KEMENTERIAN BELIA DAN SUKAN

SURAT PEKELILING KETUA SETIAUSAHA BILANGAN 1 TAHUN 2019

DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

(Versi 7.1)

KEMENTERIAN BELIA DAN SUKAN MALAYSIA

KEMENTERIAN BELIA DAN SUKAN
MALAYSIA

10 JANUARI 2019

Diedarkan Kepada:
Semua Pegawai dan Kakitangan
Kementerian Belia dan Sukan
serta Jabatan/Agensi di bawahnya

KETUA SETIAUSAHA
KEMENTERIAN BELIA DAN SUKAN MALAYSIA
Secretary General
Ministry of Youth and Sports Malaysia
Aras 15, Menara KBS
No. 27, Persiaran Perdana, Presint 4
Pusat Pentadbiran Kerajaan Persekutuan
62570 PUTRAJAYA

Tel : 603-8871 3017/3018
Faks : 603-8888 8719
Emel : lokmanhakim@kbs.gov.my

Rujukan Kami : KBS.100-1/6/1 Jld. 2(8)
Tarikh : 10 Januari 2019

Diedarkan Kepada:
Semua Pegawai dan Kakitangan
Kementerian Belia dan Sukan
serta Jabatan/Agensi di bawahnya

SURAT PEKELILING KETUA SETIAUSAHA BILANGAN 1 TAHUN 2019

DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

(Versi 7.1)

KEMENTERIAN BELIA DAN SUKAN MALAYSIA

TUJUAN

Pekeliling ini bertujuan untuk menjelaskan Dasar Keselamatan ICT KBS (DKICT) serta perkara-perkara berkaitan yang perlu diberi pertimbangan dan diambil tindakan oleh Ibu Pejabat Kementerian Belia dan Sukan, Jabatan Belia dan Sukan Negara, Jabatan Belia dan Sukan Negeri, Pejabat Belia dan Sukan Daerah, Kompleks Belia dan Sukan, Kompleks Rakan Muda, Akademi Pembangunan Belia Malaysia, Pejabat Pesuruhjaya Sukan, Pejabat Pendaftar Pertubuhan Belia Malaysia, Institut Kemahiran Belia Negara dan Institut Penyelidikan Pembangunan Belia Malaysia (termasuk pegawai, kakitangan, pembekal, pakar runding dll.). DKICT KBS Versi 7.1 adalah seperti di Lampiran kepada pekeliling ini.

LATAR BELAKANG

2.1 Surat Pekeliling Am Bil Bilangan 3 tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Kerajaan" yang dikeluarkan oleh Jabatan Perdana Menteri telah memberikan garis panduan kepada semua agensi Kerajaan untuk merujuk dan mematuhi dasar keselamatan teknologi Maklumat dan komunikasi kerajaan.

2.2 Dasar Keselamatan ICT KBS Versi 1.0 telah dikeluarkan pada Mei 2006 dan dilaksanakan mengikut syarat yang ditetapkan dalam surat pekeliling KBS Bilangan 1 Tahun 2006. Dasar ini dikeluarkan bagi memenuhi keperluan penguatkuasaan, kawalan dan langkah-langkah yang menyeluruh untuk melindungi aset ICT Kerajaan. DKICT KBS mengandungi peraturan-peraturan yang **mesti dibaca**, **difahami** dan **dipatuhi** dalam penggunaan Aset Teknologi Maklumat dan Komunikasi (ICT) KBS.

2.3 **Dasar Keselamatan ICT KBS Versi 7.1** ialah dasar yang telah dikemas kini dan dilaksanakan mengikut garis Panduan yang telah ditetapkan dalam Dasar Keselamatan ICT Versi 5.3 yang telah dikeluarkan oleh pihak MAMPU pada 13 Mei 2010.

DASAR KESELAMATAN ICT KEMENTERIAN BELIA DAN SUKAN (VERSI 7.1)

3.1 DKICT KBS Versi 7.1 ini dirumuskan bagi memenuhi keperluan penguatkuasaan, kawalan dan langkah-langkah yang menyeluruh untuk melindungi aset ICT Kerajaan. Perlindungan keselamatan ini perlu bersesuaian dengan nilai atau sensitiviti aset yang dimaksudkan. Ia juga perlu seimbang dengan kesan yang mungkin timbul akibat kegagalan perlindungan yang sesuai. Pernyataan dasar, prinsip, objektif dan skop dasar ini dijelaskan dalam lampiran kepada Pekeliling ini.

3.2 DKICT KBS Versi 7.1 yang disediakan bersama-sama dengan Pekeliling ini meliputi:

Perkara 01 : Pembangunan Dan Penyelenggaraan Dasar
Perkara 02 : Organisasi Keselamatan
Perkara 03 : Pengurusan Aset
Perkara 04 : Keselamatan Sumber Manusia
Perkara 05 : Keselamatan Fizikal Dan Persekitaran
Perkara 06 : Pengurusan Operasi Dan Komunikasi
Perkara 07 : Kawalan Capaian
Perkara 08 : Perolehan, Pembangunan Dan Penyelenggaraan Sistem Aplikasi
Perkara 09 : Pengurusan Pengendalian Insiden Keselamatan
Perkara 10 : Pengurusan Kesinambungan Perkhidmatan
Perkara 11 : Pematuhan

TANGGUNGJAWAB BAHAGIAN/JABATAN/AGENSI

4.1 Semua Bahagian/Jabatan/Agensi di bawah KBS adalah dikehendaki mematuhi

DKICT KBS Versi 7.1 dan melaksanakan tanggungjawab yang ditetapkan. Sehubungan dengan itu, semua Ketua Jabatan adalah diminta mengambil tindakan-tindakan berikut:

4.1.1 memastikan semua infrastruktur keselamatan ICT menepati prinsip-prinsip keselamatan berpandukan DKICT KBS Versi 7.1 dan Arahan Keselamatan yang disediakan oleh Ketua Pegawai Keselamatan Kerajaan.

4.1.2 menyedia dan mengkaji semula dokumen infrastruktur keselamatan ICT bagi tujuan audit keselamatan ICT.

4.1.3 mengenal pasti bidang-bidang keselamatan ICT yang perlu diberi perhatian rapi dan mengambil tindakan segera mengatasinya.

4.1.4 memastikan tahap keselamatan ICT terjamin setiap masa.

4.1.5 memastikan semua pegawai dan kakitangan membaca, memahami dan akur akan peruntukan-peruntukan yang terkandung di dalam DKICT KBS Versi 7.1 dan seterusnya menandatangani Surat Akuan Pematuhan DKICT KBS.

PEMATUHAN

5.1 Pematuhan merupakan prinsip penting dalam menghindar dan mengesan sebarang pelanggaran Dasar. Semua pengguna KBS tertakluk kepada pematuhan DKICT KBS Versi 7.1.

PEMAKAIAN

6.1 Pemakaian Pekeliling ini adalah meliputi semua warga KBS di Ibu Pejabat Kementerian Belia dan Sukan, Jabatan Belia dan Sukan Negara, Jabatan Belia dan Sukan Negeri, Pejabat Belia dan Sukan Daerah, Kompleks Belia dan Sukan, Kompleks Rakan Muda, Akademi Pembangunan Belia Malaysia, Pejabat Pesuruhjaya Sukan, Pejabat Pendaftar Pertubuhan Belia Malaysia, Institut Latihan Kemahiran Belia dan Sukan dan Institut Penyelidikan Pembangunan Belia Malaysia (termasuk pegawai, kakitangan, pembekal, pakar runding dll.).

TARIKH KUAT KUASA

7.1 Pekeliling ini berkuat kuasa mulai 10 Januari 2019.

PEMBATALAN

8.1 Dengan berkuat kuasanya Surat Pekeliling KBS ini, maka Surat Pekeliling KBS Bil 2 Tahun 2017 – Dasar Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Versi 7.0 Kementerian Belia dan Sukan adalah dibatalkan.

" BERKHIDMAT UNTUK NEGARA "

Saya yang menjalankan amanah,

(DATO' LOKMAN HAKIM BIN ALI)

10 Januari 2019

Kementerian Belia dan Sukan

DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

(Lampiran kepada
Surat Pekeliling Dasar Keselamatan ICT KBS)

VERSI 7.1

10 Januari 2019

Muka Surat

PENGENALAN

1.0 PENGENALAN

Dasar Keselamatan ICT KBS mengandungi peraturan-peraturan yang **mesti dibaca**, **difahami** dan **dipatuhi** dalam penggunaan Aset Teknologi Maklumat dan Komunikasi (ICT) KBS. Tujuan utama dasar ini ialah untuk menerangkan kepada semua pengguna ICT KBS di Ibu Pejabat Kementerian Belia dan Sukan, Jabatan Belia dan Sukan Negara, Jabatan Belia dan Sukan Negeri, Pejabat Belia dan Sukan Daerah, Kompleks Belia dan Sukan, Kompleks Rakan Muda, Akademi Pembangunan Belia Malaysia, Pejabat Pesuruhjaya Sukan, Pejabat Pendaftar Pertubuhan Belia Malaysia, Institut Latihan Kemahiran Belia dan Sukan (ILKBS) dan Institut Penyelidikan Pembangunan Belia Malaysia (termasuk pegawai, kakitangan, pembekal, pakar runding dll.) mengenai tanggungjawab dan peranan mereka dalam melindungi Aset ICT KBS.

2.0 OBJEKTIF

Dasar Keselamatan ICT KBS diwujudkan untuk menjamin kesinambungan urusan KBS dengan meminimumkan kesan insiden keselamatan ICT.

Dasar ini juga bertujuan untuk memudahkan perkongsian maklumat sesuai dengan keperluan operasi KBS. Ini hanya boleh dicapai dengan memastikan semua aset ICT dilindungi.

Manakala, objektif utama Keselamatan ICT KBS ialah seperti berikut:

(a) Memastikan kelancaran operasi KBS dan meminimumkan kerosakan atau kemusnahan;

(b) Melindungi kepentingan pihak-pihak yang bergantung kepada sistem maklumat daripada kesan kegagalan atau kelemahan dari segi kerahsiaan, integriti, kebolehsediaan, kesahihan maklumat dan komunikasi; dan

(c) Mencegah salah guna atau kecurian aset ICT Kerajaan.

3.0 PERNYATAAN DASAR

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

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

(a) Melindungi maklumat rahsia rasmi dan maklumat rasmi kerajaan dari capaian tanpa kuasa yang sah;

(b) Menjamin setiap maklumat adalah tepat dan sempurna;

(c) Memastikan ketersediaan maklumat apabila diperlukan oleh pengguna ICT KBS; dan

(d) Memastikan akses kepada hanya pengguna-pengguna ICT KBS yang sah atau penerimaan maklumat daripada sumber yang sah.

Dasar Keselamatan ICT KBS merangkumi perlindungan ke atas semua bentuk maklumat bertujuan untuk menjamin keselamatan maklumat tersebut dan kebolehsediaan kepada semua pengguna yang dibenarkan. Ciri-ciri utama keselamatan maklumat adalah seperti berikut:

(a) Kerahsiaan - Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran;

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

(c) Tidak Boleh Disangkal - Punca data dan maklumat hendaklah daripada punca

yang sah dan tidak boleh disangkal;

(d) Kesahihan - Data dan maklumat hendaklah dijamin kesahihannya; dan

(e) Ketersediaan - Data dan maklumat hendaklah boleh diakses pada bila-bila masa.

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

4.0 SKOP

Aset ICT KBS terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT KBS menetapkan keperluan-keperluan asas berikut:

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

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

Bagi menentukan Aset ICT ini terjamin keselamatannya sepanjang masa, Dasar Keselamatan ICT KBS ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnahkan, disimpan, dijana, dicetak, diakses, diedarkan, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

(a) Perkakasan

Semua aset yang digunakan untuk menyokong pemprosesan maklumat dan kemudahan storan KBS. Contoh komputer, pelayan, peralatan komunikasi dan sebagainya;

(b) Perisian

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

(c) Perkhidmatan

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

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

ii. Sistem halangan akses seperti sistem kad akses; dan

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

(d) Data atau Maklumat

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

(e) Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian KBS bagi mencapai misi dan objektif agensi. Individu berkenaan merupakan aset berdasarkan kepada tugas-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 adalah dianggap sebagai perlanggaran langkah-langkah keselamatan.

5.0 PRINSIP-PRINSIP

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT KBS adalah seperti berikut:

(i) **Capaian/Akses Atas Dasar "Perlu Mengetahui"**

Akses terhadap penggunaan Aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna ICT KBS tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna akses hanya akan diberikan sekiranya peranan atau fungsi pengguna ICT KBS memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti mana yang dinyatakan di dalam dokumen "Arahan Keselamatan" perenggan 53, muka surat 15;

(ii) Hak Akses Minimum

Hak akses kepada pengguna ICT KBS hanya diberi pada tahap set yang paling minimum iaitu untuk membaca dan/atau melihat sahaja. Kelulusan khas adalah diperlukan untuk membolehkan pengguna ICT KBS mewujud, menyimpan, mengemas kini, mengubah atau membatalkan sesuatu data atau maklumat. Hak akses adalah

dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna ICT KBS/bidang tugas;

(iii) Akauntabiliti

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

Akauntabiliti atau tanggungjawab pengguna ICT KBS termasuklah:

a. Menghalang pendedahan maklumat kepada pihak yang tidak berkenaan;

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

c. Menentukan maklumat sedia untuk digunakan;

d. Menjaga kerahsiaan kata laluan;

e. Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;

f. Memberi perhatian kepada maklumat terperingkat terutamanya semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan

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

(iv) Pengasingan

Tugas mewujud, memadam, kemas kini, mengubah dan mengesahkan data perlu diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi Aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau di manipulasi. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian;

(v) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, Aset ICT

seperti komputer, pelayan (*server*), *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

(vi) **Pematuhan**

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

(vii) **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 (*backup*) dan mewujudkan Pelan Pemulihan Bencana/Kesinambungan Perkhidmatan; dan

(viii) **Saling Bergantungan**

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

6.0 PENILAIAN RISIKO KESELAMATAN ICT

KBS hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu KBS perlu mengambil langkah-langkah proaktif dan bersesuaian untuk menilai tahap risiko aset ICT supaya pendekatan dan keputusan yang paling berkesan dikenal pasti bagi menyediakan perlindungan dan kawalan ke atas aset ICT.

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

Penilaian risiko keselamatan ICT hendaklah dilaksanakan ke atas sistem maklumat KBS termasuklah aplikasi, perisian, pelayan, rangkaian dan/atau proses serta prosedur. Penilaian risiko ini hendaklah juga dilaksanakan di premis yang menempatkan sumber-sumber teknologi

maklumat termasuklah pusat data, bilik media storan, kemudahan utiliti dan sistem-sistem sokongan lain.

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

KBS perlu mengenal pasti tindakan yang sewajarnya bagi menghadapi kemungkinan risiko berlaku dengan memilih tindakan berikut:

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

Bidang 1

PEMBANGUNAN DAN PENYELENGGARAAN DASAR

BIDANG 01		
PEMBANGUNAN DAN PENYELENGGARAAN DASAR		
0101	**Dasar Keselamatan ICT**	
Objektif:	Menerangkan hala tuju dan sokongan pengurusan KBS terhadap keselamatan selaras dengan keperluan KBS dan perundangan yang berkaitan.	
010101	**Pelaksanaan Dasar**	**Tindakan**
	Pelaksanaan dasar ini akan dijalankan oleh Ketua Setiausaha KBS (KSU) dibantu oleh Jawatankuasa Pemandu ICT (JPICT) yang terdiri daripada ahli-ahli seperti di Lampiran 1.	Ketua Setiausaha KBS
010102	**Penyebaran Dasar**	**Tindakan**
	Dasar ini perlu disebarkan kepada semua pengguna ICT KBS.	ICTSO
010103	**Penyelenggaraan Dasar**	**Tindakan**
	Dasar Keselamatan ICT KBS adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan dan kepentingan sosial. Berikut adalah prosedur yang berhubung dengan penyelenggaraan Dasar Keselamatan ICT KBS: a. Kenal pasti dan tentukan perubahan yang diperlukan; b. Mengemukakan cadangan pindaan secara bertulis kepada ICTSO untuk pembentangan dan persetujuan Mesyuarat Jawatankuasa Pemandu ICT (JPICT); c. Perubahan yang telah dipersetujui oleh JPICT dimaklumkan kepada semua pengguna ICT KBS; dan d. Dasar ini hendaklah dikaji semula mengikut keperluan semasa.	ICTSO
010104	**Pengecualian Dasar**	**Tindakan**
	Dasar Keselamatan ICT KBS adalah terpakai kepada semua pengguna ICT KBS dan tiada pengecualian diberikan.	Pengguna ICT KBS

Bidang 2

ORGANISASI KESELAMATAN

BIDANG 02		
ORGANISASI KESELAMATAN		
0201	**Infrastruktur Organisasi Dalaman**	
Objektif:	Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT KBS.	
020101	**Ketua Setiausaha**	**Tindakan**
	Peranan dan tanggungjawab Ketua Setiausaha adalah seperti berikut: a. Memastikan semua pengguna ICT KBS memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT KBS; b. Memastikan semua pengguna ICT KBS mematuhi Dasar Keselamatan ICT KBS; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT KBS; dan e. Mempengerusikan mesyuarat Jawatankuasa Pemandu ICT (JPICT), KBS.	KSU
020102	**Ketua Pegawai Maklumat (CIO)**	**Tindakan**
	Timbalan Ketua Setiausaha (Pengurusan (TKSU(P))) KBS ialah Ketua Pegawai Maklumat (CIO) KBS. Peranan dan tanggungjawab CIO KBS adalah seperti berikut: a. Membantu Ketua Setiausaha dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; b. Menentukan keperluan keselamatan ICT; c. Menyelaras dan mengurus pelan latihan dan keselamatan ICT seperti penyediaan DKICT KBS serta pengurusan risiko dan pengauditan; dan d. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT KBS. e. CIO bertanggungjawab ke atas perancangan, pengurusan, penyelarasan dan pemantauan program ICT di KBS	CIO

020103	Pengurus ICT	Tindakan
	Setiausaha Bahagian Pengurusan Maklumat ialah Pengurus ICT KBS dan juga Pengarah CERT KBS. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: a. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan KBS; b. Menentukan kawalan akses pengguna ICT KBS terhadap Aset ICT KBS; c. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KBS; d. Memastikan semua kakitangan, perunding, kontraktor dan pembekal yang terlibat dengan BPM mematuhi dasar, piawaian dan garis panduan keselamatan ICT; e. Mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan *backup* dan persekitaran pejabat yang perlu, dengan persetujuan CIO KBS; f. Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam KBS dan agensi berkaitan yang mematuhi keperluan DKICT KBS; dan g. Membangun, mengkaji semula dan mengemas kini pelan kontingensi keselamatan ICT di KBS.	SUB (PM)
020104	**Pegawai Keselamatan ICT (ICTSO)**	**Tindakan**
	Ketua Penolong Setiausaha (Pengurusan Maklumat) Cawangan Operasi (KPSU(PM)O) ialah ICTSO KBS dan Pengurus CERT KBS. Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Mengurus keseluruhan program-program keselamatan ICT KBS; b. Menguatkuasakan pelaksanaan Dasar Keselamatan ICT KBS; c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT KBS kepada semua pengguna ICT KBS; d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT KBS; e. Menjalankan pengurusan risiko berkaitan ICT;	ICTSO

	f. Menjalankan audit, mengkaji semula, merumus tindak balas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan mengenainya; g. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; h. Melaporkan insiden keselamatan ICT kepada CERT KBS untuk tindakan penyiasatan atau pemulihan serta melaporkan kepada pihak yang bertanggungjawab ke atas pengendalian insiden keselamatan sektor awam dan memaklumkan kepada CIO jika keadaan memerlukan; i. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera; j. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT; dan k. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	
020105	**Pentadbir Sistem Aplikasi**	**Tindakan**
	Ketua Penolong Setiausaha (Pengurusan Maklumat) Cawangan Pembangunan (KPSU(PM)P) ialah Pentadbir Sistem Aplikasi. Peranan dan tanggungjawab Pentadbir Sistem Aplikasi adalah seperti berikut: a. Memastikan ketepatan dan kawalan capaian pengguna ICT KBS berdasarkan kepada Dasar Keselamatan ICT KBS; b. Mengambil tindakan segera dan bersesuaian apabila dimaklumkan terdapat pegawai yang telah tamat perkhidmatan, bertukar, berkursus panjang atau berlaku perubahan dalam bidang tugas; c. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT KBS; d. Memantau aktiviti capaian harian sistem aplikasi; dan e. Memantau penggunaan Sistem Aplikasi dan melaporkan kepada ICTSO sekiranya berlaku insiden keselamatan ICT.	KPSU(PM)P

020106	Pentadbir Operasi ICT	Tindakan
	Ketua Penolong Setiausaha (Pengurusan Maklumat) Cawangan Operasi (KPSU(PM)O) di Bahagian Pengurusan Maklumat ialah Pentadbir Operasi ICT KBS. Peranan dan tanggungjawab Pentadbir Operasi ICT KBS adalah seperti berikut: a. Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti atau berlaku perubahan dalam bidang tugas; b. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam Dasar Keselamatan ICT KBS; c. Memantau aktiviti capaian harian pengguna ICT KBS; d. Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; e. Melaksanakan penilaian tahap risiko secara berkala terhadap sistem aplikasi dan infrastruktur ICT ; f. Menganalisis dan menyimpan rekod jejak audit; g. Menyediakan laporan mengenai aktiviti capaian kepada pemilik maklumat berkenaan secara berkala; h. Memastikan rangkaian setempat (LAN) dan rangkaian luas (WAN) di KBS dan agensi berkaitan beroperasi sepanjang masa; i. Memastikan semua peralatan dan perisian rangkaian diselenggarakan dengan sempurna; j. Melaksana peningkatan infrastruktur, ciri-ciri keselamatan dan prestasi rangkaian sedia ada; k. Mengesan dan mengambil tindakan pembaikan segera ke atas rangkaian yang tidak stabil; l. Memantau penggunaan rangkaian dan melaporkan kepada Pengurus ICT sekiranya berlaku penyalahgunaan sumber rangkaian; m. Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian KBS secara tidak sah seperti melalui peralatan modem *wireless* dan *dial-up*;	KPSU(PM)O

	n. Menyediakan zon khas rangkaian untuk tujuan pengujian peralatan dan perisian rangkaian; o. Melaksanakan instalasi, konfigurasi dan penambahbaikan *server* serta perisian lain yang berkaitan dengan *server*; p. Melaksanakan proses *backup* dan pemulihan ke atas Sistem Aplikasi, Sistem Pengoperasian server, Pangkalan Data dan lain-lain yang berkaitan; q. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna ICT KBS seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; r. Memastikan ketepatan dan kawalan capaian pengguna ICT KBS; s. Melaksanakan pengurusan Pusat Data KBS; dan t. Melaporkan sebarang insiden keselamatan ICT kepada Pengurus ICT dan CIO.	
020107	**Pentadbir Pangkalan Data**	**Tindakan**
	Penolong Setiausaha (Pengurusan Maklumat) Unit Sistem Aplikasi Kementerian (PSU(PM)K) dan Penolong Setiausaha (Pengurusan Maklumat) Unit Sistem Aplikasi Jabatan (PSUK(PM)J) ialah Pentadbir Pangkalan Data. Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut: a. Melaksanakan konfigurasi dan penambahbaikan pangkalan data serta perisian lain yang berkaitan dengan pangkalan data; b. Memastikan pangkalan data boleh digunakan pada setiap masa; c. Melaksanakan pemantauan dan penyenggaraan yang berterusan ke atas pangkalan data; d. Memastikan aktiviti pentadbiran pangkalan data seperti prestasi capaian, penyelesaian masalah pangkalan data dan proses pengemaskinian data dilaksanakan dengan teratur; e. Melaksanakan polisi pengguna ICT KBS pangkalan data berdasarkan kepada prinsip-prinsip DKICT KBS; f. Melaksanakan proses *housekeeping* di pangkalan data; dan g. Melaporkan sebarang insiden keselamatan ICT kepada ICTSO.	PSU(PM)K dan PSUK(PM)J

020108	Pengguna ICT KBS	Tindakan
	Semua pengguna ICT KBS di Ibu Pejabat Kementerian Belia dan Sukan, Jabatan Belia dan Sukan Negara, Jabatan Belia dan Sukan Negeri, Pejabat Belia dan Sukan Daerah, Kompleks Belia dan Sukan, Kompleks Rakan Muda, Akademi Pembangunan Belia Malaysia, Pejabat Pesuruhjaya Sukan, Pejabat Pendaftar Pertubuhan Belia Malaysia, Institut Latihan Kemahiran Belia dan Sukan (ILKBS) dan Institut Penyelidikan Pembangunan Belia Malaysia (termasuk pegawai, kakitangan, pembekal, pakar runding dll.) ialah pengguna ICT KBS. Peranan dan tanggungjawab pengguna ICT KBS adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KBS; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat KBS; d. Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera; e. Menghadiri program-program kesedaran mengenai keselamatan ICT; dan f. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT KBS. (Lampiran 2)	Pengguna ICT KBS
020109	**Jawatankuasa Pemandu ICT (JPICT)**	**Tindakan**
	Keanggotaan Jawatankuasa Pemandu ICT (JPICT) KBS adalah seperti di Lampiran 1. Bidang kuasa: a. Memperakukan/meluluskan dokumen DKICT KBS; b. Memantau tahap pematuhan keselamatan ICT; c. Menilai aspek teknikal keselamatan projek-projek ICT; d. Memperakui garis panduan, prosedur dan tatacara untuk aplikasi khusus dalam KBS yang mematuhi keperluan DKICT KBS; e. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; f. Memastikan DKICT KBS selaras dengan dasar-dasar ICT kerajaan semasa;	JPICT

	g. Menerima laporan dan membincang mengenai keselamatan ICT semasa; h. Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden; dan i. Membincang tindakan yang melibatkan pelanggaran DKICT KBS.	
020110	**Pasukan Tindak Balas Insiden Keselamatan ICT KBS (CERT KBS)**	**Tindakan**
	Keanggotaan CERT KBS adalah seperti di Lampiran 3. Peranan dan tanggungjawab CERT KBS adalah seperti berikut: a. Menerima dan mengesan aduan keselamatan ICT serta menilai tahap dan jenis insiden; b. Merekodkan dan menjalankan siasatan awal insiden yang diterima; c. Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih; d. Menghubungi dan melaporkan insiden yang berlaku kepada pihak yang bertanggungjawab ke atas pengendalian insiden keselamatan sektor awam sama ada sebagai input atau untuk tindakan seterusnya; e. Menasihati agensi-agensi di bawah kawalannya mengambil tindakan pemulihan dan pengukuhan; f. Menyebarkan makluman berkaitan pengukuhan keselamatan ICT kepada pengguna ICT KBS; dan g. Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkat tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	CERT KBS
0202	**Pihak Ketiga**	
Objektif:	Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).	
020201	**Keperluan Keselamatan Kontrak dengan Pihak Ketiga**	**Tindakan**
	Ini bertujuan memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak ketiga dikawal. Perkara yang perlu dipatuhi termasuk yang berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT KBS;	CIO, Pengurus ICT dan ICTSO

	b. Mengenal pasti risiko keselamatan maklumat dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian; c. Mengenal pasti keperluan keselamatan sebelum memberi kebenaran capaian atau penggunaan kepada pihak ketiga; d. Akses kepada aset ICT KBS perlu berlandaskan kepada perjanjian kontrak; e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT KBS; ii. Perakuan Akta Rahsia Rasmi 1972; dan iii. Hak Harta Intelek. f. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT KBS. (Lampiran 2)	

Bidang 3

PENGURUSAN ASET

BIDANG 03		
PENGURUSAN ASET		
0301	**Akauntabiliti Aset**	
Objektif:	Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT KBS.	
030101	**Inventori Aset ICT**	**Tindakan**
	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 yang dikenal pasti dan maklumat aset direkodkan dalam borang daftar harta modal dan inventori sentiasa dikemas kini; b. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna ICT KBS yang dibenarkan sahaja; c. Memastikan semua pengguna ICT KBS mengesahkan penempatan aset ICT yang ditempatkan di KBS dan agensi berkaitan; d. Peraturan bagi pengendalian aset ICT hendaklah dikenal pasti, didokumenkan dan dilaksanakan; e. Setiap pengguna ICT KBS adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan f. Aset ICT adalah di bawah tanggungjawab Pegawai Aset KBS mengikut Pekeliling Perbendaharaan semasa yang berkuat kuasa.	Pegawai Aset KBS, Pentadbir Operasi ICT dan Pengguna ICT KBS
0302	**Pengelasan dan Pengendalian Maklumat**	
Objektif:	Memastikan setiap maklumat atau aset ICT diberikan tahap perlindungan yang bersesuaian.	
030201	**Pengelasan Maklumat**	**Tindakan**
	Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	Pengguna ICT KBS

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

Bidang 4

KESELAMATAN SUMBER MANUSIA

BIDANG 04		
KESELAMATAN SUMBER MANUSIA		
0401	**Keselamatan Sumber Manusia Dalam Tugas Harian**	
Objektif:	Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan KBS, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna ICT KBS hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.	
040101	**Sebelum Perkhidmatan**	**Tindakan**
	Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a. Menyatakan dengan lengkap dan jelas mengenai peranan dan tanggungjawab pegawai dan kakitangan KBS serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pengguna ICT KBS lantikan tetap yang terlibat berdasarkan 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 perjanjian yang telah ditetapkan.	Pengguna ICT KBS
040102	**Dalam Perkhidmatan**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan pegawai dan kakitangan KBS serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh KBS; b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT KBS secara berterusan dalam melaksanakan tugas-tugas dan tanggungjawab mereka, dan sekiranya perlu diberi kepada pihak ketiga yang berkepentingan dari semasa ke semasa; c. Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan KBS serta pihak ketiga yang	Pengguna ICT KBS dan ICTSO

	berkepentingan sekiranya berlaku perlanggaran ke atas perundangan dan peraturan yang ditetapkan oleh KBS; dan d. Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul bagi menjamin kepentingan keselamatan ICT. Sekiranya terdapat keperluan kursus atau latihan, pengguna ICT KBS boleh merujuk kepada Bahagian Pengurusan Sumber Manusia, KBS.	
040103	**Bertukar Atau Tamat Perkhidmatan**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT dikembalikan kepada KBS mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; b. Memulangkan dan menghapuskan sebarang dokumen atau maklumat rasmi yang berkaitan dengan tugas atau tempat di mana ia ditugaskan; dan c. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan mengikut peraturan yang ditetapkan oleh KBS dan/atau terma perkhidmatan.	Pengguna ICT KBS, Pentadbir Operasi ICT dan Pentadbir Sistem Aplikasi dan Portal
0402	**Perlindungan Data Peribadi**	
Objektif:	Memastikan maklumat peribadi pegawai dan kakitangan KBS dilindungi.	
040201	**Maklumat Yang Boleh Dikenal Pasti Secara Peribadi**	**Tindakan**
	Maklumat yang boleh dikenal pasti secara peribadi adalah maklumat yang boleh digunakan bersama maklumat yang lain (jika ada) dan dapat mengenal pasti identiti, butiran perhubungan atau mengetahui lokasi individu. Di antara data peribadi yang dimaksudkan terhad seperti berikut :- (a) Nama Penuh (b) Alamat Tempat Tinggal (c) Alamat E-mel (d) No Kad Pengenalan (e) Alamat IP (f) No Pendaftaran Kereta (g) No Lesen Memandu (h) Wajah, Cap Jari atau Tanda Tangan (i) No Kad Kredit	Pengguna ICT KBS

(j) Tarikh Lahir

(k) Tempat Lahir

(l) No Telefon

(m) ID Pengguna

(n) Jantina

(o) Butiran Cukai

(p) Pendapatan Tahunan

(q) Bangsa

(r) Maklumat Kewangan

(s) Nama Pasangan

(t) Status Perkahwinan

(u) Pendidikan

(v) Jumlah Tanggungan

Perkara-perkara yang perlu dipatuhi termasuk yang berikut:-

(a) Tidak dibenarkan untuk mendedahkan data peribadi kepada pihak ketiga tanpa mendapat keizinan daripada pemilik data tersebut;

(b) Tidak dibenarkan untuk mendedahkan bidang kuasa atau keanggotaan pegawai dalam mana-mana jawatan kuasa kepada pihak ketiga;

(c) Anggota yang bertanggungjawab terhadap kerahsiaan data peribadi pegawai hendaklah memastikan bahawa ianya diklasifikasikan sebagai sulit dan dijaga mengikut piawaian keselamatan yang tertinggi;

(d) Dalam mengekalkan keselamatan data peribadi, sistem kawalan yang mencukupi dengan gabungan kawalan akses fizikal dan elektronik, teknologi “firewall” dan langkah-langkah keselamatan lain yang munasabah hendaklah diambil untuk melindungi kerahsiaan dan keselamatan data peribadi;

(e) akses kepada data peribadi oleh anggota Jabatan adalah berasaskan dasar perlu-tahu sahaja; dan

Sebarang keperluan untuk mendedahkan data peribadi adalah atas dasar mengutamakan kepentingan Negara dan dibenarkan di bawah mana-mana undang-undang sahaja.

Bidang 5

KESELAMATAN FIZIKAL DAN PERSEKITARAN

BIDANG 05		
KESELAMATAN FIZIKAL DAN PERSEKITARAN		
0501	**Keselamatan Kawasan**	
Objektif:	Melindungi premis, perkakasan, perisian dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
050101	**Kawalan Kawasan**	**Tindakan**
	Ini bertujuan untuk 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, pengawal keselamatan) untuk melindungi kawasan yang mengandungi maklumat dan kemudahan pemprosesan maklumat; c. Memasang alat penggera atau kamera litar tertutup (*cctv*); d. Mengehadkan jalan keluar masuk; e. Mengadakan kaunter kawalan; f. Menyediakan tempat atau bilik khas untuk pelawat-pelawat; g. Mewujudkan perkhidmatan kawalan keselamatan; h. Melindungi kawasan terhad melalui kawalan pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; i. Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat bilik dan kemudahan; j. Mereka bentuk dan melaksanakan perlindungan fizikal dari kebakaran, banjir, letupan, kacau-bilau dan bencana; k. Menyediakan garis panduan untuk kakitangan yang bekerja di dalam kawasan terhad; dan	Pejabat Ketua Pegawai Keselamatan Kerajaan, CIO, ICTSO dan Pentadbir Operasi ICT

	l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
050102	**Kawalan Masuk Fizikal**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Setiap pengguna ICT KBS hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Semua pas keselamatan hendaklah diserahkan balik kepada KBS apabila pengguna ICT KBS berhenti, bertukar keluar atau bersara; c. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di kaunter utama KBS dan hendaklah dikembalikan semula selepas tamat lawatan; dan d. Kehilangan pas mestilah dilaporkan dengan segera.	Pengguna ICT KBS dan Pelawat
050103	**Kawasan Larangan**	**Tindakan**
	Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di KBS adalah Pusat Data. a. Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang diberi kuasa dan dibenarkan sahaja; b. Pihak ketiga adalah dilarang sama sekali untuk memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa sehingga tugas di kawasan berkenaan selesai. c. Sumber data atau *server*, peralatan komunikasi dan storan perlu ditempatkan di pusat data, bilik server atau bilik khas yang mempunyai ciri-ciri keselamatan yang tinggi termasuk sistem pencegah kebakaran; d. Pemantauan dibuat menggunakan kamera litar tertutup (*cctv*) dan diperiksa secara berjadual; e. Butiran pegawai selain yang dibenarkan atau pihak ketiga yang keluar dan masuk ke kawasan larangan perlu direkodkan;	Pengguna ICT KBS

	f. Lokasi kawasan larangan hendaklah tidak berhampiran dengan kawasan pemunggahan dan laluan awam; dan g. Memperkukuhkan keselamatan perimeter.	
0502	**Keselamatan Peralatan**	
Objektif:	Melindungi peralatan ICT KBS daripada kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
050201	**Peralatan ICT**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna ICT KBS hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Pengguna ICT KBS bertanggungjawab sepenuhnya ke atas peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang pertukaran perkakasan dan konfigurasi yang telah ditetapkan; c. Pengguna ICT KBS dilarang sama sekali menambah, menanggalkan atau mengganti sebarang komponen peralatan ICT yang telah ditetapkan; d. Pengguna ICT KBS dilarang membuat pemasangan sebarang perisian tambahan tanpa kebenaran Pentadbir Operasi ICT; e. Pengguna ICT KBS adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; f. Pengguna ICT KBS mesti memastikan perisian *antivirus* di komputer peribadi mereka sentiasa aktif (*activated*) dan dikemas kini di samping melakukan imbasan ke atas media storan yang digunakan; g. Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; h. Semua peralatan sokongan ICT hendaklah dilindungi daripada kecurian kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; i. Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS) (jika perlu);	Pengguna ICT KBS

	j. Semua peralatan ICT hendaklah disimpan atau diletakkan di tempat yang teratur, bersih dan mempunyai ciri-ciri keselamatan. Peralatan rangkaian seperti *switches, router* dan lain-lain perlu diletakkan di dalam rak khas dan berkunci; k. Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan yang berhawa dingin dan mempunyai pengudaraan *(air ventilation)* yang sesuai; l. Peralatan ICT yang hendak dibawa keluar dari premis KBS, perlulah mendapat kelulusan Ketua Jabatan/Ketua Bahagian dan direkodkan bagi tujuan pemantauan; m. Peralatan ICT yang hilang hendaklah dilaporkan kepada Ketua Jabatan dengan segera; n. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa; o. Pengguna ICT KBS tidak dibenarkan mengubah lokasi komputer dari tempat asal ianya ditempatkan ke lokasi yang lain tanpa kebenaran Pentadbir Operasi ICT; p. Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Pentadbir Operasi ICT melalui Meja Bantuan (Helpdesk) untuk direkodkan dan diambil tindakan sewajarnya; q. Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan. Ini bagi menjamin peralatan tersebut sentiasa berkeadaan baik; r. Konfigurasi alamat IP tidak dibenarkan diubah daripada alamat IP yang asal; s. Kata laluan Pentadbir (*password administrator*) dilarang sama sekali diubah oleh pengguna ICT KBS selain daripada pentadbir yang dipertanggungjawabkan. t. Pengguna ICT KBS bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; u. Pengguna ICT KBS hendaklah memastikan semua perkakasan komputer, pencetak, pengimbas dan lain-lain perkakasan ICT dimatikan apabila meninggalkan pejabat; dan	

	v. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Pengurus ICT dan Ketua Jabatan/Bahagian.	
050202	**Media Storan**	**Tindakan**
	Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat antaranya seperti *floppy disk*, *optical disk*, *magnetic tape*, *flash drive*, *hard disk* dan sebagainya. Media-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 bersesuaian dengan kandungan maklumat; b. Akses untuk memasuki kawasan penyimpanan media storan hendaklah terhad kepada pengguna ICT KBS yang dibenarkan sahaja; c. Semua media storan perlu dikawal bagi mencegah daripada capaian yang tidak dibenarkan, kecurian dan kemusnahan; d. Semua media storan yang mengandungi data kritikal hendaklah disimpan di dalam peti keselamatan yang mempunyai ciri-ciri keselamatan termasuk tahan daripada dipecahkan, api, air dan medan magnet; e. Akses dan pergerakan media storan hendaklah direkodkan; f. Perkakasan *backup* hendaklah diletakkan di tempat yang terkawal; g. Mengadakan salinan atau penduaan (*backup*) pada media storan kedua bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; h. Semua media storan data yang hendak dilupuskan mestilah dihapuskan dengan teratur dan selamat; dan i. Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	Pengguna ICT KBS

050203	Media Tandatangan Digital	Tindakan
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna ICT KBS hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan,kerosakan, penyalahgunaan dan pengklonan; b. Media ini tidak boleh dipindah-milik atau dipinjamkan; dan c. Sebarang insiden kehilangan yang berlaku hendaklah dilaporkan dengan segera kepada ICTSO untuk tindakan seterusnya.	Pengguna ICT KBS
050204	**Media Perisian dan Aplikasi**	
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang berlesen atau diperakui sahaja dibenarkan bagi kegunaan KBS; b. Sistem aplikasi dalaman tidak dibenarkan didemontrasikan atau diagih kepada pihak lain kecuali dengan kebenaran pemilik sistem aplikasi; c. Lesen perisian (*registration code, serials key* dan *activation code* perlu disimpan berasingan daripada *media pemasangan seperti CDROM* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan d. *Source code* sesuatu sistem aplikasi hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan.	Pengguna ICT KBS
050205	**Penyelenggaraan Perkakasan**	**Tindakan**
	Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua perkakasan yang di selenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; b. Memastikan perkakasan hanya boleh diselenggarakan oleh pegawai atau pihak yang dibenarkan sahaja; c. Bertanggungjawab terhadap setiap perkakasan bagi penyelenggaraan perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan;	Pentadbir Operasi ICT

	d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; e. Memaklumkan pengguna ICT KBS sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan di Ibu Pejabat KBS mestilah mendapat kebenaran daripada Pengurus ICT. Manakala di JBS, ILKBS, APBM, PPS, PPPB dan IYRES perlu mendapat kebenaran ketua jabatan masing-masing.	
050206	**Peralatan Di Luar Premis**	**Tindakan**
	Peralatan yang dibawa keluar dari premis KBS adalah terdedah kepada pelbagai risiko. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Peralatan perlu dilindungi dan dikawal sepanjang masa; dan b. Penyimpanan atau penempatan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	Pengguna ICT KBS
050207	**Pelupusan Perkakasan**	**Tindakan**
	Pelupusan melibatkan semua perkakasan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh KBS dan ditempatkan di KBS. Perkakasan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KBS. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan perkakasan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan mengikut tatacara pelupusan semasa yang berkuat kuasa; b. Sekiranya maklumat perlu disimpan, maka pengguna ICT KBS bolehlah membuat penduaan; c. Perkakasan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat; d. Pegawai Aset hendaklah mengenal pasti sama ada perkakasan tertentu boleh dilupuskan atau sebaliknya;	Pegawai Aset dan Bahagian Pengurusan Maklumat, KBS

	e. Perkakasan yang hendak dilupuskan hendaklah disimpan di tempat yang telah dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan perkakasan tersebut; f. Pegawai aset bertanggungjawab merekodkan butir–butir pelupusan dan mengemas kini rekod pelupusan perkakasan ICT ke dalam sistem inventori; g. Pelupusan perkakasan ICT hendaklah dilakukan secara berpusat dan mengikut tatacara pelupusan semasa yang berkuat kuasa; dan h. Pengguna ICT KBS adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:- i. Menyimpan mana-mana perkakasan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggalkan dan menyimpan perkakasan tambahan dalaman CPU seperti RAM, *hardisk*, *motherboard* dan sebagainya; ii. Menyimpan dan memindahkan perkakasan luaran komputer seperti AVR, speaker dan mana-mana peralatan yang berkaitan ke mana-mana bahagian di KBS; iii. Memindah keluar dari KBS mana-mana perkakasan ICT yang hendak dilupuskan; iv. Melupuskan sendiri perkakasan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab KBS; dan v. Pengguna bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin ke media storan kedua seperti *floppy disk*, *optical disk*, *magnetic tape*, *flash drive*, *hard disk* dan lain-lain media storan sebelum menghapuskan maklumat tersebut daripada perkakasan komputer yang hendak dilupuskan.	
0503	**Keselamatan Persekitaran**	
Objektif:	Melindungi aset ICT KBS daripada sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301	**Kawalan Persekitaran**	**Tindakan**
	Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk	Pengguna ICT KBS

	terlebih dahulu kepada Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK). Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: a. Merancang dan menyediakan pelan keseluruhan susun atur pusat data, pejabat dan sebagainya dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna ICT KBS adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g. Semua peralatan perlindungan hendaklah disemak dan diuji secara berjadual. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan h. Akses kepada saluran *riser* hendaklah sentiasa dikunci.	
050302	**Bekalan Kuasa**	**Tindakan**
	Bekalan kuasa merupakan punca kuasa elektrik yang dibekalkan kepada peralatan ICT. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua peralatan ICT hendaklah dilindungi dari kegagalan bekalan elektrik dan bekalan yang sesuai hendaklah disalurkan kepada peralatan ICT; b. Peralatan sokongan seperti *Uninterruptable Power Supply* (UPS) dan penjana (*generator*) boleh digunakan bagi perkhidmatan kritikal seperti di Pusat Data supaya mendapat bekalan kuasa berterusan; dan	Pentadbir Operasi ICT dan ICTSO

	c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual atau mengikut keperluan semasa.	
050303	**Kabel**	**Tindakan**
	Kabel komputer hendaklah dilindungi kerana ia boleh menyebabkan maklumat menjadi terdedah. Langkah-langkah keselamatan yang perlu diambil adalah seperti berikut : a. Menggunakan kabel yang mengikut spesifikasi yang telah ditetapkan; b. Melindungi kabel daripada kerosakan yang disengajakan atau tidak disengajakan; c. Melindungi laluan pemasangan kabel sepenuhnya bagi mengelakkan ancaman kerosakan dan *wire tapping;* dan d. Semua kabel perlu dilabelkan dengan jelas dan mestilah melalui *trunking* bagi memastikan keselamatan kabel daripada kerosakan dan pintasan maklumat.	Pentadbir Operasi ICT dan ICTSO
050304	**Prosedur kecemasan**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pengguna ICT KBS hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan/Manual Keselamatan KBS; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan KBS/Jabatan yang dilantik mengikut aras.	Pengguna ICT KBS dan Pegawai Keselamatan KBS/ Jabatan
0504	**Keselamatan Dokumen**	
Objektif:	Melindungi maklumat KBS dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050401	**Dokumen**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Setiap dokumen hendaklah difailkan dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar;	Pengguna ICT KBS

	b. Pergerakan fail dan dokumen hendaklah direkodkan dan perlulah mengikut prosedur keselamatan; c. Kehilangan dan kerosakan ke atas semua jenis dokumen perlu dimaklumkan mengikut prosedur Arahan Keselamatan; d. Pelupusan dokumen hendaklah mengikut prosedur keselamatan semasa seperti mana Arahan Keselamatan, Arahan Amalan (Jadual Pelupusan Rekod) dan tatacara Jabatan Arkib Negara; dan e. Menggunakan enkripsi (*encryption*) ke atas dokumen rahsia rasmi yang disediakan dan dihantar secara elektronik.	

Bidang 6

PENGURUSAN OPERASI DAN KOMUNIKASI

BIDANG 06		
PENGURUSAN OPERASI DAN KOMUNIKASI		
0601	**Pengurusan Prosedur Operasi**	
Objektif:	Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
060101	**Pengendalian Prosedur**	**Tindakan**
	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.	Pengguna ICT KBS
060102	**Kawalan Perubahan**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengubahsuaian yang melibatkan perkakasan, sistem untuk pemprosesan maklumat, perisian, dan prosedur mestilah mendapat kebenaran daripada Pengurus ICT atau pemilik aset ICT mana yang berkenaan terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggarakan, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; c. Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkodkan dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Pengguna ICT KBS

060103	Pengasingan Tugas dan Tanggungjawab	Tindakan
	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 dimanipulasikan; dan c. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*.	Pengurus ICT dan ICTSO
0602	**Pengurusan Penyampaian Perkhidmatan Pihak Ketiga**	
Objektif:	Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
060201	**Perkhidmatan Penyampaian**	**Tindakan**
	Perkara-perkara yang mesti dipatuhi adalah seperti berikut: a. Memastikan kawalan keselamatan, definisi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; b. Perkhidmatan, laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan c. Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Pengguna ICT KBS
0603	**Perancangan dan Penerimaan Sistem**	
Objektif:	Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301	**Perancangan Kapasiti**	**Tindakan**
	Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang.	ICTSO, Pentadbir Sistem Aplikasi dan Portal ICT, Pentadbir Operasi ICT dan

	Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	Pentadbir Pangkalan Data
060302	**Penerimaan Sistem**	**Tindakan**
	Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pemilik Sistem, Pentadbir Sistem Aplikasi dan Portal ICT, dan ICTSO
0604	**Perisian Berbahaya**	
Objektif:	Melindungi integriti perisian dan maklumat dari pendedahan atau kerosakan yang disebabkan oleh perisian berbahaya seperti virus, *Trojan* dan sebagainya.	
060401	**Perlindungan dari Perisian Berbahaya**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Memasang sistem keselamatan untuk mengesan perisian atau program berbahaya seperti anti virus, *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) serta mengikut prosedur penggunaan yang betul dan selamat; b. Memasang dan menggunakan hanya perisian yang tulen, berdaftar dan dilindungi di bawah mana-mana undang-undang bertulis yang berkuat kuasa; c. Mengimbas semua perisian atau sistem dengan antivirus sebelum menggunakannya; d. Mengemas kini antivirus dengan *pattern* antivirus yang terkini ; e. Menyemak kandungan sistem atau maklumat secara berkala atau mengikut keperluan teknologi perisian yang digunakan bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; f. Menghadiri sesi kesedaran mengenai ancaman perisian berbahaya dan cara mengendalikannya; g. Memasukkan klausa tanggungan di dalam kontrak yang telah ditawarkan kepada pembekal perisian. Klausa ini bertujuan untuk tuntutan baik pulih sekiranya perisian tersebut mengandungi program berbahaya;	Pengguna ICT KBS

	h. Mengadakan program dan prosedur jaminan kualiti ke atas semua sistem aplikasi yang dibangunkan; dan i. Memberi amaran kepada pengguna ICT KBS mengenai ancaman keselamatan ICT seperti serangan virus.	
060402	**Perlindungan dari *Mobile Code***	**Tindakan**
	Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	Pengguna ICT KBS
0605	***Housekeeping***	
Objektif:	Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
060501	***Backup***	**Tindakan**
	Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, *backup* hendaklah dilakukan setiap kali konfigurasi berubah. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Membuat *backup* keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; b. Membuat *backup* ke atas semua data dan maklumat mengikut keperluan operasi. Kekerapan *backup* bergantung pada tahap kritikal maklumat; c. Menguji sistem *backup* dan prosedur *restore* sedia ada bagi memastikan ianya dapat berfungsi dengan sempurna, boleh dipercayai dan berkesan apabila digunakan khususnya pada waktu kecemasan; d. Menyimpan sekurang-kurangnya tiga (3) generasi *backup*; dan e. Merekodkan dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Pengguna ICT KBS
0606	**Pengurusan Rangkaian**	
Objektif:	Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
060601	**Kawalan Infrastruktur Rangkaian**	**Tindakan**
	Infrastruktur Rangkaian mestilah dirancang, disediakan, dibangunkan, dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi dalam rangkaian.	Pengurus ICT, ICTSO dan Pentadbir Operasi ICT

	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan; b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas daripada risiko seperti pencerobohan, haiwan perosak, banjir, gegaran dan habuk; c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna ICT KBS yang dibenarkan sahaja; d. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi; e. *Firewall* hendaklah dipasang serta dikonfigurasi dan diselia oleh Pentadbir Operasi ICT; f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan KBS; g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna ICT KBS kecuali mendapat kebenaran ICTSO; h. Memasang perisian *Intrusion Prevention System* (IPS) bagi mengesan sebarang cubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat KBS; i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang; j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan KBS adalah tidak dibenarkan; dan k. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.	
0607	**Pengurusan Media**	
Objektif:	Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060701	**Penghantaran dan Pemindahan**	**Tindakan**
	Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada pegawai atasan terlebih dahulu.	Pengguna ICT KBS

060702	Prosedur Pengendalian Media	Tindakan
	Prosedur-prosedur pengendalian media yang perlu dipatuhi adalah seperti berikut : a. Melabelkan semua media mengikut tahap sensitiviti sesuatu maklumat; b. Mengehadkan dan menentukan capaian media kepada pengguna ICT KBS yang dibenarkan sahaja; c. Mengehadkan pengedaran data atau media untuk tujuan yang dibenarkan sahaja; d. Mengawal dan merekodkan aktiviti penyelenggaraan media bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; e. Menyimpan semua media di tempat yang selamat; dan f. Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut tatacara semasa yang berkuat kuasa.	Pengguna ICT KBS
060703	**Keselamatan Sistem Dokumentasi**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut : a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; b. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	Pengguna ICT KBS
0608	**Pengurusan Pertukaran Maklumat**	
Objektif:	Memastikan keselamatan pertukaran maklumat dan perisian antara KBS dan agensi luar terjamin.	
060801	**Pertukaran Maklumat**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi pertukaran maklumat melalui penggunaan pelbagai jenis kemudahan komunikasi; b. Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara KBS dengan agensi luar;	Pengguna ICT KBS

	c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KBS; dan d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	
060802	**Pengurusan Mel Elektronik (E-mel)**	**Tindakan**
	Penggunaan e-mel di KBS hendaklah dipantau secara berterusan oleh Pentadbir Operasi ICT untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 bertajuk "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan" dan mana-mana undang-undang bertulis yang berkuat kuasa. Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut : a. Akaun atau alamat Mel elektronik (e-mel) yang diperuntukkan oleh KBS sahaja boleh digunakan. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; b. Setiap e-mel yang disediakan hendaklah mematuhi format yang telah ditetapkan oleh KBS; c. Memastikan subjek dan kandungan e-mel adalah berkaitan dan menyentuh perkara perbincangan yang sama sebelum penghantaran dilakukan; d. Penghantaran e-mel rasmi hendaklah menggunakan akaun e-mel rasmi dan pastikan alamat e-mel penerima adalah betul; e. Pengurusan sistem fail elektronik yang telah ditetapkan; f. E-mel yang tidak penting dan tidak mempunyai nilai arkib yang telah diambil tindakan dan tidak diperlukan lagi bolehlah dihapuskan; g. Pengguna ICT KBS hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; h. Respons ke atas e-mel dengan cepat dan mengambil tindakan segera; i. Pengguna ICT KBS hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan	Pengguna ICT KBS dan Pentadbir Operasi ICT

	j. Pengguna ICT KBS hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	
0609	**Perkhidmatan E-Dagang (*Electronic Commerce Services*)**	
Objektif:	Mengawal sensitiviti aplikasi dan maklumat dalam perkhidmatan ini agar sebarang risiko seperti penyalahgunaan maklumat, kecurian maklumat serta pindaan yang tidak sah dapat dihalang.	
060901	**E-Dagang**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta pengubahsuaian yang tidak dibenarkan; b. Maklumat yang terlibat dalam transaksi dalam talian (*on-line*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, duplikasi atau pengulangan mesej yang tidak dibenarkan; dan c. Integriti maklumat yang disediakan untuk sistem yang boleh dicapai oleh orang awam atau pihak lain yang berkepentingan hendaklah dilindungi untuk mencegah sebarang pindaan yang tidak diperakukan.	Pengguna ICT KBS
060902	**Maklumat Umum**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut : a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisme yang bersesuaian; b. Memastikan sistem aplikasi yang boleh di akses oleh orang awam di uji terlebih dahulu; dan c. Memastikan segala maklumat yang hendak dipaparkan telah disahkan dan diluluskan sebelum dimuat naik ke laman web/portal.	Pengguna ICT KBS
0610	**Pemantauan**	
Objektif:	Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
061001	**Pengauditan dan Forensik ICT**	**Tindakan**
	ICTSO mestilah bertanggungjawab merekodkan dan menganalisis perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT KBS;	Pentadbir Operasi ICT dan ICTSO

	b. Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*, pemalsuan (*forgery*, *phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); c. Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem aplikasi tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; d. Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; e. Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; f. Aktiviti instalasi dan penggunaan perisian yang membebankan *bandwidth* rangkaian; g. Aktiviti penyalahgunaan akaun e-mel; dan h. Aktiviti penukaran *IP address* selain daripada yang telah diperuntukkan tanpa kebenaran Pentadbir Operasi ICT.	
061002	**Jejak Audit**	**Tindakan**
	Setiap sistem aplikasi mestilah mempunyai jejak audit. Jejak audit merekodkan aktiviti-aktiviti yang berlaku dalam sistem aplikasi secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu transaksi. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a. Rekod setiap aktiviti transaksi; b. Maklumat jejak audit mengandungi identiti pengguna ICT KBS, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c. Aktiviti capaian pengguna ICT KBS ke atas sistem ICT sama ada secara sah atau sebaliknya; dan d. Maklumat aktiviti sistem yang tidak normal atau aktiviti yang tidak mempunyai ciri-ciri keselamatan. Jejak audit hendaklah disimpan untuk tempoh masa seperti yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Operasi ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat	Pentadbir Sistem Aplikasi dan Portal, Pentadbir Operasi ICT dan ICTSO

	membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi daripada kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
061003	**Sistem Log**	**Tindakan**
	Pentadbir Operasi ICT hendaklah melaksanakan perkara-perkara berikut: a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna ICT KBS; 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, hendaklah melaporkan kepada ICTSO dan CIO.	Pentadbir Operasi ICT dan ICTSO
061004	**Pemantauan Log**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu di wujud dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekodkan dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d. Aktiviti pentadbiran dan operator sistem perlu direkodkan; e. Kesalahan, kesilapan dan / atau penyalahgunaan perlu dilogkan, dianalisis dan diambil tindakan sewajarnya; dan f. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam KBS atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	Pentadbir Operasi ICT dan ICTSO

Bidang 7

KAWALAN CAPAIAN

BIDANG 07		
KAWALAN CAPAIAN		
0701	**Dasar Kawalan Capaian**	
Objektif:	Mengawal capaian ke atas maklumat.	
070101	**Keperluan Kawalan Capaian**	**Tindakan**
	Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna ICT KBS yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna ICT KBS sedia ada. Peraturan kawalan capaian yang mantap perlulah diwujudkan, didokumenkan dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan teknologi terkini. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Kawalan capaian ke atas aset ICT mengikut keperluan keselamatan dan peranan pengguna ICT KBS; b. Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; c. Keselamatan maklumat yang dicapai menggunakan kemudahan atau peralatan mudah alih; dan d. Kawalan ke atas kemudahan pemprosesan maklumat.	ICTSO, Pentadbir Operasi ICT dan Pentadbir Sistem Aplikasi dan Portal
0702	**Pengurusan Capaian Pengguna ICT KBS**	
Objektif:	Mengawal capaian pengguna ICT KBS ke atas aset ICT KBS.	
070201	**Akaun Pengguna ICT KBS**	**Tindakan**
	Pengguna ICT KBS adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna ICT KBS dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh KBS sahaja boleh digunakan; b. Akaun pengguna ICT KBS mestilah unik dan hendaklah mencerminkan identiti pengguna ICT KBS; c. Akaun pengguna ICT KBS yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu;	Pentadbir Operasi ICT, Pentadbir Sistem Aplikasi dan Portal, Pentadbir Pangkalan Data dan Pemilik Sistem Aplikasi dan Portal

	d. Pemilikan akaun pengguna ICT KBS bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan KBS. Akaun boleh ditarik balik jika penggunaannya melanggar peraturan; e. Penggunaan akaun milik orang lain atau akaun yang dikongsi bersama adalah dilarang; dan f. Pentadbir Operasi ICT boleh membeku dan menamatkan akaun pengguna ICT KBS atas sebab-sebab berikut: i. Pengguna ICT KBS yang bercuti panjang dalam tempoh waktu melebihi tiga (3) bulan; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	
070202	**Hak Capaian**	**Tindakan**
	Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem Aplikasi dan Portal, Pentadbir Operasi ICT dan Pemilik Sistem Aplikasi dan Portal
070203	**Pengurusan Kata Laluan**	**Tindakan**
	Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh KBS seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna ICT KBS hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi; c. Panjang kata laluan mestilah 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 w*indows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama;	Pengguna ICT KBS dan Pentadbir Sistem Aplikasi dan Portal

	f. Kata laluan hendaklah tidak dipaparkan semasa input, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program; g. Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas *login* kali pertama atau selepas kata laluan diset semula; h. Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna ICT KBS; i. Kata laluan bagi pengguna ICT KBS hendaklah ditukar dalam tempoh 90 hari atau selepas tempoh masa bersesuaian; dan j. Mengelakkan penggunaan semula kata laluan e-mel yang baru digunakan.	
070204	***Clear Desk* dan *Clear Screen***	**Tindakan**
	Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna ICT KBS atau di paparan skrin apabila pengguna ICT KBS tidak berada di tempatnya. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Menggunakan kemudahan *password screen saver* atau *logout* 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 faksimile dan mesin fotostat.	Pengguna ICT KBS
0703	**Kawalan Capaian Rangkaian**	
Objektif:	Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
070301	**Capaian Rangkaian**	**Tindakan**
	Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang antara muka yang bersesuaian antara rangkaian KBS, rangkaian agensi lain dan rangkaian awam;	ICTSO dan Pentadbir Operasi ICT

	b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna ICT KBS dan peralatan yang menepati kesesuaian penggunaannya; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna ICT KBS terhadap perkhidmatan rangkaian ICT.	
070302	**Capaian Internet**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Penggunaan Internet di KBS hendaklah dipantau secara berterusan oleh Pentadbir Operasi ICT bagi memastikan penggunaannya untuk tujuan capaian yang dibenarkan sahaja. Kewaspadaan ini akan dapat melindungi daripada kemasukan *malicious code,* virus dan bahan-bahan yang tidak sepatutnya ke dalam rangkaian KBS; b. Kaedah *Content Filtering* mestilah digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; c. Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti (*video conferencing*, *video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan; d. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. KSU / CIO berhak menentukan pengguna ICT KBS yang dibenarkan menggunakan Internet atau sebaliknya; e. Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/Bahagian/ pegawai yang diberi kuasa; f. Bahan yang diperoleh dari Internet hendaklah ditentukan ketepatan dan kesahihannya. Sebagai amalan terbaik, rujukan sumber Internet hendaklah dinyatakan; g. Bahan rasmi hendaklah disemak dan mendapat pengesahan daripada Ketua Jabatan/Bahagian sebelum dimuat naik ke Internet; h. Pengguna ICT KBS hanya dibenarkan memuat turun bahan yang sah seperti perisian yang berdaftar dan di bawah hak cipta terpelihara; i. Sebarang bahan yang dimuat turun dari Internet hendaklah digunakan untuk tujuan yang dibenarkan oleh KBS;	Pentadbir Operasi ICT dan Pentadbir Rangkaian

	j. Hanya pegawai yang mendapat kebenaran sahaja boleh menggunakan kemudahan perbincangan awam seperti *newsgroup* dan *bulletin board*. Walau bagaimanapun, kandungan perbincangan awam ini hendaklah mendapat kelulusan daripada CIO terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; k. Penggunaan modem untuk tujuan sambungan ke Internet tidak dibenarkan sama sekali; dan l. Pengguna ICT KBS adalah dilarang melakukan aktiviti-aktiviti seperti berikut: i. Memuat naik, memuat turun, menyimpan dan menggunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian Internet; dan ii. Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah, politik, jenayah dan pernyataan berbentuk hasutan.	
0704	**Kawalan Capaian Sistem Pengoperasian**	
Objektif:	Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
070401	**Capaian Sistem Pengoperasian**	**Tindakan**
	Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Ciri-ciri keselamatan dalam sistem operasi perlu digunakan untuk menghalang capaian ke sumber sistem komputer. Kemudahan ini juga perlu bagi: a. Mengenal pasti identiti, terminal atau lokasi bagi setiap pengguna ICT KBS yang dibenarkan; b. Merekodkan capaian yang berjaya dan gagal. c. Membekalkan kemudahan untuk pengesahan; dan d. Bagi sistem, kata laluan kunci digunakan, kualiti kata kunci perlu mendapat pengesahan; Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: a. Mengesahkan pengguna ICT KBS yang dibenarkan;	Pentadbir Sistem Keselamatan ICT dan ICTSO

	b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna ICT KBS bertaraf *super user;* c. Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem; dan d. Menyediakan tempoh penggunaan mengikut kesesuaian. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *log on* yang terjamin; b. Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna ICT KBS dan hanya digunakan oleh pengguna ICT KBS berkenaan sahaja; c. mewujudkan sistem pengurusan kata laluan secara interaktif dan memastikan kata laluan adalah berkualiti; d. Mengehadkan dan mengawal penggunaan program/perisian; dan e. Mengehadkan tempoh sambungan ke sesebuah aplikasi berisiko tinggi.	
070402	**Kad Pintar**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Penggunaan kad pintar Kerajaan Elektronik (Kad EG) hendaklah digunakan bagi capaian sistem Kerajaan Elektronik yang dikhususkan; b. Kad pintar hendaklah disimpan di tempat selamat bagi mengelakkan sebarang kecurian atau digunakan oleh pihak lain; c. Perkongsian kad pintar untuk sebarang capaian sistem adalah tidak dibenarkan sama sekali. Kad pintar yang salah kata laluan sebanyak tiga (3) kali cubaan akan disekat; dan d. Sebarang kehilangan, kerosakan dan kata laluan disekat perlu dimaklumkan kepada Bahagian yang bertanggungjawab ke atas penggunaan aplikasi yang berkaitan.	Pengguna ICT KBS
0705	**Kawalan Capaian Sistem Aplikasi dan Maklumat**	
Objektif:	Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat dalam sistem aplikasi.	

070501	Capaian Sistem Aplikasi dan Maklumat	Tindakan
	Bertujuan melindungi sistem aplikasi dan maklumat sedia ada daripada sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan kelumpuhan sistem. Bagi memastikan kawalan capaian sistem aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a. Pengguna ICT KBS hanya boleh menggunakan sistem aplikasi dan maklumat yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; b. Setiap aktiviti capaian sistem aplikasi dan maklumat pengguna ICT KBS hendaklah direkodkan (sistem log); c. Mengehadkan capaian sistem aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna ICT KBS akan disekat; d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; e. Capaian dari luar ke atas sistem aplikasi dan maklumat adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja; dan f. Had masa *idle* sistem aplikasi adalah selama lima (5) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi akan ditamatkan (*logout*).	Pentadbir Sistem, Pentadbir Operasi ICT dan ICTSO
0706	**Peralatan Mudah Alih dan Kerja Jarak Jauh**	
Objektif:	Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudahan kerja jarak jauh	
070601	**Peralatan Mudah Alih**	**Tindakan**
	Perkara yang perlu dipatuhi adalah seperti berikut : a. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan. b. Peralatan komputer mudah alih (seperti komputer riba dan tablet) hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Pengguna ICT KBS

	c. Instalasi perisian komputer mudah alih mestilah dilaksanakan oleh BPM. d. Komputer mudah alih hendaklah sentiasa di bawah penjagaan yang rapi bagi menjamin keselamatannya dari kecurian dan kerosakan. e. Pengguna yang membawa maklumat terperingkat dikehendaki mengisytiharkannya dengan mendapat kebenaran bertulis dari Ketua Jabatan atau setaraf. f. Pengguna yang menggunakan komputer mudah alih persendirian untuk tugas rasmi mestilah mendapat kelulusan bertulis daripada Ketua Jabatan.	
070602	**Kerja Jarak Jauh**	**Tindakan**
	Perkara yang perlu dipatuhi adalah seperti berikut : a. Tindakan perlindungan hendaklah diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan. Semua capaian jarak jauh (*remote access*) tidak dibenarkan melainkan dengan menggunakan sistem autentikasi dan ciri-ciri keselamatan yang dibenarkan. b. Penggunaan perkhidmatan ini hendaklah mendapatkan kebenaran ICTSO. Pengguna yang diberikan hak adalah dipertanggungjawabkan penuh ke atas penggunaan kemudahan ini.	Pengguna ICT KBS
0707	***Bring Your Own Devices* (BYOD)**	
Objektif:	Memastikan keselamatan maklumat semasa menggunakan peralatan BYOD di dalam KBS.	
070701	**Keperluan dan Kawalan Penggunaan BYOD**	**Tindakan**
	KBS membenarkan capaian sistem e-mel dan aplikasi mudah alih menggunakan peralatan mudah alih peribadi yang dibawa ke pejabat (BYOD). Walau bagaimanapun, penggunaannya perlu mematuhi perkara berikut: a. Pengguna bertanggungjawab sepenuhnya ke atas keselamatan peralatan mudah alih peribadi mereka; b. Pentadbir ICT hanya menyediakan sokongan terhad kepada pengguna bagi tujuan konfigurasi, tetapan dan penggunaan peralatan mudah alih peribadi bagi capaian ke sistem e-mel dan aplikasi yang digunakan; c. Mengaktifkan fungsi keselamatan kata laluan bagi mengelakkan akses yang tidak dibenarkan;	Pengguna ICT KBS

	d. Melaporkan kehilangan peralatan mudah alih kepada ICTSO; e. Mengaktifkan kemudahan *remote wipe* (sekiranya ada) bagi memadamkan maklumat Kerajaan daripada peralatan mudah alih peribadi.	

Bidang 8

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM APLIKASI

BIDANG 08

PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM APLIKASI

0801	**Keselamatan Dalam Membangunkan Sistem Aplikasi**	
Objektif:	Memastikan sistem aplikasi yang dibangunkan secara dalaman atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
080101	**Keperluan Keselamatan Sistem Maklumat**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Perolehan, pembangunan, penambahbaikan dan penyelenggaraan sistem aplikasi hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; b. Ujian keselamatan hendaklah dijalankan ke atas input data sistem aplikasi untuk menyemak pengesahan dan integriti data yang dimasukkan, sistem pemprosesan untuk menentukan sama ada program berjalan dengan betul dan sempurna serta output sistem aplikasi untuk memastikan data yang telah diproses adalah tepat; c. Sistem aplikasi perlu mengandungi semakan pengesahan untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan d. Semua sistem aplikasi yang dibangunkan sama ada secara dalaman atau sebaliknya hendaklah diuji terlebih dahulu bagi memastikan sistem aplikasi berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pemilik Sistem Aplikasi, Pentadbir Sistem Aplikasi, Pentadbir Operasi ICT dan ICTSO
080102	**Pengesahan Data Input dan Output**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Data input bagi sistem aplikasi perlu disemak dan disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b. Data output daripada sistem aplikasi perlu disemak dan disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem Aplikasi dan Pentadbir Sistem Aplikasi
0802	**Kawalan Kriptografi**	
Objektif:	Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.	

080201	Enkripsi	Tindakan
	a. Pengguna ICT KBS hendaklah membuat enkripsi (*encryption*) ke atas maklumat rahsia rasmi pada setiap masa. b. Menggunakan enkripsi (*encryption*) ke atas dokumen sulit dan terhad yang disediakan dan dihantar secara elektronik.	Pengguna ICT KBS
080202	**Tandatangan Digital**	**Tindakan**
	Penggunaan tandatangan digital adalah dimestikan kepada semua pengguna ICT KBS khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Pengguna ICT KBS
080203	**Pengurusan Infrastruktur Kunci Awam (*PKI*)**	**Tindakan**
	Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnahkan dan didedahkan sepanjang tempoh sah kunci tersebut.	Pengguna ICT KBS
0803	**Keselamatan Fail Sistem Aplikasi**	
Objektif:	Memastikan supaya fail sistem aplikasi dikawal dan dikendalikan dengan baik dan selamat.	
080301	**Kawalan Fail Sistem Aplikasi**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Proses pengemaskinian fail sistem aplikasi hanya boleh dilakukan oleh Pentadbir Sistem Aplikasi atau pegawai yang berkenaan dan mengikut prosedur yang telah ditetapkan; b. Kod atau atur cara sistem aplikasi yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; c. Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; d. Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan e. Mengaktifkan sistem log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pemilik Sistem Aplikasi; Pentadbir Sistem Aplikasi dan Pentadbir Operasi ICT
0804	**Keselamatan Dalam Proses Pembangunan dan Sokongan**	
Objektif:	Menjaga dan menjamin keselamatan sistem aplikasi dan maklumat.	

080401	**Prosedur Kawalan Perubahan**	**Tindakan**
	Perkara-perkara yang perlu dipatuhi adalah seperti berikut :Perubahan atau pengubahsuaian ke atas sistem aplikasi dan maklumat hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; a. Sistem aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada kesan yang buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh pembangun sistem aplikasi; b. Mengawal perubahan dan/atau pindaan ke atas sistem aplikasi dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; c. Akses kepada *source code* sistem aplikasi perlu dihadkan kepada pengguna ICT KBS yang diizinkan; dan d. Menghalang sebarang peluang untuk membocorkan maklumat.	Pemilik Sistem Aplikasi dan Pentadbir Sistem Aplikasi
080402	**Pembangunan Sistem Aplikasi Secara *Outsource***	**Tindakan**
	Pembangunan sistem aplikasi secara *outsource* perlu diselia dan dipantau oleh pemilik sistem aplikasi. *Source code* adalah menjadi hak milik KBS.	Pentadbir Sistem Aplikasi dan Pemilik Sistem
0805	**Kawalan Teknikal Keterdedahan (*Vulnerability*)**	
Objektif:	Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya	
080501	**Kawalan dari Ancaman Teknikal**	**Tindakan**
	Kawalan teknikal terhadap keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut : a. Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem aplikasi dan maklumat yang digunakan; b. Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan c. Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem Aplikasi dan ICTSO

Bidang 9

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

BIDANG 09

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

0901	**Mekanisme Pelaporan Insiden Keselamatan ICT**	
Objektif:	Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.	
090101	**Mekanisme Pelaporan**	**Tindakan**
	Insiden keselamatan ICT bermaksud musibah (*adverse event*) yang berlaku ke atas aset ICT atau ancaman kemungkinan berlaku kejadian tersebut. Ia mungkin suatu perbuatan yang melanggar dasar keselamatan ICT sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT hendaklah dilaporkan kepada CERT KBS dengan kadar segera untuk sokongan peringkat pertama (*First Level Support).* Insiden tersebut akan dilaporkan kepada CIO dan pihak yang bertanggungjawab ke atas pengendalian insiden keselamatan sektor awam bagi tujuan makluman dan nasihat lanjutan yang diperlukan (jika ada). Semua maklumat adalah SULIT, dan hanya boleh didedahkan kepada pihak-pihak yang dibenarkan. Insiden keselamatan ICT merangkumi seperti berikut : a. Maklumat disyaki hilang atau didedahkan kepada pihak-pihak yang tidak diberi kuasa; b. Sistem ICT digunakan tanpa kebenaran atau disyaki sedemikian; c. Kata laluan atau mekanisme kawalan akses hilang, didedahkan, disyaki dicuri dan disalah guna; d. Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem dan komunikasi kerap kali gagal; dan e. Berlaku percubaan menceroboh, penyelewengan dan insiden-insiden yang tidak dijangka. Dalam keadaan atau persekitaran berisiko tinggi, CIO hendaklah melaporkan kepada KSU dengan serta-merta supaya satu keputusan segera dapat diambil. Tindakan ini perlu bagi melindungi imej kementerian. Prosedur pelaporan insiden keselamatan ICT berdasarkan: a. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan	Pengguna ICT KBS

	b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
0902	**Pengurusan Maklumat Insiden Keselamatan ICT**	
Objektif:	Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
090201	**Pengurusan Maklumat Insiden Keselamatan ICT**	**Tindakan**
	Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan dan tindakan pengukuhan bagi mengawal kekerapan, kerosakan dan meminimumkan kos kejadian insiden yang akan datang. Maklumat ini juga digunakan untuk mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KBS. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut : a. Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; b. Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; c. Menyediakan pelan kontingensi dan mengaktifkan pelan kesinambungan perkhidmatan; d. Menyediakan tindakan pemulihan segera; dan e. Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	CERT KBS

Bidang 10

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

BIDANG 10

PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

1001	**Dasar Kesinambungan Perkhidmatan**	
Objektif:	Menjamin operasi perkhidmatan berjalan lancar dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
100101	**Pelan Kesinambungan Perkhidmatan**	**Tindakan**
	Pelan Kesinambungan Perkhidmatan (PKP) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Pelan ini mestilah diluluskan oleh Pengurusan Tertinggi KBS. Perkara-perkara berikut perlu diberi perhatian: a. Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes bersama dengan kemungkinan dan impak gangguan tersebut serta akibat terhadap keselamatan ICT; b. Melaksanakan prosedur-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 ICT KBS mengenai prosedur kecemasan; e. Membuat *backup*; dan f. Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ia sentiasa kekal berkesan. PKP yang dibangunkan hendaklah mengandungi perkara-perkara berikut: a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; b. Senarai personel KBS dan vendor berserta nombor yang boleh dihubungi (faksimile, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai *backup* personel untuk melaksanakan prosedur kecemasan atau pemulihan; c. Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan;	TKSU(P)

	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 PKP perlu disimpan di lokasi berasingan dan sentiasa dikemas kini serta dilindungi seperti di lokasi utama untuk mengelakkan kerosakan akibat bencana di lokasi utama. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian PKP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui tanggungjawab dan peranan mereka apabila pelan dilaksanakan.	

Bidang 11

PEMATUHAN

BIDANG 11		
PEMATUHAN		
1111	**Pematuhan dan Keperluan Perundangan**	
Objektif:	Meningkatkan tahap keselamatan ICT bagi mengelak daripada pelanggaran kepada Dasar Keselamatan ICT KBS.	
111101	**Pematuhan Dasar**	**Tindakan**
	Setiap pengguna ICT KBS perlu membaca, memahami dan mematuhi Dasar Keselamatan ICT KBS dan undang-undang atau peraturan-peraturan lain berkaitan yang berkuat kuasa. Semua aset ICT KBS adalah hak milik Kerajaan dan di bawah pengawalan Pegawai Pengawal. Pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna ICT KBS untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT KBS selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalahgunaan sumber KBS.	Pengguna ICT KBS
111102	**Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal**	**Tindakan**
	ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem ICT perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan.	ICTSO
110103	**Pematuhan Keperluan Audit**	**Tindakan**
	Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem ICT. 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 ICT perlu dipelihara dan diselia bagi mengelakkan berlaku penyalahgunaan.	Pengguna ICT KBS
110104	**Keperluan Perundangan**	**Tindakan**
	Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna ICT KBS di KBS:	Pengguna ICT KBS

	a. Arahan Keselamatan; b. Pekeliling Am Bilangan 3 Tahun 2000 - Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan; c. *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS) 2002; d. Pekeliling Am Bilangan 1 Tahun 2001 - Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT); e. Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-Agensi Kerajaan; f. Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam; g. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; h. Surat Arahan Ketua Setiausaha Negara – Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) Di Agensi-Agensi Kerajaan (20 Oktober 2006); i. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik Di Agensi-Agensi Kerajaan (1 Jun 2007); j. Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan (23 November 2007); k. Surat Pekeliling Perbendaharaan Bil.2/1995 (Tambahan Pertama) - Tatacara Penyediaan, Penilaian dan Penerimaan Tender; l. Surat Pekeliling Perbendaharaan Bil. 3/1995 -Peraturan Perolehan Perkhidmatan Perundingan; m. Akta Tandatangan Digital 1997; n. Akta Rahsia Rasmi 1972; o. Akta Jenayah Komputer 1997;	

	p. Akta Hak Cipta (Pindaan) Tahun 1997; q. Akta Komunikasi dan Multimedia 1998; r. Perintah-Perintah Am; s. Arahan Perbendaharaan; t. Arahan Teknologi Maklumat 2007; u. Garis Panduan Keselamatan MAMPU 2004; v. *Standard Operating Procedure* (SOP) ICT KBS; w. Garis Panduan Pelaksanaan Blog Bagi Agensi Sektor Awam 2009; x. Pekeliling/Arahan/Garis Panduan yang berkuat kuasa dari semasa ke semasa; y. Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010; dan z. Surat Arahan Ketua Pengarah MAMPU – Amalan Terbaik Penggunaan Media Jaringan Sosial (8 April 2011).	
110105	**Pelanggaran Dasar**	**Tindakan**
	Pelanggaran Dasar Keselamatan ICT KBS boleh dikenakan tindakan tatatertib dan / atau perundangan.	Pengguna ICT KBS

GLOSARI

GLOSARI	
Ancaman	Bermaksud apa sahaja kejadian yang berpotensi atau tindakan yang boleh menyebabkan berlaku kemusnahan atau musibah.
Antivirus	Perisian yang mengimbas virus pada media storan, seperti cakera keras (hard disk) dan disket (*diskette*) untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk komputer, media storan, server, router,firewall, rangkaian dan lain-lain.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Jalur lebar Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (e.g, di antara cakera keras dan PC utama) dalam jangka masa yang ditetapkan.
CERT KBS	*Computer Emergency Response Team* Organisasi yang ditubuhkan untuk Membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawabkan terhadap ICT dan sistem maklumat bagi menyokong arahtuju sesebuah organisasi.
Clear Desk	Bermaksud tidak meninggalkan sebarang dokumen yang sensitif di atas meja.
Clear Screen	Bermaksud tidak memaparkan sebarang maklumat sensitif apabila komputer berkenaan ditinggalkan.
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi atau penyulitan. Proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direkabentuk untuk menghalang capaian pengguna yang tidak berkenaan kepada atau daripada rangkaian dalaman. Terdapat dalam bentuk perkakasan atau perisian atau kombinasi kedua-duanya.
Forgery	Pemalsuan dan penyamaran identiti yang banyak dilakukan dalam penghantaran mesej melalui emel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (information theft / espionage), penipuan(hoaxes).
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	*Information and Communication Technology.*
ICTSO	*ICT Security Officer* Pegawai yang bertanggungjawab terhadap keselamatan sistem komputer.
Insiden Keselamatan	Musibah (adverse event) yang berlaku ke atas sistem maklumat dan komunikasi atau ancaman kemungkinan berlaku kejadian tersebut.
Internet	Sistem rangkaian seluruh dunia, di mana pengguna pada mana-mana komputer boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkain yang lain. Menjadi pemandu arah trafik dengan betul dari satu trafik ke satu trafik yang lain di

	samping mengekalkan trafik-trafik dalam rangkaian-rangkaian tersebut agar sentiasa berasingan.
Intrusion Detection System (IDS)	Sistem Pengesan Pencerobohan Perisian atau perkakasan yang mengesan aktiviti tidak berkaitan, kesilapan atau yang berbahaya kepada sistem. Sifat IDS berpandukan jenis data yang dipantau, iaitu sama ada lebih bersifat host atau rangkaian.
Intrusion Prevention System (IPS)	Sistem Pencegah Pencerobohan Perkakasan keselamatan komputer yang memantau rangkaian dan/atau aktiviti yang berlaku dalam sistem bagi mengesan perisian berbahaya. Boleh bertindakbalas menyekat atau menghalang aktiviti serangan atau malicious code. E.g. Network-based IPS yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
JPICT	Jawatan Kuasa Pemandu ICT
LAN	Local Area Network Rangkaian Kawasan Setempat yang menghubungkan komputer.
Log out	*Log-out* komputer Keluar daripada sesuatu sistem atau aplikasi komputer.
Malicious Code	Perkakasan atau perisian yang dimasukkan ke dalam sistem tanpa kebenaran bagi tujuan pencerobohan. Ia melibatkan serangan virus, trojan horse, worm, spyware dan sebagainya.
MODEM	*MOdulator DEModulator* Peranti yang boleh menukar strim bit digital ke isyarat analog dan sebaliknya. Ia biasanya disambung ke talian telefon bagi membolehkan capaian Internet dibuat dari komputer.
Outsource	Maklumat yang diproses dan diperolehi di luar daripada sesuatu organisasi atau struktur kerja.
Pemilik Sistem Aplikasi dan Portal	Jabatan/Bahagian/Cawangan/Unit yang bertanggungjawab ke atas pengurusan dan pengoperasian sistem aplikasi/portal yang berkenaan.
Pengguna	Semua pengguna ICT di Ibu Pejabat Kementerian Belia dan Sukan, Jabatan Belia dan Sukan Negara, Jabatan Belia dan Sukan Negeri, Pejabat Belia dan Sukan Daerah, Kompleks Belia dan Sukan, Kompleks Rakan Muda, Akademi Pembangunan Belia Malaysia, Pejabat Pesuruhjaya Sukan, Pejabat Pendaftar Pertubuhan Belia Malaysia dan Institut Kemahiran Belia Negara (termasuk pegawai, kakitangan, pembekal, pakar runding dll.).
Penilaian Risiko	Bermaksud penilaian ke atas kemungkinan berlakunya bahaya atau kerosakan atau kehilangan aset.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti spreadsheet dan word processing ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
PKI	*Public-Key Infrastructure* Infrastruktur Kunci Awam.
Pusat Data	Pusat simpanan data.
Rahsia	Dokumen rasmi, maklumat rasmi dan bahan rasmi yang jika didedahkan tanpa kebenaran akan membahayakan keselamatan negara, menyebabkan kerosakan besar kepada kepentingan dan martabat Malaysia atau memberi keuntungan besar kepada sesebuah kuasa asing.

Rahsia Besar	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran akan menyebabkan kerosakan yang amat besar kepada Malaysia.
Risiko	Bermaksud kemungkinan yang boleh menyebabkan bahaya, kerosakan dan kerugian.
Router	Penghala yang digunakan untuk menghantar data antara dua rangkaian yang mempunyai kedudukan rangkaian yang berlainan. Contohnya, pencapaian Internet.
Screen saver	Imej yang akan diaktifkan pada komputer setelah ianya tidak digunakan dalam jangka masa tertentu.
Server	Pelayan
Sulit	Dokumen, maklumat dan bahan rasmi yang jika didedahkan tanpa kebenaran walaupun tidak membahayakan keselamatan negara tetapi memudaratkan kepentingan atau martabat Malaysia atau kegiatan Kerajaan atau orang perseorangan atau akan menyebabkan keadaan memalukan atau kesusahan kepada pentadbiran atau akan menguntungkan sesebuah kuasa asing.
Switches	Suis merupakan gabungan hab dan titi yang menapis bingkai supaya mensegmenkan rangkaian. Kegunaan suis dapat memperbaiki prestasi rangkaian CSMA/CD secara mengurangkan perlanggaran yang berlaku.
Terhad	Dokumen rasmi, maklumat rasmi dan bahan rasmi selain daripada yang diperingkatkan Rahsia Besar, Rahsia atau Sulit tetapi berkehendakkan juga diberi satu tahap perlindungan keselamatan.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif personal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekalan kuasa ke peralatan yang bersambung.
Video streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Aturcara yang bertujuan merosakkan data atau sistem aplikasi.
Vulnerability	Bermaksud sebarang kelemahan pada aset atau sekumpulan aset yang boleh dieksploitasi oleh ancaman.
WAN	*Wide Area Network* Rangkaian yang merangkumi kawasan yang luas.
Worm	Sejenis virus yang boleh mereplikasi dan membiak dengan sendiri. Ia biasanya menjangkiti sistem operasi yang lemah atau tidak dikemas kini.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.

LAMPIRAN

LAMPIRAN 1

KEANGGOTAAN JAWATANKUASA PEMANDU ICT (JPICT) KBS

BIL	JAWATAN	PERANAN
1.	Ketua Setiausaha	**Pengerusi**
2.	Timbalan Ketua Setiausaha (Pengurusan) Merangkap Ketua Pegawai Maklumat (CIO) KBS	**Ahli**
3.	Timbalan Ketua Setiausaha (Strategik)	**Ahli**
4.	Ketua Pengarah Jabatan Belia dan Sukan Negara	**Ahli**
5.	Ketua Pengarah Bahagian Pembangunan Kemahiran	**Ahli**
6.	Setiausaha Bahagian Bahagian Pengurusan Maklumat	**Ahli**
7.	Setiausaha Bahagian Bahagian Kewangan	**Ahli**
8.	Setiausaha Bahagian Bahagian Pembangunan	**Ahli**
9.	Setiausaha Bahagian Bahagian Pengurusan Sumber Manusia	**Ahli**
10.	Setiausaha Bahagian Bahagian Khidmat Pengurusan	**Ahli**
11.	Setiausaha Bahagian Bahagian Dasar dan Perancangan Strategik	**Ahli**
12.	Setiausaha Bahagian Bahagian Akaun	**Ahli**
13.	Setiausaha Bahagian Setiausaha Hubungan Antarabangsa	**Ahli**
14.	Timbalan Ketua Pengarah Bahagian Pembangunan Sukan	**Ahli**
15.	Timbalan Ketua Pengarah Bahagian Pembangunan Belia	**Ahli**
16.	Timbalan Ketua Pengarah Bahagian Pembangunan Rakan Muda	**Ahli**
17.	Ketua Unit Komunikasi Korporat	**Ahli**

18.	Ketua Unit Audit Dalam	**Ahli**
19.	Pengarah Akademi Kemahiran Belia Golf	**Ahli**
20.	Penasihat Undang-undang Unit Undang-undang	**Ahli**
21.	Ketua Penolong Setiausaha (Operasi) Bahagian Pengurusan Maklumat Merangkap Pegawai Keselamatan ICT KBS (ICTSO)	**Ahli**
22.	Ketua Pegawai Eksekutif Institut Penyelidikan Pembangunan Belia Malaysia	**Ahli**
23.	Ketua Pegawai Eksekutif Perbadanan Stadium Malaysia	**Ahli**
24.	Pesuruhjaya Sukan Pejabat Pesuruhjaya Sukan	**Ahli**
25.	Ketua Pengarah Majlis Sukan Negara	**Ahli**
26.	Ketua Pengarah Institut Sukan Negara	**Ahli**
27.	Pendaftar Pendaftar Pertubuhan Belia Malaysia	**Ahli**
28.	Pengarah Pusat Belia Antarabangsa	**Ahli**
29.	Ketua Penolong Setiausaha (Pembangunan) Bahagian Pengurusan Maklumat	**Setiausaha**

LAMPIRAN 2

SURAT AKUAN PEMATUHAN

DASAR KESELAMATAN ICT
KEMENTERIAN BELIA DAN SUKAN (KBS)

Nama : _____

No. Kad Pengenalan : _____

Jawatan : _____

Jabatan / Bahagian /Unit : _____

Adalah dengan sesungguhnya dan sebenarnya mengaku bahawa :

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

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

.....

(Tanda Tangan Pegawai / Kakitangan)

Tarikh : .....

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

LAMPIRAN 3

KEANGGOTAAN PASUKAN TINDAK BALAS INSIDEN KESELAMATAN ICT KBS (CERT KBS)

BIL	JAWATAN	PERANAN
1	SUB (PM)	**Pengarah**
2	KPSU (PM) O	**Pengurus (ICTSO)**
3	KPSU(PM)P	**Ahli**
4	PSUK (PM) S	**Ahli**
5	PSUK (PM) M	**Ahli**
6	PSUK (PM) T	**Ahli**
7	PSU (PM) K	**Ahli**
8	PSUK (PM) R	**Ahli**
9	PSUK (PM) J	**Ahli**
10	Ketua Cawangan ICT MSN	**Ahli**
11	Ketua Cawangan ICT ISN	**Ahli**
12	Pegawai Teknologi Maklumat IPPBM	**Ahli**
13	Penolong Pegawai Teknologi Maklumat PPS	**Ahli**
14	Penolong Pegawai Teknologi Maklumat PSM	**Ahli**