DASAR KESELAMATAN TEKNOLOGI MAKLUMAT DAN KOMUNIKASI (ICT)

(Versi 5.0 2020)

09 Februari 2024

INSTITUT PENYELIDIKAN PEMBANGUNAN BELIA MALAYSIA
KEMENTERIAN BELIA DAN SUKAN MALAYSIA

PENGENALAN

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

OBJEKTIF

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

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

Manakala, objektif utama Keselamatan ICT IYRES ialah seperti berikut:

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

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

(c) Mencegah salah guna atau kecurian aset ICT Kerajaan

PERNYATAAN DASAR

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

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

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

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

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

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

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

yang sah dan tidak boleh disangkal;

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

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

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

SKOP

Aset ICT IYRES terdiri daripada perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia. Dasar Keselamatan ICT IYRES 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 IYRES ini merangkumi perlindungan semua bentuk maklumat kerajaan yang dimasukkan, diwujud, dimusnah, disimpan, dijana, dicetak, diakses, diedar, dalam penghantaran, dan yang dibuat salinan keselamatan. Ini akan dilakukan melalui pewujudan dan penguatkuasaan sistem kawalan dan prosedur dalam pengendalian semua perkara-perkara berikut:

(a) Perkakasan

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

(b) Perisian

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

(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 IYRES. Contohnya, sistem dokumentasi, prosedur operasi, rekod-rekod IYRES, 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 IYRES 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.

PRINSIP-PRINSIP

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

(a) Capaian/Akses Atas Dasar "Perlu Mengetahui"

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

(b) Hak Akses Minimum

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

(c) Akauntabiliti

Semua pengguna ICT IYRES adalah dipertanggungjawabkan ke atas semua tindakannya terhadap Aset ICT IYRES. 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 IYRES sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna ICT IYRES 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;

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

(d) Pengasingan

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

(e) Pengauditan

Pengauditan adalah tindakan untuk mengenal pasti insiden berkaitan keselamatan atau mengenal pasti keadaan yang mengancam keselamatan. Ia membabitkan pemeliharaan semua rekod berkaitan tindakan keselamatan. Dengan itu, Aset ICT seperti komputer, pelayan (*server*), *router*, *firewall* dan rangkaian hendaklah ditentukan dapat menjana dan menyimpan log tindakan keselamatan atau *audit trail*;

(f) Pematuhan

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

(g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan kebolehsediaan dan kebolehcapaian. Objektif utama adalah untuk meminimumkan sebarang gangguan atau kerugian akibat daripada ketidaksediaan. Pemulihan boleh dilakukan melalui aktiviti penduaan (*backup*) dan mewujudkan Pelan Pemulihan Bencana/Kesinambungan Perkhidmatan; dan

(h) Saling Bergantungan

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

PENILAIAN RISIKO KESELAMATAN ICT

IYRES hendaklah mengambil kira kewujudan risiko ke atas aset ICT akibat dari ancaman dan *vulnerability* yang semakin meningkat hari ini. Justeru itu IYRES 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.

IYRES 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 IYRES 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.

IYRES 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.

IYRES 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 01 PEMBANGUNAN DAN PENYELENGGARAAN DASAR	
0101 Dasar Keselamatan ICT	**Tindakan**
Objektif Menerangkan hala tuju dan sokongan pengurusan IYRES terhadap keselamatan selaras dengan keperluan KBS dan perundangan yang berkaitan.	
010101 Pelaksanaan Dasar	
Pelaksanaan dasar ini akan dijalankan oleh Ketua Pegawai Eksekutif selaku Pengerusi Jawatan Kuasa Pemandu ICT IYRES. JPICT ini terdiri daripada ahli-ahli seperti di Lampiran 1.	*Ketua Pegawai Eksekutif IYRES*
010102 Penyebaran Dasar	
Dasar ini perlu disebarkan kepada semua pengguna ICT IYRES.	*ICTSO*
010103 Penyelenggaraan Dasar	
Dasar Keselamatan ICT IYRES 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 IYRES: a. Kenal pasti dan tentukan **perubahan** yang diperlukan; b. Kemuka **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 IYRES; dan d. Dasar ini hendaklah dikaji semula sekurang- kurangnya sekali setahun atau mengikut keperluan semasa.	*ICTSO*

010104 Pengecualian Dasar	
Dasar Keselamatan ICT IYRES adalah terpakai kepada semua pengguna ICT IYRES dan tiada pengecualian diberikan.	*Pengguna ICT IYRES*

BIDANG 02 ORGANISASI KESELAMATAN	
0201 Infrastruktur Organisasi Dalaman	**Tindakan**
Objektif Menerangkan peranan dan tanggungjawab individu yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif Dasar Keselamatan ICT IYRES.	
020101 Ketua Pegawai Eksekutif	
Peranan dan tanggungjawab Ketua Pegawai Eksekutif adalah seperti berikut: a. Memastikan semua pengguna ICT IYRES memahami peruntukan-peruntukan di bawah Dasar Keselamatan ICT IYRES; b. Memastikan semua pengguna ICT IYRES mematuhi Dasar Keselamatan ICT IYRES; c. Memastikan semua keperluan organisasi (sumber kewangan, sumber kakitangan dan perlindungan keselamatan) adalah mencukupi; dan d. Memastikan penilaian risiko dan program keselamatan ICT dilaksanakan seperti yang ditetapkan di dalam Dasar Keselamatan ICT IYRES. e. Mempengerusikan mesyuarat Jawatankuasa Pemandu ICT (JPICT), IYRES	*Ketua Pegawai Eksekutif*
020102 Ketua Pegawai Maklumat (CIO)	
Pengurus Bahagian Perancangan dan Penyelidikan (P(BPP)) IYRES ialah Ketua Pegawai Maklumat (CIO) IYRES. Peranan dan tanggungjawab CIO IYRES adalah seperti berikut: a. Membantu Ketua Pegawai Eksekutif 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 IYRES serta pengurusan risiko dan pengauditan;	*P(BPP)*

dan d. Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT IYRES. e. Mengkaji semula dan melaksanakan kawalan keselamatan ICT selaras dengan keperluan IYRES; f. Menentukan kawalan akses pengguna ICT IYRES terhadap Aset ICT IYRES; g. Memastikan semua kakitangan, perunding, kontraktor dan pembekal yang terlibat dengan IYRES mematuhi dasar, piawaian dan garis panduan keselamatan ICT; h. Membangunkan garis panduan, prosedur dan tatacara untuk aplikasi-aplikasi khusus dalam IYRES dan agensi berkaitan yang mematuhi keperluan DKICT IYRES; dan i. Membangun, mengkaji semula dan mengemaskini pelan kontingensi keselamatan ICT di IYRES ;	
020103 Pegawai Keselamatan ICT (ICTSO)	
Pegawai Teknologi Maklumat ialah ICTSO IYRES Peranan dan tanggungjawab ICTSO yang dilantik adalah seperti berikut: a. Mengurus keseluruhan program-program keselamatan ICT IYRES; b. Menguatkuasakan pelaksanaan Dasar Keselamatan ICT IYRES; c. Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT IYRES kepada semua pengguna ICT IYRES; d. Mewujudkan garis panduan, prosedur dan tatacara selaras dengan keperluan Dasar Keselamatan ICT IYRES; e. Menjalankan pengurusan risiko;(tambah berkaitan ICT) f. Menjalankan audit, mengkaji semula, merumus tindakbalas pengurusan agensi berdasarkan hasil penemuan dan menyediakan laporan	*ICTSO*

mengenainya; g. Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada CIO IYRES; h. Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT IYRES; i. Memberi amaran terhadap kemungkinan berlakunya ancaman berbahaya seperti virus dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; j. Mengkaji semula aspek-aspek keselamatan fizikal seperti kemudahan backup dan persekitaran pejabat yang perlu, dengan persetujuan CIO IYRES; k. Melaporkan insiden keselamatan ICT kepada CERT KBS untuk tindakan penyiasatan atau pemulihan serta melaporkan kepada Pasukan Tindak Balas Insiden Keselamatan ICT (GCERT) KBS jika keadaan memerlukan; l. Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan memperakukan langkah-langkah baik pulih dengan segera;dan m. Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT.	
020104 Pentadbir Sistem Aplikasi dan Portal	
Eksekutif Teknologi Maklumat ialah Pentadbir Sistem Aplikasi dan Portal. Peranan dan tanggungjawab Pentadbir Sistem Aplikasi dan Portal adalah seperti berikut: a. Memastikan ketepatan dan kawalan capaian pengguna ICT IYRES berdasarkan kepada Dasar keselamatan ICT IYRES; b. Mengambil tindakan segera dan bersesuaian apabila dimaklumkan terdapat pegawai yang telah tamat perkhidmatan, bertukar, berkursus panjang atau berlaku perubahan dalam bidang tugas;	*ETM*

c. Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat sebagaimana yang telah ditetapkan di dalam DKICT IYRES; d. Memantau aktiviti capaian harian sistem aplikasi; dan e. Memantau penggunaan Sistem Aplikasi dan Portal dan melaporkan kepada ICTSO sekiranya berlaku insiden keselamatan ICT.	
020105 Pentadbir Operasi ICT	
Eksekutif Teknologi Maklumat ialah Pentadbir Operasi ICT IYRES. Peranan dan tanggungjawab Pentadbir Operasi ICT IYRES 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 IYRES; c. Memantau aktiviti capaian harian pengguna ICT IYRES; 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 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 IYRES dan agensi berkaitan beroperasi sepanjang masa; i. Memastikan semua peralatan dan perisian rangkaian diselenggarakan	*ETM*

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 ~~ICTSO~~ Pengurus ICT sekiranya berlaku penyalahgunaan sumber rangkaian; m. Memastikan laluan trafik keluar dan masuk diuruskan secara berpusat dan tidak membenarkan sambungan ke rangkaian IYRES secara tidak sah seperti melalui peralatan modem wireless dan dial-up; 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, Portal, Sistem Pengoperasian server, Pangkalan Data, Sistem emel dan lain-lain yang berkaitan; q. Bertanggungjawab memantau setiap perkakasan ICT yang diagihkan kepada pengguna ICT IYRES seperti komputer peribadi, komputer riba, pencetak, pengimbas dan sebagainya di dalam keadaan yang baik; r. Memastikan ketepatan dan kawalan capaian pengguna ICT IYRES; s. Melaksanakan pengurusan Pusat Data IYRES; dan t. Melaporkan sebarang insiden keselamatan ICT kepada ~~ICTSO.~~ Pengurus ICT dan CIO.	
020106 Pentadbir Pangkalan Data	
Eksekutif Teknologi Maklumat ialah Pentadbir Pangkalan Data. Peranan dan tanggungjawab Pentadbir Pangkalan Data adalah seperti berikut: a. Melaksanakan konfigurasi dan penambahbaikan pangkalan data serta	*ETM*

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 IYRES pangkalan data berdasarkan kepada prinsip-prinsip DKICT IYRES; f. Melaksanakan proses di pangkalan data; dan g. Melaporkan sebarang insiden keselamatan ICT kepada ICTSO.	
020107 Pengguna ICT IYRES	
Semua pengguna ICT IYRES di Institut Penyelidikan dan Pembangunan Belia Malaysia (termasuk pegawai, kakitangan, pembekal, pakar runding dan lain-lain.) ialah pengguna ICT IYRES. Peranan dan tanggungjawab pengguna ICT IYRES adalah seperti berikut: a. Membaca, memahami dan mematuhi Dasar Keselamatan ICT IYRES; b. Mengetahui dan memahami implikasi keselamatan ICT kesan dari tindakannya; c. Melaksanakan prinsip-prinsip Dasar Keselamatan ICT dan menjaga kerahsiaan maklumat IYRES; 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 IYRES. (Lampiran 2)	*Pengguna ICT IYRES*

020108 Jawatankuasa Pemandu ICT (JPICT)	
Jawatankuasa Pemandu ICT (JPICT) adalah jawatankuasa yang bertanggungjawab dalam pelaksanaan ICT dan berperanan sebagai penasihat dan pemangkin dalam merumuskan rancangan dan strategi ICT IYRES. Keanggotaan JPICT IYRES adalah seperti berikut: Pengerusi : Ketua Pegawai Eksekutif Ahli : 1. Eksekutif Penyelidik Kanan I 2. Eksekutif Penyelidik Kanan 2 3. Eksekutif Penyelidik Kanan 3 4. Eksekutif Penyelidik Kanan 4 5. Eksekutif Penyelidik Kanan 5 6. Eksekutif Teknologi Maklumat Kanan 7. Eksekutif Khidmat Pengurusan 8. Penolong Eksekutif Kanan Kewangan Bidang kuasa: a. Memperakukan/Meluluskan dokumen DKICT IYRES; b. Memantau tahap pematuhan keselamatan ICT; c. Menilai aspek teknikal keselamatan projek-projek ICT; d. Memperaku garis panduan, prosedur dan tatacara untuk aplikasi khusus dalam IYRES yang mematuhi keperluan DKICT IYRES; e. Menilai teknologi yang bersesuaian dan mencadangkan penyelesaian terhadap keperluan keselamatan ICT; f. Memastikan DKICT IYRES selaras dengan dasar-dasar ICT kerajaan semasa; g. Menerima laporan dan membincang mengenai keselamatan ICT semasa; dan	

h. Membuat keputusan mengenai tindakan yang perlu diambil mengenai sebarang insiden.	
0202 Pihak Ketiga	**Tindakan**
Objektif Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain).	
020201 Keperluan Keselamatan Kontrak dengan Pihak Ketiga	
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 IYRES; 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 IYRES perlu berlandaskan kepada perjanjian kontrak; e. Memastikan semua syarat keselamatan dinyatakan dengan jelas dalam perjanjian dengan pihak ketiga. Perkara-perkara berikut hendaklah dimasukkan di dalam perjanjian yang dimeterai. i. Dasar Keselamatan ICT IYRES; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. f. Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT	*CIO, Pengurus ICT dan ICTSO*

IYRES (Lampiran 2)	

BIDANG 03 PENGURUSAN ASET	
0301 Akauntabiliti Aset	**Tindakan**
Objektif Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT IYRES.	
030101 Inventori Aset ICT	
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 dikenalpasti dan maklumat aset direkod dalam borang daftar harta modal dan inventori dan sentiasa dikemaskini; b. Memastikan semua aset ICT mempunyai pemilik dan dikendalikan oleh pengguna ICT IYRES yang dibenarkan sahaja; c. Memastikan semua pengguna ICT IYRES mengesahkan penempatan aset ICT yang ditempatkan di IYRES dan agensi berkaitan; d. Peraturan bagi pengendalian aset ICT hendaklah dikenalpasti, didokumen dan dilaksanakan; e. Setiap pengguna ICT IYRES adalah bertanggungjawab ke atas semua aset ICT di bawah kawalannya; dan f. Aset ICT adalah di bawah tanggungjawab Pengawai Aset IYRES mengikut Pekeliling Perbendaharaan semasa yang berkuatkuasa.	*Pegawai Aset IYRES, Pentadbir Operasi ICT dan Pengguna ICT IYRES*

0302 Pengkelasan dan Pengendalian Maklumat	Tindakan
Objektif Memberi dan menyokong perlindungan yang bersesuaian ke atas semua aset ICT IYRES.	
030201 Pengkelasan & Pengendalian Maklumat	
Maklumat hendaklah dikelaskan dan dilabelkan sewajarnya. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang telah ditetapkan di dalam dokumen Arahan Keselamatan seperti berikut: a. Rahsia Besar; b. Rahsia; c. Sulit; atau d. Terhad.	*Pengguna ICT IYRES*
030202 ~~Pengendalian~~ Pengkelasan Maklumat	
Aktiviti pengendalian maklumat seperti mengumpul, memproses, menyimpan, menghantar, menyampai, menukar dan memusnah hendaklah mengambilkira langkah-langkah keselamatan berikut: a. Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; b. Memeriksa maklumat dan menentukan ia tepat dan lengkap dari semasa ke semasa; c. 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 pengwujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan	*Pengguna ICT IYRES*

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

BIDANG 04 PENGURUSAN ASET	
0401 Keselamatan Sumber Manusia Dalam Tugas Harian	**Tindakan**
Objektif Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan IYRES, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua pengguna ICT IYRES hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuatkuasa.	
040101 Sebelum Perkhidmatan	
Perkara-perkara yang mesti dipatuhi adalah seperti-berikut: a. Menyatakan dengan lengkap dan jelas mengenai peranan dan tanggungjawab pegawai dan kakitangan IYRES serta pihak ketiga yang terlibat dalam menjamin keselamatan aset ICT sebelum, semasa dan selepas perkhidmatan; b. Menjalankan tapisan keselamatan untuk pengguna ICT IYRES 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 IYRES*
040102 Dalam Perkhidmatan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan pegawai dan kakitangan IYRES serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh IYRES;	*Pengguna ICT IYRES dan ICTSO*

b. Memastikan latihan kesedaran dan yang berkaitan mengenai pengurusan keselamatan aset ICT diberi kepada pengguna ICT IYRES 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 IYRES serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan yang ditetapkan oleh IYRES; 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 dan latihan pengguna ICT IYRES boleh merujuk kepada Bahagian Pengurusan Sumber Manusia, IYRES.	
040103 Bertukar Atau Tamat Perkhidmatan	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Memastikan semua aset ICT dikembalikan kepada IYRES mengikut peraturan dan/atau terma perkhidmatan yang ditetapkan; dan b. Membatalkan atau menarik balik semua kebenaran capaian ke atas maklumat dan kemudahan mengikut peraturan yang ditetapkan oleh IYRES dan/atau terma perkhidmatan.	*Pengguna ICT IYRES, Pentadbir Operasi ICT dan Pentadbir Sistem Aplikasi dan Portal*

BIDANG 05 KESELAMATAN FIZIKAL DAN PERSEKITARAN	
0501 Keselamatan Kawasan	**Tindakan**
Objektif Melindungi premis, perkakasan, perisian dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.	
050101 Kawalan Kawasan	
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;	*CIO, ICTSO, dan Pengguna ICT IYRES*

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 l. Memastikan kawasan-kawasan penghantaran dan pemunggahan dan juga tempat-tempat lain dikawal dari pihak yang tidak diberi kebenaran memasukinya.	
050102 Kawalan Masuk Fizikal	
Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a. Setiap pengguna ICT IYRES hendaklah memakai atau mengenakan pas keselamatan sepanjang waktu bertugas; b. Semua pas keselamatan hendaklah diserahkan balik kepada IYRES apabila pengguna ICT IYRES berhenti, bertukar keluar atau bersara; c. Setiap pelawat hendaklah mendapatkan Pas Keselamatan Pelawat di ~~pintu~~ kaunter utama KBS dan hendaklah dikembalikan semula selepas tamat lawatan; dan d. Kehilangan pas mestilah dilaporkan dengan segera.	*Pengguna ICT IYRES dan Pelawat*
0502 Keselamatan Peralatan	**Tindakan**
Objektif Melindungi peralatan ICT IYRES dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.	
050201 Peralatan ICT	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna ICT IYRES hendaklah menyemak dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; b. Pengguna ICT IYRES bertanggungjawab sepenuhnya ke atas ~~komputer~~ peralatan ICT masing-masing dan tidak dibenarkan membuat sebarang	*Pengguna ICT IYRES*

pertukaran perkakasan dan konfigurasi yang telah ditetapkan;

c. Pengguna ICT IYRES dilarang sama sekali menambah, menanggal atau mengganti sebarang perkakasan ICT yang telah ditetapkan;

d. Pengguna ICT IYRES dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Operasi ICT;

e. Pengguna ICT IYRES adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya;

f. Pengguna ICT IYRES 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);

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

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 IYRES, perlulah mendapat kelulusan Ketua Jabatan/Ketua Bahagian dan direkodkan bagi tujuan pemantauan;

m. Peralatan ICT yang hilang hendaklah dilaporkan kepada Pegawai Keselamatan ICTSO dan Pegawai Aset dengan segera;

n. Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada

peraturan semasa yang berkuat kuasa; o. Pengguna ICT IYRES 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. Katalaluan Pentadbir (password administrator) dilarang sama sekali diubah oleh pengguna ICT IYRES selain daripada pentadbir yang dipertanggungjawabkan. t. Pengguna ICT IYRES bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan rasmi sahaja; u. Pengguna ICT IYRES hendaklah memastikan semua perkakasan komputer, pencetak, pengimbas dan lain-lain perkakasan ICT dalam dimatikan apabila meninggalkan pejabat; v. Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada Pengurus ICT dan Ketua Jabatan/Bahagian; dan w. Memastikan plag dicabut daripada *main switch* bagi mengelakkan kerosakan perkakasan sebelum meninggalkan pejabat jika berlaku kejadian seperti petir, kilat dan sebagainya.	
050202 Media Storan	
Media storan merupakan peralatan elektronik yang digunakan untuk menyimpan data dan maklumat seperti, *floppy disk*, cakera padat, pita magnetik, *optical disk*,	*Pengguna*

flash disk, CDROM, *thumb drive* dan lain-lain media storan ~~lain~~. 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 IYRES yang dibenarkan sahaja; c. Semua media storan perlu dikawal bagi mencegah dari 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 dari 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.	*ICT IYRES*
050203 Media Tandatangan Digital	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Pengguna ICT IYRES hendaklah bertanggungjawab sepenuhnya ke atas media tandatangan digital bagi melindungi daripada kecurian, kehilangan, kerosakan, penyalahgunaan dan pengklonan;	*Pengguna ICT IYRES*

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.	
050204 Media Perisian dan Aplikasi	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Hanya perisian yang berlesen atau diperakui sahaja dibenarkan bagi kegunaan IYRES; b. Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran pemilik sistem aplikasi; c. Lesen perisian (*registration code, serials key, activation code*) perlu disimpan berasingan daripada *CD-rom* 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 IYRES*
050205 Penyelenggaraan Perkakasan	
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 diselenggara 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; d. Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan;	*Pentadbir Operasi ICT*

e. Memaklumkan pengguna ICT IYRES sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan f. Semua penyelenggaraan mestilah mendapat kebenaran daripada Pengurus ICT.	
050206 Peralatan Di Luar Premis	
Peralatan yang dibawa keluar dari premis IYRES 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 IYRES*
050207 Pelupusan Perkakasan	
Pelupusan melibatkan semua perkakasan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekalkan oleh IYRES dan ditempatkan di IYRES. Perkakasan ICT yang hendak dilupuskan perlu melalui prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan IYRES. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua kandungan perkakasan khususnya maklumat rahsia rasmi hendaklah dihapuskan terlebih dahulu sebelum pelupusan sama ada melalui *shredding, grinding, degauzing* atau pembakaran; b. Sekiranya maklumat perlu disimpan, maka pengguna ICT IYRES bolehlah membuat penduaan; c. Perkakasan ICT yang akan dilupuskan sebelum dipindah-milik hendaklah dipastikan data-data dalam storan telah dihapuskan dengan cara yang selamat;	*Pegawai Aset dan Unit Pengurusan Maklumat, IYRES*

d. Pegawai Aset hendaklah mengenal pasti sama ada perkakasan tertentu boleh dilupuskan atau sebaliknya;

e. Perkakasan yang hendak dilupus 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 IYRES adalah **DILARANG SAMA SEKALI** daripada melakukan perkara-perkara seperti berikut:-

   i. Menyimpan mana-mana perkakasan ICT yang hendak dilupuskan untuk milik peribadi. Mencabut, menanggal 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 IYRES;

   iii. Memindah keluar dari IYRES mana-mana perkakasan ICT yang hendak dilupuskan;

   iv. Melupuskan sendiri perkakasan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab IYRES; 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	Tindakan
Objektif Melindungi asset ICT IYRES dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.	
050301 Kawalan Persekitaran	
Bagi menghindarkan kerosakan dan gangguan terhadap premis dan aset ICT, semua cadangan berkaitan premis sama ada untuk memperoleh, menyewa, ubahsuai, pembelian hendaklah dirujuk 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 (bilik percetakan, peralatan komputer dan ruang atur pejabat dan sebagainya) dengan teliti; b. Semua ruang pejabat khususnya kawasan yang mempunyai kemudahan ICT hendaklah dilengkapi dengan perlindungan keselamatan yang mencukupi dan dibenarkan seperti alat pencegah kebakaran dan pintu kecemasan; c. Peralatan perlindungan hendaklah dipasang di tempat yang bersesuaian, mudah dikenali dan dikendalikan; d. Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; e. Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; f. Pengguna ICT IYRES adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; g. Semua peralatan perlindungan hendaklah disemak dan diuji mengikut	*Pengguna ICT IYRES*

keperluan semasa. 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	
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 c. Semua peralatan sokongan bekalan kuasa hendaklah disemak dan diuji secara berjadual.	*Pentadbir Operasi ICT dan ICTSO*
050303 Kabel	
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	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Setiap pengguna ICT IYRES hendaklah membaca, memahami dan mematuhi prosedur kecemasan dengan merujuk kepada Garis Panduan/Manual Keselamatan IYRES; dan b. Kecemasan persekitaran seperti kebakaran hendaklah dilaporkan kepada Pegawai Keselamatan IYRES/Jabatan yang dilantik mengikut aras.	*Pengguna ICT IYRES dan* *Pegawai Keselamatan IYRES/ Jabatan*
0504 Keselamatan Dokumen	**Tindakan**
Objektif Melindungi maklumat IYRES dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan atau kecuaian.	
050401 Dokumen	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Setiap dokumen hendaklah difail dan dilabelkan mengikut klasifikasi keselamatan seperti Terbuka, Terhad, Sulit, Rahsia atau Rahsia Besar; 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.	*Pengguna ICT IYRES*

BIDANG 06 PENGURUSAN OPERASI DAN KOMUNIKASI	
0601 Pengurusan Prosedur Operasi	**Tindakan**
Objektif Memastikan pengurusan operasi berfungsi dengan betul dan selamat daripada sebarang ancaman dan gangguan.	
060101 Pengendalian Prosedur	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Semua prosedur pengurusan operasi yang diwujud, 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 IYRES*
060102 Kawalan Perubahan	
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 terlebih dahulu; b. Aktiviti-aktiviti seperti memasang, menyelenggara, 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	*Pengguna ICT IYRES*

d. Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	
060103 Pengasingan Tugas dan Tanggungjawab	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; b. Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan c. Perkakasan yang digunakan bagi tugas membangun, mengemas kini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	*CIO dan ICTSO*
0602 Pengurusan Penyampaian Perkhidmatan Pihak Ketiga	**Tindakan**
Objektif Memastikan pelaksanaan dan penyelenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.	
060201 Perkhidmatan Penyampaian	
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	*Pengguna ICT IYRES*

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.	
0603 Perancangan dan Penerimaan Sistem	**Tindakan**
Objektif Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.	
060301 Perancangan Kapasiti	
Kapasiti sesuatu komponen atau sistem ICT hendaklah dirancang, diurus dan dikawal dengan teliti oleh pegawai yang berkenaan bagi memastikan keperluannya adalah mencukupi dan bersesuaian untuk pembangunan dan kegunaan sistem ICT pada masa akan datang. Keperluan kapasiti ini juga perlu mengambil kira ciri-ciri keselamatan ICT bagi meminimumkan risiko seperti gangguan pada perkhidmatan dan kerugian akibat pengubahsuaian yang tidak dirancang.	*ICTSO, Pentadbir Sistem Aplikasi dan Portal ICT, Pentadbir Operasi ICT dan Pentadbir Pangkalan Data*
060302 Penerimaan Sistem	
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	**Tindakan**
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	
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 berkuatkuasa; 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 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; h. Mengadakan program dan prosedur jaminan kualiti ke atas semua perisian yang dibangunkan; dan i. Memberi amaran kepada pengguna ICT IYRES mengenai ancaman keselamatan ICT seperti serangan virus;	*Pengguna ICT IYRES*
060402 Perlindungan dari Mobile Code	
Penggunaan *Mobile Code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan.	*Pengguna ICT IYRES*

0605 Housekeeping	**Tindakan**
Objektif Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.	
060501 *Backup*	
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. Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	*Pengguna ICT IYRES*
0606 Pengurusan Rangkaian	**Tindakan**
Objektif Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.	
060601 Kawalan Infrastruktur Rangkaian	
Infrastruktur Rangkaian mestilah dirancang, disedia, dibangun, dikawal dan diuruskan sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Pengurusan Rangkaian IYRES dikendalikan oleh pihak BPM, KBS. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	*ICTSO dan Pentadbir Operasi ICT*

a. Tanggungjawab atau kerja-kerja operasi rangkaian dan komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;

b. Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti pencerobohan, haiwan perosak, banjir, gegaran dan habuk;

c. Capaian kepada peralatan rangkaian hendaklah dikawal dan terhad kepada pengguna ICT IYRES yang dibenarkan sahaja;

d. Semua peralatan mestilah melalui proses *Factory Acceptance Check* (FAC) semasa pemasangan dan konfigurasi;

e. *Firewall* hendaklah dipasang serta di konfigurasi dan diselia oleh Pentadbir Operasi ICT;

f. Semua trafik keluar dan masuk hendaklah melalui *firewall* di bawah kawalan BPM, KBS;

g. Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna ICT IYRES 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 IYRES;

i. Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

j. Sebarang penyambungan rangkaian yang bukan di bawah kawalan IYRES adalah tidak dibenarkan;

k. Semua pengguna ICT IYRES hanya dibenarkan menggunakan rangkaian KBS sahaja dan penggunaan modem adalah dilarang sama sekali; dan

l. Kemudahan bagi *wireless* LAN perlu dipastikan kawalan keselamatan.

0607 Pengurusan Media	Tindakan
Objektif Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.	
060701 Penghantaran dan Pemindahan	
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran daripada Ketua Jabatan terlebih dahulu.	*Pengguna ICT IYRES*
060702 Prosedur Pengendalian Media	
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 IYRES 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 prosedur yang betul dan selamat.	*Pengguna ICT IYRES*
060703 Keselamatan Sistem Dokumentasi	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan sistem dokumentasi adalah seperti berikut : a. Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri	*Pengguna ICT IYRES*

keselamatan; b. Menyedia dan memantapkan keselamatan sistem dokumentasi; dan c. Mengawal dan merekodkan semua aktiviti capaian dokumentasi sedia ada.	
0608 Pengurusan Pertukaran Maklumat	**Tindakan**
Objektif Memastikan keselamatan pertukaran maklumat dan perisian antara IYRES dan agensi luar terjamin.	
060801 Pertukaran Maklumat	
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 IYRES dengan agensi luar; c. Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari IYRES; dan d. Maklumat yang terdapat dalam mel elektronik perlu dilindungi sebaik-baiknya.	*Pengguna ICT IYRES*
060802 Pengurusan Mel Elektronik (E-mel)	
Penggunaan e-mel di IYRES 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.	*Pengguna ICT IYRES dan Pentadbir Operasi ICT*

Perkara-perkara yang perlu dipatuhi dalam pengendalian mel elektronik adalah seperti berikut : a. Akaun atau alamat Mel elektronik (e-mel) yang diperuntukkan oleh IYRES 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 IYRES; 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 IYRES hendaklah menentukan tarikh dan masa sistem komputer adalah tepat; h. Respons ke atas e-mel dengan cepat dan mengambil tindakan segera; i. Pengguna ICT IYRES hendaklah memastikan alamat e-mel persendirian (seperti yahoo.com, gmail.com, streamyx.com.my dan sebagainya) tidak boleh digunakan untuk tujuan rasmi; dan j. Pengguna ICT IYRES hendaklah bertanggungjawab ke atas pengemaskinian dan penggunaan *mailbox* masing-masing.	
0609 Perkhidmatan E-Dagang *(Electronic Commerce Services)*	**Tindakan**
Objektif Memastikan keselamatan pertukaran maklumat dan perisian antara IYRES dan agensi luar terjamin.	

060901 E-Dagang	
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 IYRES*
060902 Maklumat Umum	
Perkara-perkara yang perlu dipatuhi dalam memastikan keselamatan maklumat adalah seperti berikut : a. Memastikan perisian, data dan maklumat dilindungi dengan mekanisma 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 disah dan diluluskan sebelum dimuat naik ke laman web/portal.	*Pengguna ICT IYRES*

0610 Pemantauan	Tindakan
Objektif Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.	
061001 Pengauditan dan Forensik ICT	
ICTSO mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: a. Sebarang percubaan pencerobohan kepada sistem ICT IYRES; 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.	*Pentadbir Operasi ICT dan ICTSO*
061002 Jejak Audit	
Setiap sistem mestilah mempunyai jejak audit. Jejak audit merekod aktiviti-aktiviti yang berlaku dalam sistem aplikasi secara kronologi bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan	*Pentabdir Sistem Aplikasi dan Portal,*

dalam sesuatu transaksi. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: a. Rekod setiap aktiviti transaksi; b. Maklumat jejak audit mengandungi identiti pengguna ICT IYRES, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; c. Aktiviti capaian pengguna ICT IYRES 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 membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	*Pentadbir Operasi ICT dan ICTSO*
061003 Sistem Log	
Pentadbir Sistem Aplikasi dan Portal dan Pentadbir Operasi ICT hendaklah melaksanakan perkara-perkara berikut: a. Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna ICT IYRES; 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, Pentadbir Sistem Aplikasi dan Portal hendaklah melaporkan kepada ICTSO dan CIO.	*Pentadbir Sistem Aplikasi dan Portal, Pentadbir Operasi ICT, dan ICTSO*

061004 Pemantauan Log	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: a. Log Audit yang merekodkan semua aktiviti perlu dihasilkan dan disimpan untuk tempoh masa yang dipersetujui bagi membantu siasatan dan memantau kawalan capaian; b. Prosedur untuk memantau penggunaan kemudahan memproses maklumat perlu di wujud dan hasilnya perlu dipantau secara berkala; c. Kemudahan merekod dan maklumat log perlu dilindungi daripada diubahsuai dan sebarang capaian yang tidak dibenarkan; d. Aktiviti pentadbiran dan operator sistem perlu direkodkan; e. Kesalahan, kesilapan dan / atau penyalahgunaan perlu dilog, dianalisis dan diambil tindakan sewajarnya; dan f. Waktu yang berkaitan dengan sistem pemprosesan maklumat dalam IYRES atau domain keselamatan perlu diselaraskan dengan satu sumber waktu yang dipersetujui.	*Pentadbir Operasi ICT dan ICTSO*

BIDANG 07 KAWALAN CAPAIAN	
0701 Dasar Kawalan Capaian	**Tindakan**
Objektif Mengawal capaian ke atas maklumat.	
070101 Keperluan Kawalan Capaian	
Capaian kepada proses dan maklumat hendaklah dikawal mengikut keperluan keselamatan dan fungsi kerja pengguna ICT IYRES yang berbeza. Ia perlu direkodkan, dikemas kini dan menyokong dasar kawalan capaian pengguna ICT IYRES 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 IYRES; 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 Sistem Aplikasi dan Portal,* *Pentadbir Operasi ICT*
0702 Pengurusan Capaian Pengguna ICT IYRES	**Tindakan**
Objektif Mengawal capaian pengguna ICT IYRES ke atas aset ICT IYRES.	
070201 Akaun Pengguna ICT IYRES	
Pengguna ICT IYRES adalah bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna ICT IYRES dan aktiviti yang	*Pentadbir Operasi ICT,*

dilakukan, perkara-perkara berikut hendaklah dipatuhi: a. Akaun yang diperuntukkan oleh IYRES sahaja boleh digunakan; b. Akaun pengguna ICT IYRES mestilah unik dan hendaklah mencerminkan identiti pengguna ICT IYRES; c. Akaun pengguna ICT IYRES yang diwujudkan pertama kali akan diberi tahap capaian paling minimum iaitu untuk melihat dan membaca sahaja. Sebarang perubahan tahap capaian hendaklah mendapat kelulusan daripada pemilik sistem ICT terlebih dahulu; d. Pemilikan akaun pengguna ICT IYRES bukanlah hak mutlak seseorang dan ia tertakluk kepada peraturan IYRES. 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 IYRES atas sebab-sebab berikut: i. Pengguna ICT IYRES yang bercuti panjang dalam tempoh waktu melebihi dua (2) minggu; ii. Bertukar bidang tugas kerja; iii. Bertukar ke agensi lain; iv. Bersara; atau v. Ditamatkan perkhidmatan.	*Pentadbir Sistem Aplikasi dan Portal, Pentadbir Pangkalan Data,* *Pemilik Sistem Aplikasi dan Portal*
070202 Hak Capaian	
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, Pemilik Sistem Aplikasi dan*

	Portal
070203 Pengurusan Kata Laluan	
Pemilihan, penggunaan dan pengurusan kata laluan sebagai laluan utama bagi mencapai maklumat dan data dalam sistem mestilah mematuhi amalan terbaik serta prosedur yang ditetapkan oleh IYRES seperti berikut: a. Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; b. Pengguna ICT IYRES hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau di kompromi; c. Panjang kata laluan mestilah sekurang-kurangnya lapan (8) 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; 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 IYRES; i. Tentukan had masa pengesahan selama dua (2) minit (mengikut kesesuaian sistem) dan selepas had itu, sesi ditamatkan; j. Kata laluan hendaklah ditukar selepas 90 hari atau selepas tempoh masa bersesuaian; dan k. Mengelakkan penggunaan semula kata laluan yang baru digunakan.	*Pengguna ICT IYRES dan* *Pentadbir Sistem Aplikasi dan Portal*
070204 *Clear Desk* dan *Clear Screen*	
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan	*Pengguna ICT IYRES*

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 IYRES atau di paparan skrin apabila pengguna ICT IYRES 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 dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	
0703 Kawalan Capaian Rangkaian	**Tindakan**
Objektif Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.	
070301 Capaian Rangkaian	
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: a. Menempatkan atau memasang antara muka yang bersesuaian di antara rangkaian IYRES, rangkaian agensi lain dan rangkaian awam; b. Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna ICT IYRES dan peralatan yang menepati kesesuaian penggunaannya; dan c. Memantau dan menguatkuasakan kawalan capaian pengguna ICT IYRES terhadap perkhidmatan rangkaian ICT.	*ICTSO dan Pentadbir Operasi ICT*
070302 Capaian Internet	
Perkara-perkara yang perlu dipatuhi adalah seperti berikut : a. Penggunaan Internet di IYRES adalah tertakluk sepertimana polisi	*Pentadbir Operasi ICT*

Capaian Internet DKICT 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 IYRES;

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 c onferencing*, *video streaming, chat, downloading*) adalah perlu bagi menguruskan penggunaan *bandwidth* yang maksimum dan lebih berkesan;

d. Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. Pengurus ICT berhak menentukan pengguna ICT IYRES 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 IYRES 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 IYRES;

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. Pengguna ICT IYRES 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	**Tindakan**
Objektif Menghalang capaian tidak sah dan tanpa kebenaran ke atas sistem pengoperasian.	
070401 Capaian Sistem Pengoperasian	
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 IYRES yang dibenarkan; b. Merekodkan capaian yang berjaya dan gagal. c. Membekalkan kemudahan untuk pengesahan; d. Bagi sistem, kata laluan kunci digunakan, kualiti kata kunci perlu mendapat pengesahan; dan e. Menghadkan masa penggunaan rangkaian bagi pengguna ICT IYRES. Kaedah-kaedah yang digunakan hendaklah mampu menyokong perkara-perkara	*Pentadbir Sistem Keselamatan ICT dan ICTSO*

berikut: a. Mengesahkan pengguna ICT IYRES yang dibenarkan; b. Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna ICT IYRES 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 IYRES dan hanya digunakan oleh pengguna ICT IYRES 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	
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 IYRES*

0705 Kawalan Capaian Sistem Aplikasi dan Maklumat	Tindakan
Objektif Menghalang capaian tidak sah dan tanpa kebenaran ke atas maklumat yang terdapat di dalam sistem aplikasi.	
070501 Capaian Sistem Aplikasi dan Maklumat	
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari sebarang bentuk capaian yang tidak dibenarkan yang boleh menyebabkan ~~kerosakan~~ kelumpuhan sistem. Bagi memastikan kawalan capaian sistem aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: a. Pengguna ICT IYRES 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 IYRES hendaklah direkodkan (sistem log); c. Mengehadkan capaian sistem aplikasi kepada tiga (3) kali percubaan. Sekiranya gagal, akaun atau kata laluan pengguna ICT IYRES akan disekat; d. Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan e. Capaian dari luar ke atas sistem sistem aplikasi dan maklumat adalah digalakkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	*Pentadbir Sistem, Pentadbir Operasi ICT dan ICTSO*
0706 Peralatan Mudah Alih dan Kerja Jarak Jauh	**Tindakan**
Objektif Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih	

dan kemudahan kerja jarak jauh	
070601 Peralatan Mudah Alih	
Perkara yang perlu dipatuhi adalah seperti berikut : a. Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	*Pengguna ICT IYRES*
070602 Kerja Jarak Jauh	
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.	*Pengguna ICT IYRES*

BIDANG 08 PEROLEHAN, PEMBANGUNAN DAN PENYELENGGARAAN SISTEM APLIKASI	
0801 Keselamatan Dalam Membangunkan Sistem Komputer dan Aplikasi	**Tindakan**
Objektif Memastikan sistem aplikasi yang dibangunkan secara dalaman atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.	
080101 Keperluan Keselamatan Sistem Maklumat	
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 validasi 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 berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	*Pemilik Sistem Aplikasi dan portal,* *Pentadbir Sistem Aplikasi dan Portal, Pentadbir Operasi ICT dan ICTSO*

BIDANG 09 PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN	
0901 Mekanisme Pelaporan Insiden Keselamatan ICT	**Tindakan**
Objektif Memastikan insiden dikendalikan dengan cepat dan berkesan bagi meminimumkan kesan insiden keselamatan ICT.	
090101 Mekanisme Pelaporan	
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 GCERT MAMPU 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	*Pengguna ICT IYRES*

yang tidak dijangka. Dalam keadaan atau persekitaran berisiko tinggi, CIO hendaklah melaporkan kepada KPE 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 b. Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	
0902 Pengurusan Maklumat Insiden Keselamatan ICT	**Tindakan**
Objektif Memastikan pendekatan yang konsisten dan efektif digunakan dalam pengurusan maklumat insiden keselamatan ICT.	
090201 Pengurusan Maklumat Insiden Keselamatan ICT	
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 IYRES. 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	*CERT KBS*

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.	

BIDANG 10 PENGURUSAN KESINAMBUNGAN PERKHIDMATAN	
1001 Dasar Kesinambungan Perkhidmatan	**Tindakan**
Objektif Menjamin operasi perkhidmatan berjalan lancar dan penyampaian perkhidmatan yang berterusan kepada pelanggan.	
100101 Pelan Kesinambungan Perkhidmatan	
Pelan Kesinambungan Perkhidmatan (BCM) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Pelan ini mestilah diluluskan oleh JPICT IYRES. 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 IYRES mengenai prosedur kecemasan;	*CIO*

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.

Pelan BCM yang dibangunkan hendaklah mengandungi perkara-perkara berikut:

a. Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan;

b. Senarai personel IYRES dan vendor berserta nombor yang boleh dihubungi (faksimili, 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;

d. Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan

e. Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan.

Salinan pelan BCM 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 pelan BCM hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui tanggungjawab dan peranan mereka apabila pelan dilaksanakan.

BIDANG 11 PEMATUHAN	
1101 Pematuhan dan Keperluan Perundangan	**Tindakan**
Objektif Meningkatkan tahap keselamatan ICT bagi mengelak dari pelanggaran kepada Dasar Keselamatan ICT IYRES.	
110101 Pematuhan Dasar	
Setiap pengguna ICT IYRES perlu membaca, memahami dan mematuhi Dasar Keselamatan ICT IYRES dan undang-undang atau peraturan-peraturan lain berkaitan yang berkuat kuasa. Semua aset ICT IYRES adalah hak milik Kerajaan dan di bawah pengawalan Ketua Pegawai Eksekutif (KPE). Pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna ICT IYRES untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. Sebarang penggunaan aset ICT IYRES selain daripada maksud dan tujuan yang telah ditetapkan adalah merupakan satu penyalahgunaan sumber IYRES.	*Pengguna ICT IYRES*
110102 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal	
ICTSO perlu memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. Sistem ICT perlu melalui pemeriksaan secara berkala bagi mematuhi standard pelaksanaan keselamatan.	*ICTSO*
110103 Pematuhan Keperluan Audit	
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	*Pengguna ICT IYRES*

gangguan dalam penyediaan perkhidmatan. Capaian ke atas peralatan audit sistem ICT perlu dipelihara dan diselia bagi mengelakkan berlaku penyalahgunaan	
110104 Keperluan Perundangan	
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna ICT IYRES di IYRES: 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	*Pengguna ICT IYRES*

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 IYRES; w. Garis Panduan Pelaksanaan Blog Bagi Agensi Sektor Awam 2009; dan x. Pekeliling/Arahan/Garis Panduan yang berkuat kuasa dari semasa ke semasa.	
110105 Pelanggaran Dasar	
Pelanggaran Dasar Keselamatan ICT IYRES boleh dikenakan tindakan tatatertib dan/atau perundangan.	*Pengguna ICT IYRES*

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).
GCERT	*Government Computer Emergency Response Team* Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab merupakan peranti yang menghubungkan dua atau lebih stesen kerja menjadi suatu topologi bas berbentuk bintang dan menyiarkan (broadcast) data yang diterima daripada sesuatu port kepada semua port yang lain.
ICT	*Information and Communication Technology.*

GLOSARI

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,

GLOSARI

	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.

GLOSARI

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.