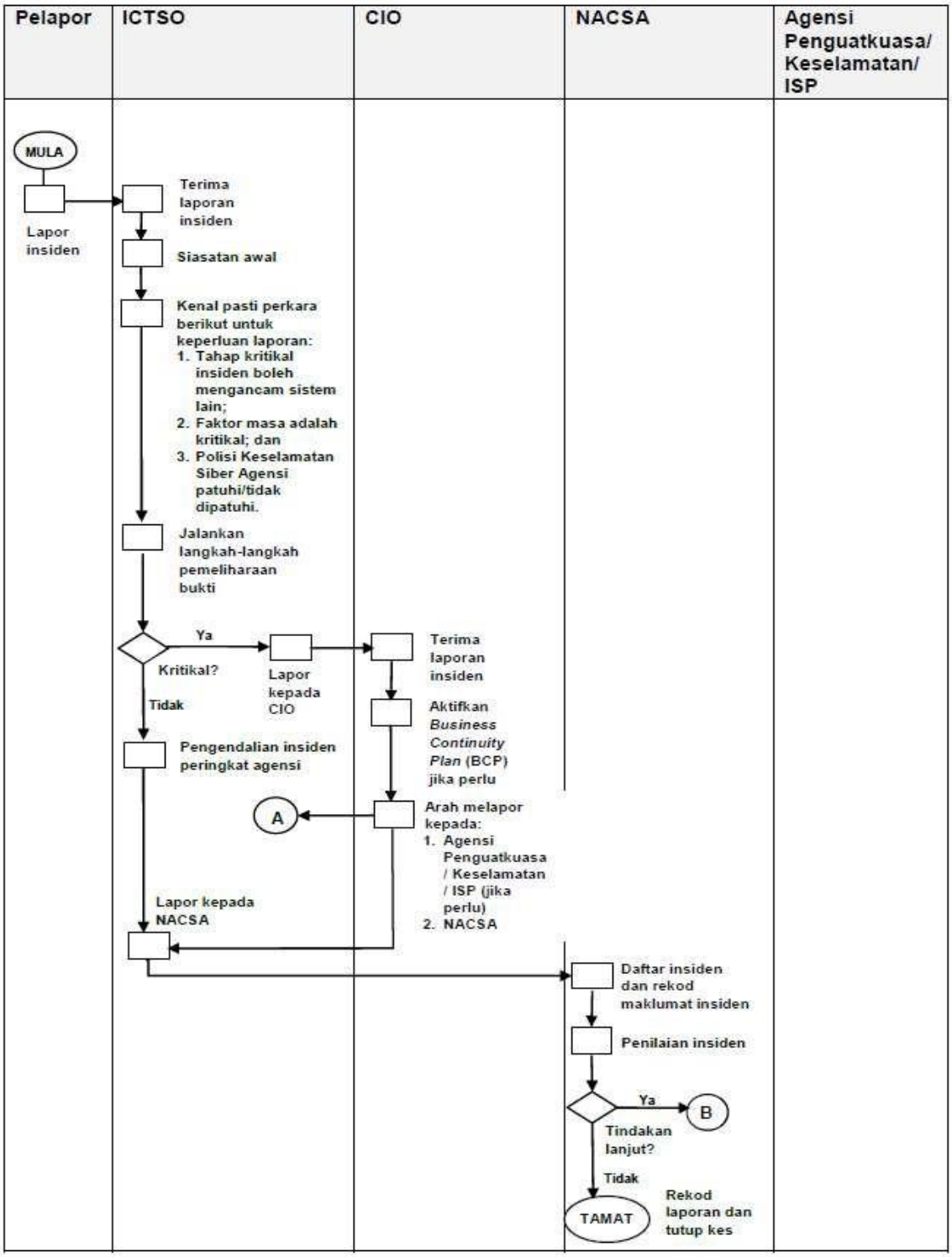
Pengesahan Pegawai Keselamatan ICT

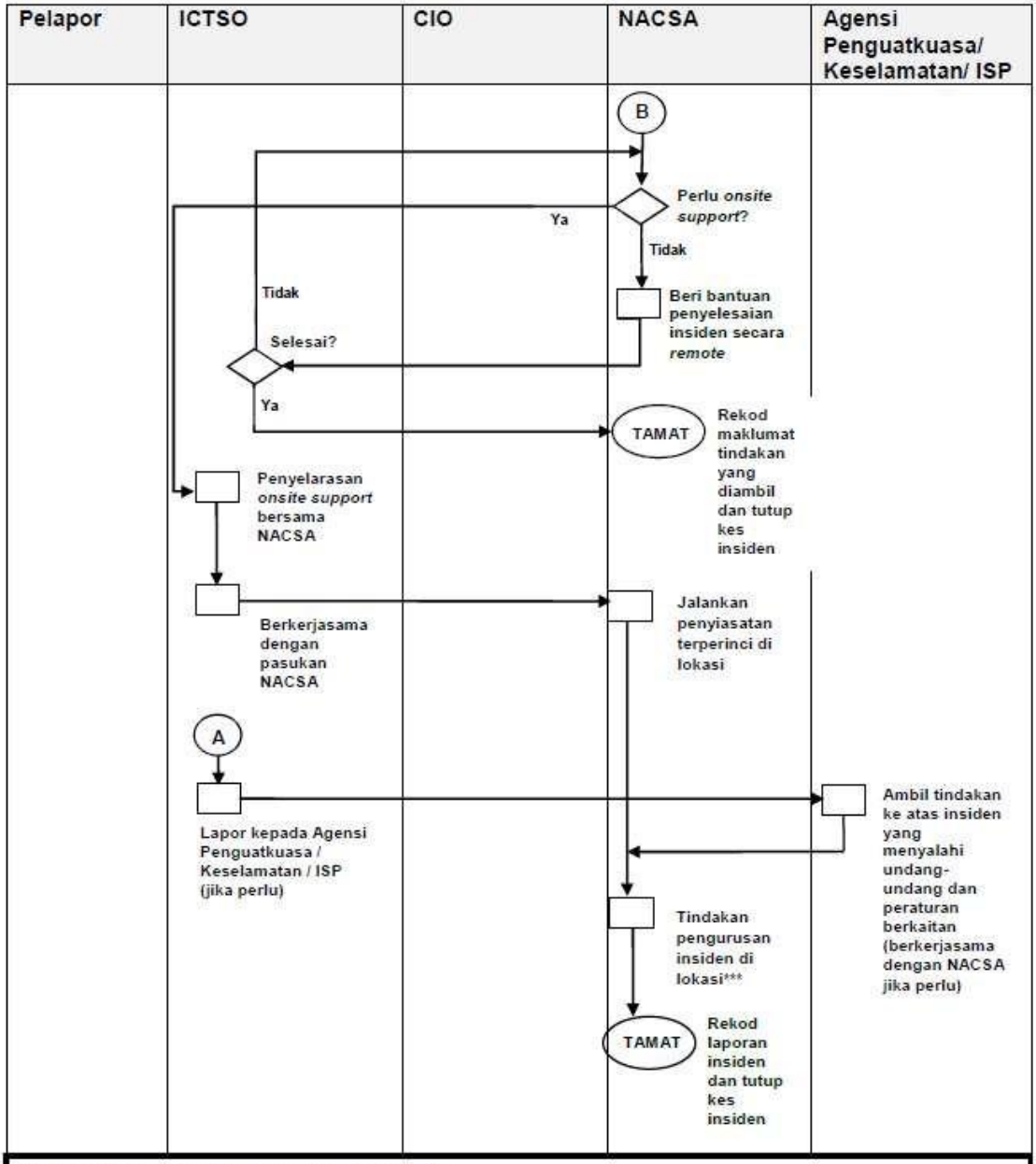
.....

( )
b.p Ketua Setiausaha
Kementerian Kerja Raya
Tarikh :

LAMPIRAN 2
Pindaan 1/2019

PROSES KERJA PELAPORAN INSIDEN KESELAMATAN ICT (CERT) KKR





*** Tindakan pengurusan insiden di lokasi:

1. Kawal kerosakan;
2. Baik pulih minima dengan segera;
3. Siasat insiden dengan terperinci;
4. Analisis impak (Business Impact Analysis);
5. Hasilkan laporan insiden;
6. Bentang dan kemukakan laporan kepada agensi; dan
7. Selaraskan tindakan di antara agensi dan Agensi Penguatkuasa/Keselamatan/ISP (jika berkenaan).

LAMPIRAN 3

SENARAI PERUNDANGAN DAN PERATURAN		
BIL.	**PERUNDANGAN DAN PERATURAN**	**RUJUKAN**
1.	Arahan Teknologi Maklumat 2007 bertarikh 19 Disember 2007	MAMPU
2.	Akta 680 – Akta Aktiviti Kerajaan Elektronik2007	MAMPU
3.	Garis Panduan IT *Outsourcing* 2006 bertarikhOktober 2006	MAMPU
4.	Garis Panduan Penggunaan ICT ke arah ICT Hijau dalam Perkhidmatan Awam 2010 bertarikh 3 Ogos 2010	MAMPU
5.	Malaysian Public Sector Management of Information and Communications Technology Security Handbook (MyMIS) 2002 bertarikh 15 Januari 2002	MAMPU
6.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 2 Tahun 2015 – Pengurusan Laman Web Agensi Sektor Awam bertarikh 30 September 2015.	MAMPU
7.	Pekeliling Am Bilangan 1 Tahun 2012 – Pemansuhan Keperluan Pengesahan Yang Tiada Nilai Tambah pada Borang Rasmi Kerajaan dan Salinan Dokumen Sokongan bertarikh 2 Mac 2012.	MAMPU
8.	Pekeliling Am Bilangan 2 Tahun 2002 – Penggunan dan Pemakaian *DataDictionary* Sektor Awam (DDSA) Sebagai Standard di Agensi-Agensi Kerajan bertarikh 2 September 2002.	MAMPU
9.	Pekeliling Am Bilangan 2 Tahun 2006 – Pengukuhan Tadbir Urus Jawatankuasa IT dan Internet Kerajaan bertarikh 13 November 2006.	MAMPU

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
10.	Pekeliling Am Bilangan 3 Tahun 2011 – Pemansuhan Keperluan Mengemukakan Laporan Yang tidak Merupakan Suatu Kehendak Undang-undang dalam Berurusan dengan Agensi Kerajaan bertarikh 29 September 2011.	MAMPU
11.	Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) bertarikh 4 April 2001.	MAMPU
12.	Pekeliling Am Bilangan 3 Tahun 2000 – Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan bertarikh 1 Oktober 2000.	MAMPU
13.	Pekeliling Am Bilangan 1 Tahun 2015 – Pelaksanaan Data Terbuka Sektor Awam bertarikh 30 September 2015.	MAMPU
14.	Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan bertarikh 28 November 2003.	MAMPU
15.	Risalah Penerapan Etika Penggunaan MediaSosial dalam Sektor Awam.	MAMPU
16.	Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan MelElektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007.	MAMPU
17.	Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007.	MAMPU
18.	Surat Arahan Ketua Pengarah MAMPU –Pengaktifan Fail Log Server bertarikh 23 Mac 2009.	MAMPU

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
19.	Surat Arahan Ketua Pengarah MAMPU – Panduan Penyediaan dan Penyiaran BeritaOnline di Laman Web Agensi-Agensi Kerajaanbertarikh 11 September 2009.	MAMPU
20.	Surat Arahan Ketua Pengarah MAMPU – Penggunaan Smartphone, Personel Digital Assistant dan Alat Komunikasi Mudah Alih Sebagai Saluran Komunikasi Tambahan bertarikh 15 September 2009.	MAMPU
21.	Surat Arahan Ketua Pengarah MAMPU – Penggunaan Media Jaringan Sosial di Sektor Awam bertarikh 19 November 2009.	MAMPU
22.	Surat Arahan Ketua Pengarah MAMPU – Garis Panduan Transisi IPv6 Sektor Awam yang bertarikh 4 Januari 2010.	MAMPU
23.	Surat Arahan Ketua Pengarah MAMPU – Pengurusan KesinambunganPerkhidmatanAgensi Sektor Awam yang bertarikh 22 Januari 2010.	MAMPU
24.	Surat Arahan Ketua Pengarah MAMPU – Panduan Pelaksanaan Pengurusan Projek ICT Sektor Awam yang bertarikh 5 Mac 2010.	MAMPU
25.	Surat Arahan Ketua Pengarah MAMPU – Pemantapan Penggunaan dan Pengurusan E-Mel di Agensi-Agensi Kerajaan yang bertarikh 1 Julai 2010.	MAMPU
26.	Surat Arahan Ketua Pengarah MAMPU – Pelaksanaan Pensijilan MS ISO/IEC 27001:2007 dalam Sektor Awam yang bertarikh 24 November 2010.	MAMPU

27.	Surat Arahan Ketua Pengarah MAMPU –Amalan Terbaik Penggunaan Media Jaringan Sosial di Sektor Awam bertarikh 8 April 2011.	MAMPU

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
28.	Surat Arahan Ketua Pengarah MAMPU –Pelaksanaan dan Penggunaan Aplikasi Digital Document Management System (DDMS) Sektor Awam bertarikh 26 Januari 2015.	MAMPU
29.	Surat Arahan Ketua Pengarah MAMPU – Pelaksanaan Rasionalisasi Laman Web bertarikh 26 Mei 2015.	MAMPU
30.	Surat Arahan Ketua Pengarah MAMPU – Pelaksanaan Penilaian Risiko Keselamatan Maklumat Menggunakan MyRAM App. 2.0 di Agensi Sektor Awam bertarikh 12 Ogos 2015.	MAMPU
31.	Surat Pekeliling Am Bilangan 2 Tahun 2000 – Peranan Jawatankuasa- Jawatankuasa di bawah Jawatankuasa IT dan Internet Kerajaan (JITIK) bertarikh 20 Disember 2000.	MAMPU
32.	Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko KeselamatanMaklumat Sektor Awam bertarikh 7 November 2005.	MAMPU
33.	Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam bertarikh 9 November 2006.	MAMPU
34.	Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009.	MAMPU
35.	Surat Pekeliling Am Bilangan 3 Tahun 2015 – Garis Panduan Permohonan Kelulusan Teknikal dan Pemantauan Projek Teknologi Maklumat dan Komunikasi (ICT) Agensi Sektor Awam yang bertarikh 11 November 2015.	MAMPU

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
36.	Pekeliling Am Bilangan 2 Tahun 2012 – Tatacara Pengurusan Aset Tak Alih Kerajaan bertarikh 21 Jun 2012.	JPM
37.	Pekeliling Am Bilangan 3 Tahun 2012 – SistemKod Aset Tak Alih bertarikh 21 Jun 2012.	JPM
38.	Pekeliling Am Bil. 1 Tahun 2009 – Manual Pengurusan Aset Menyeluruh Kerajaanbertarikh 27 Mac 2009.	JPM
39.	Surat Arahan Ketua Setiausaha Negara – Langkah-Langkah untuk Memperkukuhjan Keselamatan Rangkaian Setempat Tanpa Wayar (Wireless Local Area Network) di Agensi-agensi Kerajaan yang bertarikh Oktober 2006.	JPM
40.	Surat Arahan Ketua Setiausaha Negara – Langkah-Langkah Keselamatan Perlindungan untuk Larangan Penggunaan Telefon Bimbit atau Lain-Lain Peralatan Komunikasi di Agensi- Agensi Kerajaan bertarikh 31 Januari 2007.	JPM
41.	Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 – Panduan Pengurusan Pejabat bertarikh 30 April2007	JPA
42.	Garis Panduan Keselamatan KKR	KKR
43.	Standard Operating Procedure (SOP) ICT KKR	KKR
44.	Akta 588 – Akta Komunikasi dan Multimedia1998 bertarikh 15 Oktober 1998	SKMM
45.	Akta 589 – Akta Suruhanjaya Komunikasi dan Multimedia 1998 bertarikh 15 Oktober 1998	SKMM
46.	Akta A563 – Akta Jenayah Komputer 1997bertarikh 30 Jun 1997	Jabatan Peguam Negara
47.	Akta 562 – Akta Tandatangan Digital 1997bertarikh 30 Jun 1997	Jabatan Peguam Negara
48.	1 Pekeliling Perbendaharaan	Kementerian Kewangan Malaysia

BIL.	PERUNDANGAN DAN PERATURAN	RUJUKAN
49.	Pekeliling Perkhidmatan Bilangan 5 Tahun 2007 – Tatacara Pengurusan Aset Alih Kerajaanbertarikh 2 Mac 2007	Kementerian Kewangan Malaysia
50.	Akta 709 – Akta Perlindungan Data Peribadi 2010	Kementerian Komunikasi dan Multimedia Malaysia (Jabatan Perlindungan Data Peribadi)
51.	Akta 629 – Akta Arkib Negara 2003	Kementerian Pelancongan dan Kebudayaan Malaysia (Akib Negara Malaysia)
52.	Arahan Keselamatan Kerajaan	Pejabat Ketua Pegawai Keselamatan Kerajaan Malaysia
53.	Akta 332 – Akta Hak Cipta Tahun 1987	KPDNKK (Perbadanan Harta Intelek Malaysia)
54.	Akta 88 – Akta Rahsia Rasmi 1972	SPRM