DASAR KESELAMATAN ICT

KEMENTERIAN LUAR NEGERI

28 DISEMBER 2010

Telah diluluskan pada Mesyuarat JPICT Bil. 1/2011 bertarikh 28 Mac 2011

Versi 2.0

Kandungan **Muka Surat**

PENGENALAN

Pembangunan Dasar Keselamatan ICT di Kementerian Luar Negeri (KLN) adalah selaras dengan arahan yang dikeluarkan melalui Surat Pekeliling Am Bilangan 3 Tahun 2000 bertajuk "Rangka Dasar Keselamatan Teknologi Maklumat Dan Komunikasi Kerajaan" yang mengarahkan semua agensi Kerajaan mematuhi Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan.

Dasar Keselamatan ICT KLN ini mengandungi peraturan-peraturan yang mesti dibaca dan dipatuhi dalam menggunakan aset teknologi maklumat dan komunikasi (ICT) KLN. Dasar ini juga menerangkan kepada semua pengguna di KLN mengenai tanggungjawab dan peranan mereka dalam melindungi aset ICT KLN.

OBJEKTIF

Dasar Keselamatan ICT KLN diwujudkan untuk memastikan tahap keselamatan ICT KLN terurus dan bagi menjamin kesinambungan urusan KLN dengan meminimumkan kesan insiden keselamatan ICT.

Objektif utama Keselamatan ICT KLN ialah seperti berikut:

(a) Memastikan kelancaran operasi KLN dan meminimumkan kerosakan, kehilangan 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;

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

(d) Meningkatkan keupayaan baik pulih di peringkat peralatan, sistem dan organisasi; dan

(e) Menyediakan saluran dan persekitaran yang selamat bagi semua komunikasi secara elektronik.

PENYATAAN 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 masa ke semasa untuk menjamin keselamatan kerana ancaman dan kelemahan sentiasa berubah.

Keselamatan ICT adalah bermaksud keadaan di mana 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 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; dan
(d) Memastikan akses hanya kepada pengguna-penguna yang sah atau penerimaan maklumat dari sumber yang sah.

Dasar keselamatan ICT KLN 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:

Ciri	Penerangan
Kerahsiaan (*Confidential*)	Maklumat tidak boleh didedahkan sewenang-wenangnya atau dibiarkan diakses tanpa kebenaran
Integriti (*Integrity*)	Data dan maklumat hendaklah tepat, lengkap dan kemas kini. Ia hanya boleh diubah dengan cara yang dibenarkan
Tidak Boleh Disangkal (*Non-Repudiation*)	Punca data dan maklumat hendaklah dari punca yang sah dan tidak boleh disangkal
Kesahihan (*Validity*)	Data dan maklumat hendaklah dijamin kesahihannya
Ketersediaan	Data dan maklumat hendaklah boleh diakses pada bila-bila

(*Availability*)	masa

Selain dari itu, langkah-langkah ke arah menjamin keselamatan ICT hendaklah bersandarkan kepada

(a) polisi dan prosidur serta penilaian yang bersesuaian dengan perubahan semasa terhadap kelemahan semula jadi aset ICT;
(b) ancaman yang wujud akibat daripada kelemahan tersebut;
(c) risiko yang mungkin timbul; dan
(d) langkah-langkah pencegahan sesuai yang boleh diambil untuk menangani risiko berkenaan.

SKOP

Dasar Keselamatan ICT KLN ini merangkumi perlindungan terhadap semua bentuk maklumat kerajaan yang dimasukkan, diwujudkan, dimusnah, disimpan, dijana, dicetak, diakses, diedar, disalin, dalam penghantaran dan yang dibuat salinan. 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 KLN.

Contoh komputer, *server*, peralatan komunikasi dan sebagainya;

(b) Perisian dan Aplikasi

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 KLN;

(c) Perkhidmatan

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

Contohnya:

(i) Perkhidmatan rangkaian seperti LAN, WAN dan lain-lain;

(ii) Sistem kawalan 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 KLN.

Contohnya, prosedur operasi, sistem dokumentasi, rekod-rekod KLN, profil-profil pelanggan, pangkalan data dan fail-fail data, maklumat-maklumat arkib dan lain-lain;

(e) Sumber Manusia

Individu yang mempunyai pengetahuan dan kemahiran untuk melaksanakan skop kerja harian di KLN 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.

PRINSIP-PRINSIP KESELAMATAN ICT

Prinsip-prinsip yang menjadi asas kepada Dasar Keselamatan ICT KLN dan perlu dipatuhi adalah seperti berikut:

(a) Akses Atas Dasar "perlu mengetahui"

Akses terhadap penggunaan aset ICT hanya diberikan untuk tujuan spesifik dan dihadkan kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja.

Ini bermakna akses hanya akan diberikan mengikut peranan dan fungsi mereka yang memerlukan maklumat tersebut. Pertimbangan untuk akses adalah berdasarkan kategori maklumat seperti yang dinyatakan di dalam Dokumen Arahan Keselamatan perenggan 53, muka surat 15 ;

(b) Hak Akses Minimum

Hak akses pengguna hanya diberi pada tahap yang paling minimum iaitu untuk dibaca dan/atau dilihat sahaja. Kelulusan adalah perlu untuk membolehkan pengguna mewujud, menyimpan, mengemaskini, mengubah atau membatalkan sesuatu maklumat. Hak akses adalah dikaji dari semasa ke semasa berdasarkan kepada peranan dan tanggungjawab pengguna (bidang tugas);

(c) Akauntabiliti

Semua pengguna adalah bertanggungjawab di atas semua tindakannya terhadap aset ICT di KLN. Tanggungjawab ini perlu dinyatakan dengan jelas sesuai dengan tahap sensitiviti sesuatu sumber ICT. Untuk menentukan tanggungjawab ini dipatuhi, sistem ICT hendaklah mampu menyokong kemudahan mengesan atau mengesah bahawa pengguna sistem maklumat boleh dipertanggungjawabkan atas tindakan mereka.

Akauntabiliti atau tanggungjawab pengguna termasuklah:

- Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan;
- Memeriksa maklumat dan menentukan ianya tepat dan lengkap dari semasa ke semasa;

- Menentukan maklumat sedia untuk digunakan;
- Menjaga kerahsiaan kata laluan;
- Mematuhi standard, prosedur, langkah dan garis panduan keselamatan yang ditetapkan;
- Memberi perhatian kepada maklumat terperingkat terutama semasa pewujudan, pemprosesan, penyimpanan, penghantaran, penyampaian, pertukaran dan pemusnahan; dan
- Menjaga kerahsiaan langkah-langkah keselamatan ICT dari diketahui umum.

(d) Pengasingan

Tugas mewujud, memadam, mengemaskini, mengubah dan mengesahkan data perlu diasingkan bagi mengelak daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau manipulasi. 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 ICT. Oleh 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 KLN hendaklah dibaca, difahami dan dipatuhi bagi mengelakkan sebarang perlanggaran ke atasnya yang boleh membawa ancaman keselamatan ICT;

(g) Pemulihan

Pemulihan sistem amat perlu untuk memastikan 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 Bergantung

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

PENILAIAN RISIKO KESELAMATAN MAKLUMAT

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

Pelaksanaan penilaian risiko keselamatan ICT hendaklah dilakukan secara berkala dan berterusan bergantung kepada perubahan teknologi dan keperluan keselamatan ICT semasa. Seterusnya tindakan susulan dan/atau langkah-langkah bersesuaian perlulah diambil bagi mengurangkan atau mengawal risiko keselamatan ICT berdasarkan penemuan penilaian risiko.

Pelaksanaan penilaian risiko keselamatan ICT hendaklah dilakukan ke atas sistem maklumat KLN 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.

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

KLN perlu mengenalpasti 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 kritera 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.

PERKARA 01

PEMBANGUNAN DAN PENYELENGGARAAN DASAR

01-01 Dasar Keselamatan ICT KLN

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

01-01-01 Pelaksanaan Dasar

Keterangan	T/jawab
Ketua Setiausaha KLN adalah bertanggungjawab ke atas pelaksanaan arahan dengan dibantu oleh Ketua Pegawai Maklumat (CIO), Pegawai Keselamatan ICT (ICTSO) dan ahli pasukan CERT KLN.	Ketua Setiausaha KLN

01-01-02 Penyebaran Dasar

Keterangan	T/jawab
Dasar ini perlu disebarkan kepada semua pengguna KLN (termasuk kakitangan, pembekal, pakar runding dan lain-lain individu yang berurusan dengan KLN).	ICTSO

01-01-03 Penyelenggaraan Dasar

Keterangan	T/jawab
Dasar Keselamatan ICT KLN adalah tertakluk kepada semakan dan pindaan dari semasa ke semasa selaras dengan perubahan teknologi, aplikasi, prosedur, perundangan, dasar Kerajaan dan kepentingan sosial. Prosedur penyelenggaraan Dasar Keselamatan ICT KLN adalah seperti berikut: (a) Mengkaji semula dasar ini sekurang-kurangnya sekali setahun sekali atau mengikut keperluan bagi mengenal pasti dan menentukan perubahan yang diperlukan; (b) Cadangan pindaan perlu dibentangkan di Mesyuarat Jawatankuasa Pemandu ICT (JPICT) KLN untuk mendapatkan kelulusan ; dan (c) Memaklumkan perubahan dasar yang telah dipersetujui oleh JPICT kepada semua pengguna KLN.	ICTSO

01-01-04 Pemakaian dan Pengecualian Dasar	
Keterangan	**T/jawab**
Dasar ini adalah terpakai kepada semua pengguna di KLN termasuk kakitangan, pembekal dan pakar runding yang mengurus, menyelenggara, memproses, mencapai, memuat turun, menyedia, memuat naik, berkongsi, menyimpan dan menggunakan aset ICT KLN dan tiada pengecualian diberikan. Sebarang pengecualian hendaklah mendapatkan kelulusan secara bertulis daripada KSU.	Semua pengguna ICT KLN

PERKARA 02

ORGANISASI KESELAMATAN

02-01 Infrastruktur Organisasi Dalaman

Objektif:
Menerangkan peranan dan tanggungjawab individu/kumpulan yang terlibat dengan lebih jelas dan teratur dalam mencapai objektif keselamatan ICT KLN.

02-01-01 Ketua Setiausaha KLN

Keterangan	T/jawab
Peranan dan tanggungjawab Ketua Setiausaha KLN adalah seperti berikut: (a) Menubuhkan pasukan khusus untuk pengurusan insiden keselamatan selaras dengan Surat Pekeliling Am Bil. 4 Tahun 2006: Garis Panduan Pengurusan Pengendalian Insiden Keselamatan ICT Sektor Awam. (b) Memastikan semua pengguna memahami dan mematuhi peruntukan-peruntukan di bawah Dasar Keselamatan ICT KLN; (c) Memastikan semua keperluan KLN (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 KLN.	Ketua Setiausaha KLN

02-01-02 Ketua Pegawai Maklumat (CIO)

Keterangan	T/jawab
Ketua Pegawai Maklumat (CIO) KLN ialah Timbalan Ketua Setiausaha III, Jabatan Khidmat Pengurusan, KLN. Peranan dan tanggungjawab CIO adalah seperti berikut: (a) Membantu Ketua Setiausaha KLN dalam melaksanakan tugas-tugas yang melibatkan keselamatan ICT; (b) Menentukan keperluan keselamatan ICT disediakan bagi tujuan pelaksanaan dasar-dasar ICT KLN; (c) Menyelaras pembangunan dan pelaksanaan pelan latihan dan program kesedaran mengenai keselamatan ICT; dan (d) Bertanggungjawab ke atas perkara-perkara yang berkaitan dengan keselamatan ICT KLN. (e) Memperakui pengambilan tindakan tatatertib kepada Lembaga Tatatertib KLN ke atas kesalahan yang berkaitan keselamatan	CIO

ICT kepada Lembaga Tatatertib KLN.	
02-01-03 Pengurus ICT	
Keterangan	**T/jawab**
Pengurus ICT bagi KLN ialah Setiausaha Bahagian ICT KLN. Peranan dan tanggungjawab Pengurus ICT adalah seperti berikut: (a) Mengkaji dan melaksanakan kawalan keselamatan ICT selaras dengan dasar dan keperluan KLN; (b) Menentukan kawalan akses pengguna terhadap aset ICT KLN; (c) Melaporkan sebarang perkara atau penemuan mengenai keselamatan ICT kepada ICTSO; dan (d) Menyimpan rekod, bahan bukti dan laporan terkini mengenai ancaman keselamatan ICT KLN.	
02-01-04 Pegawai Keselamatan ICT (ICTSO)	
Keterangan	**T/jawab**
ICTSO KLN adalah Timbalan Setiausaha Bahagian ICT. Peranan dan tanggungjawab adalah seperti berikut: (a) Menguruskan keseluruhan program-program keselamatan ICT KLN; (b) Menguatkuasakan dan memantau pematuhan Dasar Keselamatan ICT KLN; (c) Mewujudkan garis panduan dan prosedur selaras dengan keperluan Dasar Keselamatan ICT KLN; (d) Memberi penerangan dan pendedahan berkenaan Dasar Keselamatan ICT KLN kepada semua pengguna; (e) Menyedia dan melaksanakan program-program kesedaran mengenai keselamatan ICT kepada semua pengguna; (f) Menjalankan pengurusan risiko; (g) Menjalankan penilaian, audit, mengkaji semula dan merumus tindak balas pengurusan berdasarkan hasil penemuan dan menyediakan laporan mengenainya; (h) Memberi amaran terhadap kemungkinan berlakunya ancaman keselamatan siber dan memberi khidmat nasihat serta menyediakan langkah-langkah perlindungan yang bersesuaian; (i) Melaporkan insiden keselamatan ICT kepada Pasukan Tindak balas Insiden Keselamatan ICT (GCERT) MAMPU dan memaklumkan kepada CIO;	ICTSO

(j) Bekerjasama dengan semua pihak yang berkaitan dalam mengenal pasti punca ancaman atau insiden keselamatan ICT dan melakukan langkah-langkah baik pulih dengan segera; dan (k) Mencadangkan pengambilan tindakan tatatertib ke atas pengguna yang melanggar Dasar Keselamatan ICT KLN.	

02-01-05 Pentadbir Sistem ICT	
Keterangan	**T/jawab**
Pentadbir Sistem ICT adalah Pegawai Teknologi Maklumat dan Penolong Pegawai Teknologi Maklumat di Bahagian ICT KLN, SEARCCT dan IDFR. Peranan dan tanggungjawab adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT KLN; (b) Memastikan kerahsiaan aset ICT bagi kata laluan, maklumat konfigurasi dan pengalamatan IP; (c) Mengambil tindakan yang bersesuaian dengan segera apabila dimaklumkan mengenai kakitangan yang berhenti, bertukar, bercuti, berkursus panjang atau berlaku perubahan dalam bidang tugas; (d) Menentukan ketepatan dan kesempurnaan sesuatu tahap capaian berdasarkan arahan pemilik sumber maklumat; (e) Memantau aktiviti capaian harian sistem aplikasi pengguna; (f) Mengenal pasti aktiviti-aktiviti tidak normal seperti pencerobohan dan pengubahsuaian data tanpa kebenaran dan membatalkan atau memberhentikannya dengan serta merta; (g) Menganalisis dan menyimpan rekod jejak audit; (h) Menyediakan laporan mengenai aktiviti capaian secara berkala;	Pentadbir Sistem ICT

02-01-06 Pengguna ICT KLN	
Keterangan	**T/jawab**
Peranan dan tanggungjawab adalah seperti berikut: (a) Membaca, memahami dan mematuhi Dasar Keselamatan ICT KLN; (b) Mengetahui dan memahami implikasi keselamatan ICT serta kesan dari pencerobohan/kebocoran maklumat; (c) Menjalani tapisan keselamatan sekiranya dikehendaki berurusan dengan maklumat rasmi terperingkat;	Semua Pengguna ICT KLN

(d) Melaksanakan prinsip-prinsip Dasar Keselamatan ICT KLN dan menjaga kerahsiaan maklumat kerajaan; (e) Mematuhi dasar, standard, prosedur/tatacara dan garis panduan keselamatan yang ditetapkan; (f) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT KLN seperti di **Lampiran 1**; dan (g) Melaporkan sebarang aktiviti yang mengancam keselamatan ICT kepada ICTSO dengan segera.	

02-01-07Pasukan Tindak Balas Insiden Keselamatan ICT KLN (CERT KLN)	
Keterangan	**T/jawab**
Keanggotaan CERT KLN adalah seperti berikut: Pengarah CERT: Ketua Pegawai Maklumat - Timbalan Ketua Setiausaha III, Kementerian Luar Negeri Timbalan Pengarah CERT: Pengurus Komputer - SUB ICT, Kementerian Luar Negeri Pengurus CERT: Pegawai Keselamatan ICT (ICTSO) – Timbalan SUB ICT, Kementerian Luar Negeri Ahli-ahli lain yang dilantik: Ketua Penolong Setiausaha MEED, Kementerian Ketua Penolong Setiausaha JPDA, Kementerian Pegawai Teknologi Maklumat, IDFR Pegawai Teknologi Maklumat, SEARCCT Pegawai Teknologi Maklumat, Kementerian Penolong Pegawai Teknologi Maklumat, Kementerian Tanggungjawab CERT Kementerian meliputi semua bidang tugas pengurusan pengendalian insiden keselamatan ICT yang dialami oleh agensi di bawah kawalannya seperti berikut : • Menerima dan mengesan aduan keselamatan ICT dan menilai tahap dan jenis insiden; • Merekod dan menjalankan siasatan awal insiden yang diterima; • Menangani tindak balas (*response*) insiden keselamatan ICT dan mengambil tindakan baik pulih minima; • Menghubungi dan melaporkan insiden yang berlaku kepada GCERT MAMPU sama ada sebagai input atau untuk tindakan seterusnya;	CERT KLN

• Menasihatkan agensi-agensi di bawah kawalannya mengambil tindakan pemulihan dan pengukuhan; • Menyebarkan makluman berkaitan dengan agensi di bawah kawalannya; dan • Menjalankan penilaian untuk memastikan tahap keselamatan ICT dan mengambil tindakan pemulihan atau pengukuhan bagi meningkatkan tahap keselamatan infrastruktur ICT supaya insiden baru dapat dielakkan.	

02-02 Pihak luar/ketiga

Objektif:
Menjamin keselamatan semua aset ICT yang digunakan oleh pihak ketiga (Pembekal, Pakar Runding dan lain-lain)

02-02-01 Keperluan Keselamatan Aset ICT di dalam Kontrak dengan Pihak Ketiga

Keterangan	T/jawab
KLN hendaklah memastikan penggunaan maklumat dan kemudahan proses maklumat oleh pihak luar/ketiga dikawal. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti risiko keselamatan maklumat, keperluan keselamatan dan kemudahan pemprosesan maklumat serta melaksanakan kawalan yang sesuai sebelum memberi kebenaran capaian kepada pihak ketiga; (b) Akses capaian kepada aset ICT KLN perlu berlandaskan kepada Perjanjian Kontrak; (c) Memastikan semua syarat keperluan keselamatan dinyatakan dengan jelas di dalam perjanjian dengan pihak ketiga, merangkumi perkara-perkara seperti berikut: i. Dasar Keselamatan ICT KLN; ii. Tapisan Keselamatan; iii. Perakuan Akta Rahsia Rasmi 1972; dan iv. Hak Harta Intelek. (d) Menandatangani Surat Akuan Pematuhan Dasar Keselamatan ICT KLN seperti di **Lampiran 2.**	CIO, ICTSO dan Pentadbir Sistem ICT

PERKARA 03

PENGURUSAN ASET

03-01 Akauntabiliti Aset

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

03-01-01 Tanggungjawab ke atas Inventori Aset ICT

Keterangan	T/jawab
(a) Pengurusan dan pengendalian aset ICT hendaklah berpandukan kepada Pekeliling Perbendaharaan Bil. 5 Tahun 2007: Tatacara Pengurusan Aset Alih Kerajaan, dan adalah di bawah tanggungjawab Pengendali Aset ICT dan pengguna/pemilik aset ICT. (b) Tanggungjawab Pengendali Aset ICT adalah: i. Memastikan penerimaan aset ICT dari pembekal; ii. Menguruskan pendaftaran aset ICT; iii. Menguruskan pengagihan dan peminjaman aset ICT kepada pengguna KLN berpandukan kepada Dasar Pengagihan dan Peminjaman Peralatan ICT KLN; iv. Menyelenggara aset ICT; dan v. Menguruskan pelupusan aset ICT. (c) Tanggungjawab pengguna ICT adalah: i. Menerima aset ICT dari Pengendali Aset ICT; ii. Bertanggungjawab ke atas semua aset ICT di bawah kawalannya; iii. Menggunakan aset ICT untuk urusan RASMI sahaja; iv. Menghantar/menyerah aset ICT kepada Pengendali Aset ICT bagi tujuan penyelenggaraan pencegahan (*Preventive Maintenance*) atau sekiranya berlaku kerosakan; v. Mengembalikan aset kepada Pengendali Aset ICT apabila tidak lagi bertugas di KLN, bertukar penempatan atau berkursus melebihi 6 bulan.	Semua Pengguna ICT dan Pengendali Aset ICT

03-02 Pengelasan Maklumat

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

03-02-01 Pengelasan Maklumat

Keterangan	T/jawab

Memastikan setiap maklumat diberi perlindungan yang bersesuaian berdasarkan tahap sensitiviti masing-masing. Perkara yang patut dipatuhi adalah seperti berikut: (a) Maklumat hendaklah dikelaskan berasaskan nilai, keperluan perundangan, tahap sensitiviti dan tahap kritikal kepada KLN. Setiap maklumat yang dikelaskan mestilah mempunyai peringkat keselamatan sebagaimana yang ditetapkan di dalam Dokumen Arahan Keselamatan seperti berikut: i. Rahsia Besar; ii. Rahsia; iii. Sulit; atau iv. Terhad. (b) Maklumat hendaklah dilabel dan dikendalikan berasaskan peringkat keselamatan yang dikenal pasti dengan peraturan/prosedur yang ditetapkan oleh KLN dan Dokumen Arahan Keselamatan.	Semua Pengguna ICT KLN
03-02-01 Pengendalian Maklumat	
Keterangan	**T/jawab**
Aktiviti pengendalian maklumat seperti pewujudan, pengumpulan, pemprosesan, penyimpanan, penghantaran, penyampaian, penukaran dan pemusnahan hendaklah mengambil kira langkah-langkah keselamatan berikut: (a) Menghalang pendedahan maklumat kepada pihak yang tidak dibenarkan; (b) Memeriksa, menyemak dan menentukan maklumat adalah tepat dan lengkap dari semasa ke semasa; (c) Memasti dan menentukan maklumat sedia untuk digunakan; (d) Menjaga kerahsiaan kata laluan; (e) Mematuhi piawaian, prosedur dan garis panduan keselamatan yang dikeluarkan dari semasa ke semasa; (f) Memberi perhatian kepada pengendalian maklumat rahsia rasmi terperingkat terutama semasa pewujudan, pemprosesan, penyampaian, penghantaran, pertukaran dan pemusnahan; dan (g) Menjaga kerahsiaan langkah-langkah keselamatan ICT bagi pengurusan pengendalian maklumat rahsia rasmi dari diketahui umum.	Semua Pengguna KLN

PERKARA 04

KESELAMATAN SUMBER MANUSIA

04-01 Keselamatan Sumber Manusia

Objektif:
Memastikan semua sumber manusia yang terlibat termasuk pegawai dan kakitangan KLN, pembekal, pakar runding dan pihak-pihak yang berkepentingan memahami tanggungjawab dan peranan serta meningkatkan pengetahuan dalam keselamatan aset ICT. Semua warga KLN hendaklah mematuhi terma dan syarat perkhidmatan serta peraturan semasa yang berkuat kuasa.

04-01-01 Sebelum Perkhidmatan

Keterangan	T/jawab
Memastikan semua pengambilan sumber manusia perlu diuruskan dengan teratur berdasarkan langkah keselamatan yang ditetapkan. Perkara yang patut dipatuhi adalah seperti berikut: (a) Peranan dan tanggungjawab penjawat awam, kontraktor, pihak ketiga dan lain-lain pihak berkepentingan ke atas keselamatan ICT sebelum, semasa dan selepas perkhidmatan mestilah dinyatakan dengan lengkap dan jelas; (b) Menjalankan tapisan keselamatan untuk pegawai dan kakitangan KLN serta pihak ketiga yang terlibat berasaskan keperluan perundangan, peraturan dan etika terpakai yang selaras dengan keperluan perkhidmatan, peringkat maklumat yang akan dicapai serta risiko yang dijangkakan; dan (c) Mematuhi terma dan syarat perkhidmatan yang ditawarkan dan peraturan semasa yang berkuat kuasa berdasarkan perjanjian yang telah ditetapkan.	Bahagian Pengurusan Sumber Manusia dan Bahagian Pentadbiran dan Keselamatan

04-01-02 Dalam Perkhidmatan

Keterangan	T/jawab
Memastikan semua pengguna ICT KLN sedar akan ancaman keselamatan maklumat, peranan dan tanggungjawab masing-masing dan menyokong Dasar Keselamatan ICT KLN dan meminimumkan risiko kesilapan, kecuaian, penipuan dan penyalahgunaan aset ICT kerajaan. Perkara yang patut dipatuhi adalah seperti berikut: (a) Memastikan semua pengguna KLN serta pihak ketiga yang berkepentingan mengurus keselamatan aset ICT berdasarkan perundangan dan peraturan yang ditetapkan oleh KLN; (b) Memastikan latihan kesedaran yang berkaitan mengenai pengurusan keselamatan ICT diberi secara berterusan kepada semua pengguna KLN, dan sekiranya perlu latihan perlu diberikan kepada pihak ketiga yang berkepentingan;	Semua Pengguna ICT KLN

(c) Memastikan adanya proses tindakan disiplin dan/atau undang-undang ke atas pegawai dan kakitangan KLN serta pihak ketiga yang berkepentingan sekiranya berlaku perlanggaran dengan perundangan dan peraturan yang ditetapkan oleh KLN; (d) Memantapkan pengetahuan berkaitan dengan penggunaan aset ICT bagi memastikan setiap kemudahan ICT digunakan dengan cara dan kaedah yang betul demi menjamin kepentingan keselamatan ICT; dan (e) Sebarang kursus dan latihan teknikal yang diperlukan oleh pengguna boleh dirujuk kepada Bahagian Pengurusan Sumber Manusia, KLN.	

04-01-03 Bertukar, Berkursus/Cuti Tanpa Gaji Atau Tamat Perkhidmatan	
Keterangan	**T/jawab**
Memastikan semua pengguna KLN diurus dengan teratur apabila telah bertukar penempatan, berkursus/cuti tanpa gaji (melebihi tempoh 6 bulan), atau tamat perkhidmatan. Perkara-perkara yang perlu dipatuhi termasuk yang berikut: a) Memastikan semua aset ICT Kerajaan dikembalikan kepada Pengendali Aset ICT dan kepada Pegawai Aset Perwakilan (bagi pegawai di Perwakilan) mengikut peraturan/terma perkhidmatan yang ditetapkan; dan b) Membatal atau menarik balik semua kebenaran capaian/proses maklumat mengikut peraturan/terma perkhidmatan yang ditetapkan.	Semua Pengguna KLN, Pentadbir Sistem ICT

PERKARA 05
KESELAMATAN FIZIKAL DAN PERSEKITARAN

05-01 Keselamatan Kawasan

Objektif:
Melindungi premis dan maklumat daripada sebarang bentuk pencerobohan, ancaman, kerosakan serta akses yang tidak dibenarkan.

05-01-01 Kawalan Kawasan

Keterangan	T/jawab
Keselamatan kawasan adalah bertujuan untuk mengesan, mencegah dan menghalang cubaan untuk menceroboh ke kawasan yang menempatkan peralatan, maklumat dan kemudahan proses maklumat. Perlindungan bersesuaian yang perlu dipatuhi adalah seperti berikut: (a) Mengenal pasti kawasan keselamatan dengan jelas. Lokasi serta keteguhan kawasan hendaklah bergantung kepada keperluan untuk melindungi aset dalam kawasan dan juga 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) Menghadkan jalan masuk keluar; (d) Mengadakan kaunter kawalan; (e) Melindungi kawasan terhad melalui pintu masuk yang bersesuaian bagi memastikan kakitangan yang diberi kebenaran sahaja boleh melalui pintu masuk ini; (f) Menyediakan tempat dan bilik khas untuk pelawat; (g) Mewujudkan perkhidmatan kawalan keselamatan; (h) Memasang alat penggera atau kamera (CCTV) jika berkaitan. (i) Mereka bentuk dan melaksanakan keselamatan fizikal di dalam pejabat, bilik; (j) Mereka bentuk dan melaksanakan pelindungan 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	Bahagian Pentadbiran dan Keselamatan

kebenaran memasukinya.	

05-01-02 Kawalan Masuk Fizikal

Keterangan	T/jawab
Kawalan masuk fizikal adalah bertujuan untuk mewujudkan kawalan masuk ke premis/bangunan KLN. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Warga KLN i. Setiap warga KLN hendaklah memakai atau mempamerkan pas keselamatan sepanjang waktu bertugas; ii. Kehilangan pas keselamatan mestilah dilaporkan kepada balai polis berhampiran; iii. Kerosakan pas keselamatan perlulah dilaporkan kepada Bahagian Pentadbiran dan Keselamatan KLN; iv. Semua pas keselamatan hendaklah diserahkan semula kepada Bahagian Pentadbiran dan Keselamatan setelah menamatkan perkhidmatan dengan KLN; (b) Pelawat/Orang Awam/Pihak Ketiga i. Setiap pelawat/orang awam/pihak ketiga hendaklah mendaftar dan diwajibkan mendapatkan pas pelawat di Pondok Pengawal terlebih dahulu sebelum ke tempat berurusan dan hendaklah memulangkan semula selepas selesai urusan; ii. Kehilangan pas pelawat/sementara mestilah dilaporkan dengan segera kepada Bahagian Pentadbiran dan Keselamatan KLN; iii. Pihak ketiga yang telah menamatkan kontrak/perkhidmatan hendaklah menyerahkan pas pelawat/sementara kepada Bahagian Pentadbiran dan Keselamatan. iv. Jurujual/Pegawai Pemasaran tidak dibenarkan berniaga/mempromosikan barangan di premis KLN tanpa kebenaran rasmi oleh pengurusan KLN; dan v. Aktiviti pihak ketiga yang melakukan tugas-tugas di premis KLN hendaklah dipantau.	Semua Pengguna KLN, Bahagian Pentadbiran dan Keselamatan

05-01-03 Kawasan Larangan

Keterangan	T/jawab

Kawasan larangan ditakrifkan sebagai kawasan yang dihadkan kemasukan kepada pegawai-pegawai yang tertentu sahaja. Ini dilaksanakan untuk melindungi aset ICT yang terdapat di dalam kawasan tersebut. Kawasan larangan di KLN adalah *Control Room* (WP1 dan WP2), Bilik PABX, Bilik *Termination Control* (TC), Pusat Data (*Data Centre*) WP1, Bilik SPIDER, Bilik Saifer, Bilik Perhubungan Awam 108, Bilik Pendaftaran Terbuka dan Pendaftaran Rahsia, Bilik Kebal dan Bilik Bencana dan lain-lain kawasan yang ditetapkan sebagai kawasan larangan oleh Bahagian Pentadbiran dan Keselamatan. Perkara-perkara yang perlu dipatuhi dalam melindungi kawasan larangan adalah seperti berikut: (a) Akses kepada kawasan larangan hanyalah kepada pegawai-pegawai yang dibenarkan sahaja; (b) Pihak ketiga adalah dilarang sama sekali memasuki kawasan larangan kecuali, bagi kes-kes tertentu seperti memberi perkhidmatan sokongan atau bantuan teknikal, dan mereka hendaklah diiringi sepanjang masa oleh pegawai yang bertugas di kawasan larangan tersebut sehingga tugas di kawasan berkenaan selesai; dan (c) Mewujudkan buku log bagi menyenaraikan aktiviti yang dilakukan semasa berurusan.	Bahagian Pentadbiran dan Keselamatan, dan Bahagian ICT.

05-02 Keselamatan Peralatan

Objektif:
Melindungi peralatan ICT KLN dari kehilangan, kerosakan, kecurian serta gangguan kepada peralatan tersebut.

05-02-01 Peralatan ICT

Keterangan	T/jawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Pengguna hendaklah memeriksa dan memastikan semua peralatan ICT di bawah kawalannya berfungsi dengan sempurna; (b) Pengguna dilarang sama sekali menambah, menanggal atau menggantikan sebarang pertukaran perkakasan dan konfgurasi yang telah ditetapkan; (c) Pengguna dilarang membuat instalasi sebarang perisian tambahan tanpa kebenaran Pentadbir Sistem ICT melainkan dengan kelulusan; (d) Pengguna adalah bertanggungjawab di atas kerosakan atau kehilangan peralatan ICT di bawah kawalannya; (e) Pengguna mesti memastikan perisian antivirus di komputer peribadi mereka sentiasa aktif (a*ctivated*) dan dikemas kini di	Semua pengguna KLN

samping melakukan imbasan ke atas media storan yang digunakan; (f) Penggunaan kata laluan untuk akses ke sistem komputer adalah diwajibkan; (g) Semua peralatan ICT hendaklah dilindungi daripada kecurian, kerosakan, penyalahgunaan atau pengubahsuaian tanpa kebenaran; (h) Peralatan-peralatan kritikal perlu disokong oleh *Uninterruptable Power Supply* (UPS); (i) 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; (j) Semua peralatan yang digunakan secara berterusan mestilah diletakkan di kawasan berhawa dingin dan mempunyai pengudaraan (*air ventilation*) yang sesuai; (k) Peralatan ICT yang hendak dibawa keluar dari premis KLN, perlulah mendapat kelulusan Ketua Jabatan/Bahagian/Unit dan direkodkan bagi tujuan pemantauan; (l) Peralatan ICT yang hilang hendaklah dilaporkan kepada ICTSO dan Pegawai Aset (mengisi borang KEW.PA-28) dengan mengemukakan bersama laporan polis; (m) Sebarang bentuk penyelewengan atau salah guna peralatan ICT hendaklah dilaporkan kepada ICTSO; (n) Pengendalian peralatan ICT hendaklah mematuhi dan merujuk kepada peraturan semasa yang berkuat kuasa. (o) Pengguna tidak dibenarkan mengubah kedudukan komputer dari tempat asal tanpa kebenaran Bahagian ICT; (p) Sebarang kerosakan peralatan ICT hendaklah dilaporkan kepada Bahagian ICT untuk dibaik pulih; (q) Sebarang pelekat selain bagi tujuan rasmi tidak dibenarkan bagi menjamin peralatan tersebut sentiasa berkeadaan baik; (r) Pengguna dilarang sama sekali mengubah kata laluan bagi pentadbir (*administrator password*) yang telah ditetapkan oleh Pentadbir Sistem ICT; (s) Pengguna bertanggungjawab terhadap perkakasan, perisian dan maklumat di bawah jagaannya dan hendaklah digunakan sepenuhnya bagi urusan RASMI sahaja. (t) Pengguna hendaklah memastikan semua perkakasan komputer, pencetak dan pengimbas dalam keadaan "OFF" apabila	

meninggalkan pejabat; dan (u) Memastikan *plug* dicabut daripada suis utama (*main switch*) sebelum meninggalkan pejabat bagi mengelakkan kerosakan perkakasan jika berlaku kejadian seperti petir, kilat dan sebagainya.	

05-02-02 Media Storan

Keterangan	T/jawab
Media storan merupakan peralatan elektoronik yang digunakan untuk menyimpan data dan maklumat seperti disket, cakera padat, pita magnetik*, external hard disk*, *pendrive* dan media storan lain. Keselamatan media storan perlu diberi perhatian khusus kerana ia berupaya menyimpan maklumat rasmi dan rahsia rasmi kerajaan. Langkah-langkah pencegahan hendaklah diambil untuk memastikan kerahsiaan, integriti dan kebolehsediaan maklumat yang disimpan dalam media storan dan ianya hendaklah dijamin selamat. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Media storan hendaklah disimpan di ruang penyimpanan yang mempunyai ciri-ciri keselamatan bersesuaian dengan kandungan maklumat; (b) Menghadkan akses memasuki kawasan menyimpan media kepada pengguna yang dibenarkan sahaja; (c) Merekodkan sistem pengurusan media termasuk inventori, pergerakan, melabel dan penduaan (*backup*). (d) Semua media storan perlu dikawal dari capaian yang tidak dibenarkan, dicuri dan dimusnahkan; (e) Akses dan pergerakan media storan hendaklah direkodkan; (f) Mengadakan salinan atau penduaan (*backup*) kedua pada media storan bagi tujuan keselamatan dan bagi mengelakkan kehilangan data; (g) Semua media storan yang hendak dilupuskan mestilah dihapuskan mengikut pekeliling yang telah ditetapkan; dan (h) Penghapusan maklumat atau kandungan media mestilah mendapat kelulusan pemilik maklumat terlebih dahulu.	Semua Pengguna ICT

05-02-03 Media Perisian dan Aplikasi

Keterangan	T/jawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Hanya perisian yang diperakui sahaja dibenarkan bagi kegunaan KLN.	Pentadbir Sistem

(b) Sistem aplikasi dalaman tidak dibenarkan didemonstrasi atau diagih kepada pihak lain kecuali dengan kebenaran Pengurus ICT; (c) Lesen perisian (*registration code, serials, CD-keys*) perlu disimpan berasingan daripada CD-rom, *disk* atau media berkaitan bagi mengelakkan dari berlakunya kecurian atau cetak rompak; dan (d) *Source code* sesuatu sistem hendaklah disimpan dengan teratur dan sebarang pindaan mestilah mengikut prosedur yang ditetapkan. (e) Penduaan (*backup*) bagi sistem aplikasi hendaklah dibuat bagi tujuan rekod keselamatan.	

05-02-04 Penyelengaraan Perkakasan ICT

Keterangan	**T/jawab**
Perkakasan hendaklah diselenggarakan dengan betul bagi memastikan kebolehsediaan, kerahsiaan dan integriti. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua perkakasan yang diselenggara hendaklah mematuhi spesifikasi yang ditetapkan oleh pengeluar; (b) Memastikan perkakasan hanya boleh diselenggara oleh kakitangan atau pihak yang dibenarkan sahaja; (c) Setiap perkakasan sama ada dalam tempoh jaminan atau telah habis tempoh jaminan hendaklah diselengara; (d) Menyemak dan menguji semua perkakasan sebelum dan selepas proses penyelenggaraan; (e) Memaklumkan pengguna sebelum melaksanakan penyelenggaraan mengikut jadual yang ditetapkan atau atas keperluan; dan (f) Memastikan segala maklumat sulit dan dan rahsia di dalam komputer di salin pada media storan kedua seperti *pendrive* sebelum menghapuskan maklumat tersebut sekiranya penyelenggaraan dilakukan oleh pihak ketiga.	Bahagian ICT dan Pengguna ICT

05-02-05 Pelupusan Peralatan ICT

Keterangan	**T/jawab**
Semua peralatan ICT yang telah rosak, usang dan tidak boleh dibaiki sama ada harta modal atau inventori yang dibekal dan ditempatkan di KLN hendaklah dilupuskan mengikut prosedur pelupusan semasa. Pelupusan perlu dilakukan secara terkawal dan lengkap supaya maklumat tidak terlepas dari kawalan KLN. Perkara-perkara yang perlu dipatuhi adalah seperti berikut:	Pegawai Aset dan Pengguna ICT

(a) Semua kandungan peralatan 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 bolehlah membuat penduaan; (c) Data-data dalam storan peralatan ICT yang hendak dilupuskan hendaklah dihapuskan dengan cara yang selamat; (d) Pegawai Aset hendaklah mengenal pasti sama ada peralatan tertentu boleh dilupuskan atau sebaliknya; (e) Peralatan ICT yang hendak dilupuskan hendaklah disimpan di tempat yang dikhaskan yang mempunyai ciri-ciri keselamatan bagi menjamin keselamatan peralatan tersebut. (f) Pegawai aset bertanggungjawab merekodkan butir-butir pelupusan dan mengemas kini rekod pelupusan peralatan ICT ke dalam sistem inventori; (g) Pengguna ICT DILARANG SAMA SEKALI daripada melakukan perkara-perkara seperti berikut: i. Menyimpan mana-mana peralatan 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 KLN; iii. Memindah keluar dari KLN mana-mana peralatan ICT yang hendak dilupuskan; iv. Melupuskan sendiri peralatan ICT kerana kerja-kerja pelupusan di bawah tanggungjawab KLN; dan v. Pengguna ICT bertanggungjawab memastikan segala maklumat sulit dan rahsia di dalam komputer disalin pada media storan kedua seperti disket atau *pendrive* sebelum menghapuskan maklumat tersebut daripada peralatan komputer yang hendak dilupuskan.	
05-02-06 Pengendalian Peralatan Luar yang Dibawa Masuk	
Keterangan	**T/jawab**
Bagi peralatan yang dibawa masuk ke premis KLN, perkara yang perlu dipatuhi adalah seperti berikut: (a) Mendapat kelulusan mengikut peraturan yang telah ditetapkan oleh KLN bagi membawa masuk peralatan;	ICTSO

(b) Memeriksa dan memastikan peralatan yang dibawa masuk selamat digunakan dan tidak mengancam peralatan ICT KLN; dan (c) Penyimpanan peralatan mestilah mengambil kira ciri-ciri keselamatan yang bersesuaian.	

05-03 Keselamatan Persekitaran

Objektif:
Melindungi aset ICT KLN dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, kesilapan, kecuaian atau kemalangan.

05-03-01 Kawalan Persekitaran

Keterangan	T/jawab
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 (CGSO). Bagi menjamin keselamatan persekitaran, perkara-perkara berikut hendaklah dipatuhi: (a) Merancang dan menyediakan pelan keseluruhan susun atur pusat data (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 dikenal pasti dan dikendalikan; (d) Bahan mudah terbakar hendaklah disimpan di luar kawasan kemudahan penyimpanan aset ICT; (e) Semua bahan cecair hendaklah diletakkan di tempat yang bersesuaian dan berjauhan dari aset ICT; (f) Pengguna adalah dilarang merokok atau menggunakan peralatan memasak seperti cerek elektrik berhampiran peralatan komputer; (g) Semua peralatan perlindungan hendaklah disemak dan diuji sekurang-kurangnya dua (2) kali setahun. Aktiviti dan keputusan ujian ini perlu direkodkan bagi memudahkan rujukan dan tindakan sekiranya perlu; dan (h) Akses kepada saluran *riser* hendaklah sentiasa dikunci.	Bahagian Pentadbiran dan Keselamatan, dan Semua Pengguna

05-03-02 Bekalan Kuasa (UPS/*Generator*)

Keterangan	T/jawab

Perkara yang perlu dipatuhi bagi menjamin keselamatan bekalan kuasa adalah seperti berikut: (a) Melindungi semua peralatan ICT dari kegagalan bekalan elektrik dalam menyalurkan bekalan yang sesuai kepada peralatan ICT; (b) Menggunakan peralatan sokongan seperti UPS (*Uninterruptable Power Supply*) dan penjana kuasa (generator) bagi perkhidmatan kritikal seperti di bilik server supaya mendapat bekalan kuasa yang berterusan; dan (c) Menyemak dan menguji semua peralatan sokongan bekalan kuasa berjadual.	Bahagian Pentadbiran dan Keselamatan, dan Bahagian ICT

05-03-03 Keselamatan Kabel

Keterangan	**T/jawab**
Kabel merangkumi kabel elektrik dan telekomunikasi yang menyalurkan data dan menyokong perkhidmatan penyampaian maklumat. Kabel tersebut hendaklah dilindungi kerana boleh menjadi maklumat terdedah. Perkara yang perlu dipatuhi 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.	Bahagian Pentadbiran dan Keselamatan

05-03-04 Prosedur Kecemasan

Keterangan	**T/jawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan setiap pengguna membaca, memahami dan mematuhi prosedur kecemasan yang ditetapkan; (b) Melaporkan insiden kecemasan persekitaran seperti kebakaran kepada pegawai keselamatan KLN; (c) Mengadakan, menguji dan mengemaskini pelan kecemasan dari semasa ke semasa ; dan (d) Merancang dan mengadakan latihan kebakaran bangunan (*fire drill*) secara berkala.	Bahagian Pentadbiran dan Keselamatan

05-04 Keselamatan Dokumen

Objektif:

Melindungi maklumat KLN dari sebarang bentuk ancaman persekitaran yang disebabkan oleh bencana alam, pencerobohan, kesilapan atau kecuaian.

05-04-01 Dokumen	
Keterangan	**T/jawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Setiap dokumen hendaklah difail 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 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.	Semua Pengguna ICT

PERKARA 06
PENGURUSAN OPERASI DAN KOMUNIKASI

06-01 Pengurusan Prosedur Operasi

Objektif:
Memastikan pengurusan operasi sistem dan komunikasi dapat berfungsi dengan betul dan selamat daripada ancaman dan gangguan.

06-01-01 Pengendalian Prosedur

Keterangan	T/jawab
Memastikan kemudahan pemprosesan maklumat beroperasi seperti yang ditetapkan dan selamat. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Semua prosedur operasi keselamatan ICT hendaklah dikenal pasti, didokumenkan dengan jelas lagi teratur, dikemaskini dan boleh diguna pakai oleh pengguna mengikut keperluan; (b) Setiap prosedur mestilah mengandungi arahan-arahan yang jelas, teratur dan lengkap sebagai contoh keperluan kapasiti, pengendalian dan pemprosesan maklumat, pengendalian dan penghantaran ralat, pengendalian *output*, bantuan teknikal dan pemulihan sekiranya pemprosesan tergendala atau terhenti; (c) Semua prosedur hendaklah dikemas kini dari semasa ke semasa mengikut keperluan.	Pengurus ICT dan ICTSO

06-01-02 Kawalan Perubahan

Keterangan	T/jawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Permohonan untuk membuat pengubahsuaian yang melibatkan sistem untuk pemprosesan maklumat, perisian dan prosedur mestilah secara bertulis; (b) Aktiviti-aktiviti seperti memasang, menyenggara, menghapus dan mengemas kini mana-mana komponen sistem ICT hendaklah dikendalikan oleh pihak atau pegawai yang diberi kuasa dan mempunyai pengetahuan atau terlibat secara langsung dengan aset ICT berkenaan; (c) Semua aktiviti pengubahsuaian komponen sistem ICT hendaklah mematuhi spesifikasi perubahan yang telah ditetapkan; dan (d) Semua aktiviti perubahan atau pengubahsuaian hendaklah direkod dan dikawal bagi mengelakkan berlakunya ralat sama ada secara sengaja atau pun tidak.	Pengurus ICT dan Pentadbir Sistem

06-01-03 Pengasingan Tugas dan Tanggungjawab	
Keterangan	**T/jawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Skop tugas dan tanggungjawab perlu diasingkan bagi mengurangkan peluang berlaku penyalahgunaan atau pengubahsuaian yang tidak dibenarkan ke atas aset ICT; (b) Tugas mewujud, memadam, mengemas kini, mengubah dan mengesahkan data hendaklah diasingkan bagi mengelakkan daripada capaian yang tidak dibenarkan serta melindungi aset ICT daripada kesilapan, kebocoran maklumat terperingkat atau dimanipulasi; dan (c) Perkakasan (seperti *server*) yang digunakan bagi tugas membangun, mengemaskini, menyenggara dan menguji aplikasi hendaklah diasingkan dari perkakasan yang digunakan sebagai *production*. Pengasingan juga merangkumi tindakan memisahkan antara kumpulan operasi dan rangkaian.	Pentadbir Sistem ICT

06-02 Pengurusan Perkhidmatan Kontrak Oleh Pihak Ketiga
Objektif: Memastikan pelaksanaan dan penyenggaraan tahap keselamatan maklumat dan penyampaian perkhidmatan yang sesuai selaras dengan perjanjian perkhidmatan dengan pihak ketiga.

06-02-01 Perkhidmatan Kontrak	
Keterangan	**T/jawab**
Perkara-perkara yang mesti dipatuhi adalah seperti berikut: (a) Memastikan kawalan keselamatan, definasi perkhidmatan dan tahap penyampaian yang terkandung dalam perjanjian dipatuhi, dilaksanakan dan diselenggarakan oleh pihak ketiga; (b) Perkhidmatan laporan dan rekod yang dikemukakan oleh pihak ketiga perlu sentiasa dipantau, disemak semula dan diaudit dari semasa ke semasa; dan (c) Pengurusan perubahan dasar perlu mengambil kira tahap kritikal sistem dan proses yang terlibat serta penilaian semula risiko.	Pengurus ICT dan Pentadbir Sistem

06-03 Perancangan dan Penerimaan Sistem
Objektif: Meminimumkan risiko yang menyebabkan gangguan atau kegagalan sistem.

06-03-01 Perancangan Kapasiti	
Keterangan	**T/jawab**
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.	Pentadbir Sistem ICT

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.	

06-03-02 Penerimaan Sistem

Keterangan	T/jawab
Semua sistem baru (termasuklah sistem yang dikemas kini atau diubahsuai) hendaklah memenuhi kriteria yang ditetapkan sebelum diterima atau dipersetujui.	Pentadbir Sistem ICT

06-04 Perisian Berbahaya

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

06-04-01 Perlindungan dan Perisian Berbahaya

Keterangan	T/jawab
Perkara-pekara 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 hak cipta terpelihara; (c) Mengimbas semua perisian atau sistem dengan perisian anti-virus sebelum menggunakannya; (d) Mengemas kini anti-virus dengan *pattern* anti-virus yang terkini; (e) Menyemak kandungan sistem atau maklumat secara berkala bagi mengesan aktiviti yang tidak diingini seperti kehilangan dan kerosakan maklumat; (f) Menghadiri program kesedaran mengenai ancaman perisian berbahaya dan cara pengendaliannya; (g) Memasukkan klausa tanggungan di dalam kontrak yang 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 mengenai ancaman keselamatan ICT seperti serangan virus.	Semua Pengguna ICT, ICTSO dan pegawai ICT yang menyediakan kontrak

06-04-02 Perlindungan dari *Mobile Code*

Keterangan	T/jawab

Penggunaan *mobile code* yang boleh mendatangkan ancaman keselamatan ICT adalah tidak dibenarkan. Walau bagaimanapun, dalam keadaaan *mobile code* dibenarkan, konfigurasinya hendaklah dipastikan supaya ianya beroperasi berdasarkan kepada dasar keselamatan yang jelas.	Pentadbir Sistem ICT dan Pihak Ketiga

06-05 *Housekeeping*

Objektif:
Melindungi integriti maklumat agar boleh diakses pada bila-bila masa.

06-05-01 *Backup*

Keterangan	T/jawab
Bagi memastikan sistem dapat dibangunkan semula setelah berlakunya bencana, salinan pendua hendaklah dilakukan setiap kali konfigurasi berubah. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Membuat salinan keselamatan ke atas semua sistem perisian dan aplikasi sekurang-kurangnya sekali atau setelah mendapat versi terbaru; (b) Membuat salinan pendua 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) Salinan maklumat dan perisian perlu dibuat dan diuji secara berkala berdasarkan kepada prosedur penduaan; (e) Menyimpan sekurang-kurangnya dua (2) generasi *backup*; dan (f) Merekod dan menyimpan salinan *backup* di lokasi yang berlainan dan selamat.	Pentadbir Sistem ICT

06-06 Pengurusan Rangkaian

Objektif:
Melindungi maklumat dalam rangkaian dan infrastruktur sokongan.

06-06-01 Kawalan Infrastruktur Rangkaian

Keterangan	T/jawab
Infrastruktur Rangkaian mestilah dikawal dan diurus sebaik mungkin demi melindungi ancaman kepada sistem dan aplikasi di dalam rangkaian. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar dan prosedur perlu dibangunkan dan dilaksanakan bagi	Pentadbir Sistem ICT

melindungi maklumat yang berhubung kait dengan sistem rangkaian;

(b) Ciri-ciri keselamatan, tahap perkhidmatan dan keperluan pengurusan bagi semua perkhidmatan rangkaian perlu dikenal pasti dan dimasukkan dalam mana-mana perjanjian perkhidmatan rangkaian sama ada perkhidmatan berkenaan disediakan secara dalaman atau melalui khidmat luar;

(c) Tanggungjawab atau kerja-kerja operasi rangkaian komputer hendaklah diasingkan untuk mengurangkan capaian dan pengubahsuaian yang tidak dibenarkan;

(d) Peralatan rangkaian hendaklah diletakkan di lokasi yang mempunyai ciri-ciri fizikal yang kukuh dan bebas dari risiko seperti banjir, gegaran dan habuk;

(e) Capaian kepada peralatan rangkaian hendaklah dikawal dan dihadkan kepada pengguna yang dibenarkan sahaja;

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

(g) *Firewall* hendaklah dipasang serta dikonfigurasi oleh pentadbir sistem yang dibenarkan sahaja;

(h) Semua trafik keluar dan masuk hendaklah melalui *Firewall* di bawah kawalan KLN;

(i) Semua perisian *sniffer* atau *network analyser* adalah dilarang dipasang pada komputer pengguna kecuali mendapat kebenaran ICTSO;

(j) Memasang perisian *Intrusion Detection System* (IDS) dan *Intrusion Prevention System* (IPS) bagi mengesan sebarang percubaan menceroboh dan aktiviti-aktiviti lain yang boleh mengancam sistem dan maklumat jabatan;

(k) Memasang *Web Content Filtering* pada *Internet Gateway* untuk menyekat aktiviti yang dilarang;

(l) Semua pengguna ICT hanya dibenarkan menggunakan rangkaian KLN sahaja dan penggunaan modem peribadi adalah dilarang sama sekali;

(m) Penggunaan *wireless* LAN di KLN perlu dipastikan kawalan keselamatannya.

06-07 Pengurusan *Server*

Objektif:
Melindungi peralatan *server* dari sebarang pencerobohon, pengubahsuaian, pemindahan, kerosakan atau pemusnahan.

06-07-01 Keselamatan *Server*	
Keterangan	**T/jawab**
Peralatan *server* perlulah dilindungi dan dikawal sebaik mungkin bagi mengurangkan ancaman ke atasnya. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar dan prosedur perlu dibangunkan dan dilaksanakan bagi melindungi keselamatan *server* dari aspek capaian fizikal dan capaian logikal; (b) Semua server perlulah diletakkan di bilik *server* yang dikawal aksesnya (rujuk para 05-01-03: Kawasan Larangan); dan (c) Ciri-ciri keselamatan bilik *server* mestilah memenuhi keperluan keselamatan yang ditetapkan (rujuk para 05-03-01: Keselamatan Persekitaran)	Pentadbir Sistem ICT (Pengurus Pusat Data) dan ICTSO

06-08 Pengurusan Media
Objektif: Melindungi aset ICT dari sebarang pendedahan, pengubahsuaian, pemindahan atau pemusnahan serta gangguan ke atas aktiviti perkhidmatan.

06-08-01 Penghantaran dan Pemindahan	
Keterangan	**T/jawab**
Penghantaran atau pemindahan media ke luar pejabat hendaklah mendapat kebenaran pemilik terlebih dahulu. Media yang mengandungi maklumat kerajaan perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KLN. Prosedur perlu disediakan untuk pengurusan media mudah alih.	Bahagian ICT

06-08-02 Prosedur Pengendalian Media	
Keterangan	**T/jawab**
Perkara yang patut dipatuhi adalah seperti berikut: (a) Semua media hendaklah dilabelkan mengikut tahap sensitiviti sesuatu maklumat; (b) Menghadkan dan menentukan capaian kepada pengguna yang dibenarkan sahaja; (c) Menghadkan pengedaran data untuk yang dibenarkan sahaja; (d) Penyelenggaraan media hendaklah dikawal dan direkodkan bagi mengelak dari sebarang kerosakan dan pendedahan yang tidak dibenarkan; (e) Semua media hendaklah disimpan di tempat yang selamat; dan (f) Media yang mengandungi maklumat terperingkat yang hendak dihapuskan atau dimusnahkan mestilah dilupuskan mengikut	Semua Pengguna KLN

prosedur yang betul dan selamat.	

06-08-03 Keselamatan Sistem Dokumentasi

Keterangan	T/jawab
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memastikan sistem penyimpanan dokumentasi mempunyai ciri-ciri keselamatan; (b) Menyedia dan memantapkan lagi keselamatan sistem dokumentasi dalam rangkaian; dan (c) Mengawal dan merekodkan semua aktiviti capaian sistem dokumentasi sedia ada.	Semua Pengguna ICT

06-09 Pengurusan Pertukaran Maklumat

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

06-09-01 Pertukaran Maklumat

Keterangan	T/jawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Dasar, prosedur dan kawalan pertukaran maklumat yang formal perlu diwujudkan untuk melindungi penggunaan pelbagai jenis kemudahan komunkasi; (b) Perjanjian perlu diwujudkan untuk pertukaran maklumat dan perisian di antara KLN dengan agensi luar; (c) Media yang mengandungi maklumat perlu dilindungi daripada capaian yang tidak dibenarkan, penyalahgunaan atau kerosakan semasa pemindahan keluar dari KLN; dan (d) Maklumat yang terdapat dalam e-mel perlu dilindungi sebaik-baiknya.	Semua Pengguna ICT

06-09-02 Pengurusan Internet dan E-mel

Keterangan	T/jawab
Penggunaan Internet dan e-mel di KLN hendaklah dipantau secara berterusan untuk memenuhi keperluan etika penggunaan e-mel dan Internet yang terkandung dalam Tatacara Penggunaan Internet dan E-mel KLN.	ICTSO dan Pentadbir Sistem

06-09-03 Perkhidmatan Atas-Talian

Keterangan	T/jawab
Perkara-perkara berikut perlu dipatuhi bagi memelihara keselamatan penggunaan aplikasi perkhidmatan atas-talian (*online*): (a) Maklumat yang terlibat dalam e-dagang perlu dilindungi daripada aktiviti penipuan, pertikaian kontrak dan pendedahan serta	Pentadbir Sistem

pengubahsuaian yang tidak dibenarkan; (b) Maklumat yang terlibat dalam transaksi atas-talian (*online*) perlu dilindungi bagi mengelak penghantaran yang tidak lengkap, salah destinasi, pengubahsuaian, pendedahan, salinan berganda (*duplication*) atau pengulangan mesej yang tidak dibenarkan; dan (c) Integriti maklumat yang disediakan dalam sistem untuk kegunaan awam perlu dilindungi untuk mengelak daripada pengubahsuaian yang tidak dibenarkan.	

06-10 Pemantauan

Objektif:
Memastikan pengesanan aktiviti pemprosesan maklumat yang tidak dibenarkan.

06-10-01 Pengauditan dan Forensik ICT

Keterangan	T/jawab
CERT KLN mestilah bertanggungjawab merekod dan menganalisis perkara-perkara berikut: (a) Sebarang percubaan pencerobohan kepada sistem ICT KLN; (b) Serangan kod perosak (*malicious code*), halangan pemberian perkhidmatan (*denial of service*), *spam*), pemalsuan (*forgery, phising*), pencerobohan (*intrusion*), ancaman (*threats*) dan kehilangan fizikal (*physical loss*); (c) Pengubahsuaian ciri-ciri perkakasan, perisian atau mana-mana komponen sesebuah sistem tanpa pengetahuan, arahan atau persetujuan mana-mana pihak; (d) Aktiviti melayari, menyimpan atau mengedar bahan-bahan lucah, berunsur fitnah dan propaganda anti kerajaan; (e) Aktiviti pewujudan perkhidmatan-perkhidmatan yang tidak dibenarkan; (f) Aktiviti instalasi dan penggunaan perisian yang membebankan jalur lebar (*bandwidth*) rangkaian; (g) Aktiviti penyalahgunaan akaun e-mel;	CERT KLN

06-10-02 Jejak Audit

Keterangan	T/jawab
Setiap sistem mestilah mempunyai jejak audit (*audit trail*) bagi membenarkan pemeriksaan dan pembinaan semula dilakukan bagi susunan dan perubahan dalam sesuatu acara. Jejak audit hendaklah mengandungi maklumat-maklumat berikut: (a) Rekod setiap aktiviti transaksi;	Pentadbir Sistem ICT

(b) Maklumat jejak audit mengandungi identiti pengguna, sumber yang digunakan, perubahan maklumat, tarikh dan masa aktiviti, rangkaian dan aplikasi yang digunakan; (c) Aktiviti capaian pengguna 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 yang disarankan oleh Arahan Teknologi Maklumat dan Akta Arkib Negara. Pentadbir Sistem ICT hendaklah menyemak catatan jejak audit dari semasa ke semasa dan menyediakan laporan jika perlu. Ini akan dapat membantu mengesan aktiviti yang tidak normal dengan lebih awal. Jejak audit juga perlu dilindungi dari kerosakan, kehilangan, penghapusan, pemalsuan dan pengubahsuaian yang tidak dibenarkan.	
06-10-03 Sistem Log	
Keterangan	**T/jawab**
Pentadbir Sistem ICT hendaklah melaksanakan perkara-perkara berikut: (a) Mewujudkan sistem log bagi merekodkan semua aktiviti harian pengguna; (b) Menyemak sistem log secara berkala bagi mengesan ralat yang menyebabkan gangguan kepada sistem dan mengambil tindakan membaik pulih dengan segera; dan (c) Sekiranya wujud aktiviti-aktiviti lain yang tidak sah seperti kecurian maklumat dan pencerobohan, Pentadbir Sistem ICT hendaklah melaporkan kepada ICTSO.	Pentadbir Sistem ICT
06-10-04 Pemantauan Log	
Keterangan	**T/jawab**
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 diwujud 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; dan	Pentadbir Sistem ICT

(e) Kesalahan, kesilapan dan/atau penyalahgunaan perlu direkodkan log, dianalisis dan diambil tindakan sewajarnya.	

PERKARA 07
KAWALAN CAPAIAN

07-01 Dasar Kawalan Capaian

Objektif:
Mengawal capaian ke atas maklumat.

07-01-01 Keperluan Kawalan Capaian

Keterangan	T/jawab
Peraturan kawalan capaian hendaklah diwujud, didokumen dan dikaji semula berasaskan keperluan perkhidmatan dan keselamatan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Kawalan capaian ke atas maklumat hendaklah mengikut keperluan keselamatan dan peranan pengguna; (b) Kawalan capaian ke atas perkhidmatan rangkaian dalaman dan luaran; (c) Kawalan capaian ke atas kemudahan memproses maklumat seperti capaian pengguna; dan (d) Kawalan capaian ke atas maklumat yang menggunakan kemudahan atau peralatan mudah alih hendaklah dipastikan selamat.	Pentadbir Sistem ICT dan Semua Pengguna ICT

0702 Pengurusan Capaian Pengguna

Objektif:
Mengawal capaian pengguna ke atas aset KLN.

07-02-01 Akaun Pengguna Sistem Perkhidmatan ICT KLN

Keterangan	T/jawab
Setiap pengguna bertanggungjawab ke atas sistem ICT yang digunakan. Bagi mengenal pasti pengguna dan aktiviti yang dilakukan, perkara-perkara berikut hendaklah dipatuhi: (a) Akaun yang diperuntukkan oleh KLN sahaja boleh digunakan. (b) Akaun pengguna adalah unik dan pengguna bertanggungjawab ke atas akaun tersebut selepas pengesahan penerimaan dibuat; (c) Akaun pengguna yang diwujudkan dan tahap capaian termasuk sebarang perubahan mestilah mendapat kebenaran secara bertulis dan direkodkan; (d) Pemilikan akaun dan capaian pengguna adalah tanggungjawab Bahagian ICT dengan kelulusan CIO/SUB PSM bagi	CIO, Bahagian ICT, Bahagian PSM

membeku/membatalan/mengubahsuai akaun pengguna atas sebab berikut: (i) Pengguna tidak hadir bertugas tanpa kebenaran melebihi satu tempoh yang ditentukan oleh Ketua Jabatan; (ii) Pengguna bercuti atau bertugas di luar pejabat melebihi satu tempoh yang ditentukan oleh Ketua Jabatan; (iii) Pengguna bertukar penempatan, jawatan, tanggungjawab dan/atau bidang tugas; (iv) Pengguna bertukar atau berpindah agensi; dan (v) Pengguna bersara atau tamat perkhidmatan/kontrak. (e) Aktiviti capaian oleh pengguna direkod, diselenggara dengan sistematik dan dikaji dari semasa ke semasa. Maklumat yang direkod termasuk identiti pengguna, perubahan maklumat, tarikh, masa, rangkaian dilalui, aplikasi digunakan dan aktiviti capaian secara sah atau sebaliknya.	

07-02-02 Hak Capaian

Keterangan	**T/jawab**
Penetapan dan penggunaan ke atas hak capaian perlu diberi kawalan dan penyeliaan yang ketat berdasarkan keperluan skop tugas.	Pentadbir Sistem ICT

07-02-03 Pengurusan Kata Laluan

Keterangan	**T/jawab**
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 KLN seperti berikut: (a) Dalam apa jua keadaan dan sebab, kata laluan hendaklah dilindungi dan tidak boleh dikongsi dengan sesiapa pun; (b) Pengguna hendaklah menukar kata laluan apabila disyaki berlakunya kebocoran kata laluan atau dikompromi; (c) Panjang kata laluan mestilah sekurang-kurangnya lapan (8) aksara dengan gabungan aksara dan angka; (d) Kata laluan hendaklah diingat dan TIDAK BOLEH dicatat, disimpan atau didedahkan dengan apa cara sekalipun; (e) Kata laluan *windows* dan *screen saver* hendaklah diaktifkan terutamanya pada komputer yang terletak di ruang guna sama; (f) Kata laluan hendaklah tidak dipaparkan semasa *input*, dalam laporan atau media lain dan tidak boleh dikodkan di dalam program;	Semua Pengguna ICT

(g) Kuatkuasakan pertukaran kata laluan semasa *login* kali pertama atau selepas kata laluan diset semula; (h) Kata laluan hendaklah berlainan daripada pengenalan identiti pengguna; (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 yang bersesuaian; dan (k) Mengelakkan penggunaan semula kata laluan yang sama (kata laluan baru tidak boleh sama dengan kata lalun sebelum)	

07-02-04 *Clear Desk* dan *Clear Screen*

Keterangan	**T/jawab**
Semua maklumat dalam apa jua bentuk media hendaklah disimpan dengan teratur dan selamat bagi mengelakkan kerosakan, kecurian atau kehilangan. *Clear Desk* dan *Clear Screen* bermaksud tidak meninggalkan bahan-bahan yang sensitif terdedah sama ada atas meja pengguna atau di paparan skrin komputer apabila pengguna tidak berada di tempatnya. 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 berkunci; dan (c) Memastikan semua dokumen diambil segera dari pencetak, pengimbas, mesin faksimile dan mesin fotostat.	Semua Pengguna ICT

07-03 Kawalan Capaian Rangkaian

Objektif:
Menghalang capaian tidak sah dan tanpa kebenaran ke atas perkhidmatan rangkaian.

07-03-01 Capaian Rangkaian

Keterangan	**T/jawab**
Kawalan capaian perkhidmatan rangkaian hendaklah dijamin selamat dengan: (a) Menempatkan atau memasang antara muka (*firewall*) yang bersesuaian di antara rangkaian KLN, rangkaian agensi lain dan rangkaian awam; (b) Mewujudkan dan menguatkuasakan mekanisme untuk pengesahan pengguna dan peralatan yang menepati kesesuaian penggunaannya; dan	Pentadbir Sistem ICT dan ICTSO

(c) Memantau dan menguatkuasakan kawalan capaian pengguna terhadap perkhidmatan rangkaian ICT;	

07-03-02 Capaian Internet	
Keterangan	**T/jawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Penggunaan Internet di KLN hendaklah dipantau secara berterusan oleh Pentadbir Sistem ICT (Pentadbir Rangkaian) bagi memastikan capaian hanyalah tujuan penggunaan yang dibenarkan sahaja supaya keselamatan rangkaian KLN adalah terkawal; (b) *Content Filtering* digunakan bagi mengawal akses Internet mengikut fungsi kerja dan pemantauan tahap pematuhan; (c) Penggunaan teknologi (*packet shaper*) untuk mengawal aktiviti seperti video conferencing, video streaming, chat, downloading, adalah perlu bagi menguruskan penggunaan jalur lebar (*bandwidth*) yang maksimum dan lebih berkesan; (d) Penggunaan Internet hanyalah untuk kegunaan rasmi sahaja. (e) Laman yang dilayari hendaklah hanya yang berkaitan dengan bidang kerja dan terhad untuk tujuan yang dibenarkan oleh Ketua Jabatan/ pegawai yang diberi kuasa; (f) Bahan yang diperolehi 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 laman rasmi KLN; (h) Pengguna 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 KLN; (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 atau Ketua Jabatan/Bahagian terlebih dahulu tertakluk kepada dasar dan peraturan yang telah ditetapkan; (k) Penggunaan modem peribadi untuk tujuan sambungan ke Internet TIDAK DIBENARKAN sama sekali; dan (l) Pengguna adalah dilarang melakukan aktiviti-aktiviti peribadi	Pentadbir Sistem ICT dan Semua Pengguna ICT

dalam masa waktu bekerja seperti berikut:

(i) Memuat naik, memuat turun, menyimpan dan mengunakan perisian tidak berlesen dan sebarang aplikasi seperti permainan elektronik, video, lagu yang boleh menjejaskan tahap capaian Internet;

(ii) Menyedia, memuat naik, memuat turun dan menyimpan material, teks ucapan atau bahan-bahan yang mengandungi unsur-unsur lucah;

(iii) *Chatting* dan *blogging*; dan

(iv) Melayari dan mengaktifkan diri di laman web sosial (facebook, twitter, friendster dll).

07-04 Kawalan Capaian Ke Atas Sistem Pengoperasian

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

07-04-01 Capaian Sistem Pengoperasian

Nota Penting	Keterangan	T/jawab
Kawalan capaian sistem pengoperasian perlu bagi mengelakkan sebarang capaian yang tidak dibenarkan. Ciri-ciri keselamatan dalam sistem operasi perlu dilaksanakan untuk menghalang capaian ke sumber sistem komputer. Ciri-ciri termasuk seperti berikut: (a) Mengenai pasti identiti, terminal atau lokasi bagi setiap pengguna yang dibenarkan; (b) Merekodkan capaian yang berjaya dan gagal; Kaedah yang digunakan hendaklah mampu menyokong perkara-perkara berikut: (a) Mengesahkan pengguna yang dibenarkan; (b) Mewujudkan jejak audit ke atas semua capaian sistem pengoperasian terutama pengguna bertaraf *super user*; dan (c) Menjana amaran (*alert*) sekiranya berlaku perlanggaran ke atas peraturan keselamatan sistem. Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Mengawal capaian ke atas sistem pengoperasian menggunakan prosedur *login* yang terjamin; (b) Mewujudkan satu pengenalan diri (ID) yang unik untuk setiap pengguna dan hanya digunakan oleh pengguna berkenaan sahaja;		Pentadbir Sistem ICT

(c) Menghad dan mengawal penggunaan program aplikasi; dan	

07-04-02 Kad Pintar

Keterangan	T/jawab
Pekara-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 dbenarkan sama sekali; dan (d) Sebarang kehilangan, kerosakan dan kata laluan yang telah disekat perlu dimaklumkan kepada Jabatan yang berkaitan.	Semua Pengguna Kad Pintar

07-05 Kawalan Capaian Aplikasi dan Maklumat

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

07-05-01 Capaian Aplikasi dan Maklumat

Keterangan	T/jawab
Bertujuan melindungi sistem aplikasi dan maklumat sedia ada dari capaian yang tidak dibenarkan. Bagi memastikan kawalan capaian sistem dan aplikasi adalah kukuh, perkara-perkara berikut hendaklah dipatuhi: (a) Pengguna hanya boleh menggunakan sistem maklumat dan aplikasi yang dibenarkan mengikut tahap capaian dan keselamatan maklumat yang telah ditentukan; (b) Setiap aktiviti capaian sistem maklumat dan aplikasi pengguna hendaklah direkodkan (sistem log); (c) Memastikan kawalan sistem rangkaian adalah kukuh dan lengkap dengan ciri-ciri keselamatan bagi mengelakkan aktiviti atau capaian yang tidak sah; dan (d) Capaian sistem maklumat dan aplikasi melalui jarak jauh adalah dibenarkan. Walau bagaimanapun, penggunaannya terhad kepada perkhidmatan yang dibenarkan sahaja.	Pentadbir Sistem

07-06 Peralatan Mudah Alih dan Kerja Jarak Jauh

Objektif:
Memastikan keselamatan maklumat semasa menggunakan peralatan mudah alih dan kemudhan kerja jarak jauh.

07-06-01 Peralatan Mudah Alih	
Keterangan	**T/jawab**
Perkara yang perlu dipatuhi adalah seperti berikut: (a) Peralatan mudah alih hendaklah disimpan dan dikunci di tempat yang selamat apabila tidak digunakan.	Semua Pengguna ICT
07-06-02 Kerja Jarak Jauh	
Keterangan	**T/jawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Tindakan perlindungan hendak diambil bagi menghalang kehilangan peralatan, pendedahan maklumat dan capaian tidak sah serta salah guna kemudahan.	Semua Pengguna ICT

PERKARA 08
PEROLEHAN, PEMBANGUNAN DAN PENYENGGARAAN SISTEM

08-01 Keselamatan Dalam Membangunkan Sistem dan Aplikasi

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

08-01-01 Keperluan Keselamatan Sistem Maklumat

Keterangan	T/jawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perolehan, pembangunan, penambahbaikan dan penyenggaraan sistem hendaklah mengambil kira kawalan keselamatan bagi memastikan tidak wujud sebarang ralat yang boleh mengganggu pemprosessan dan ketepatan maklumat; (b) Ujian keselamatan hendaklah dijalankan ke atas sistem *input* untuk memastikan tidak wujudnya sebarang ralat yang boleh mengganggu pemprosesan dan ketepatan maklumat; (c) Aplikasi perlu mengandungi semakan pengesahan (*validation*) untuk mengelakkan sebarang kerosakan maklumat akibat kesilapan pemprosesan atau perlakuan yang disengajakan; dan (d) Semua sistem yang dibangunkan sama ada secara dalaman atau oleh pihak ketiga hendaklah diuji terlebih dahulu bagi memastikan sistem berkenaan memenuhi keperluan keselamatan yang telah ditetapkan sebelum digunakan.	Pentadbir Sistem (Pentadbir Sistem Aplikasi)

08-01-02 Pengesahan Data Input dan Output

Keterangan	T/jawab
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Data *input* bagi aplikasi perlu disemak dan disahkan bagi memastikan data yang dimasukkan betul dan bersesuaian; dan b) Data *output* daripada aplikasi perlu disemak dan disahkan bagi memastikan maklumat yang dihasilkan adalah tepat.	Pemilik Sistem

08-02 Kawalan Kriptografi

Objektif:
Melindungi kerahsiaan, integriti dan kesahihan maklumat melalui kawalan kriptografi.

08-02-01 Enkripsi

Keterangan	T/jawab
Pengguna hendaklah membuat enkripsi (*encryption*) ke atas maklumat sensitif atau maklumat rahsia pada setiap masa.	Semua Pengguna SPIDER

08-02-02 Tandatangan Digital	
Keterangan	**T/jawab**
Penggunaan tandatangan digital adalah digalakkan kepada semua pengguna khususnya mereka yang menguruskan transaksi maklumat rahsia rasmi secara elektronik.	Semua Pengguna ICT

08-02-03 Pengurusan Infrastruktur Kunci Awam (PKI)	
Keterangan	**T/jawab**
Pengurusan ke atas PKI hendaklah dilakukan dengan berkesan dan selamat bagi melindungi kunci berkenaan dari diubah, dimusnah dan didedahkan sepanjang tempoh sah kunci tersebut.	Semua Pengguna ICT

08-03 Keselamatan Sistem Fail

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

08-03-01 Kawalan Fail Pengaturcaraan (*Source Code*)	
Keterangan	**T/jawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Proses pengemaskinian *source code* hanya boleh dilakukan oleh Pentadbir Sistem ICT atau pegawai yang berkenaan mengikut prosedur yang telah ditetapkan; (b) Kod atau atur cara sistem yang telah dikemas kini hanya boleh dilaksanakan atau digunakan selepas diuji; (c) Mengawal capaian ke atas kod atau atur cara program bagi mengelakkan kerosakan, pengubahsuaian tanpa kebenaran, penghapusan dan kecurian; (d) Data ujian perlu dipilih dengan berhati-hati, dilindungi dan dikawal; dan (e) Mewujudkan log bagi merekodkan semua aktiviti pengemaskinian untuk tujuan statistik, pemulihan dan keselamatan.	Pentadbir Sistem ICT

08-04 Keselamatan Dalam Proses Pembangunan dan Sokongan

Objektif:
Menjaga dan menjamin keselamatan sistem maklumat dan aplikasi.

08-04-01 Prosedur Kawalan Perubahan	
Keterangan	**T/jawab**
Perkara-perkara yang perlu dipatuhi adalah seperti berikut: (a) Perubahan atau pengubahsuaian ke atas sistem maklumat dan aplikasi hendaklah dikawal, diuji, direkodkan dan disahkan sebelum diguna pakai; (b) Aplikasi kritikal perlu dikaji semula dan diuji apabila terdapat perubahan kepada sistem pengoperasian untuk memastikan tiada	Pentadbir Sistem ICT dan Pengguna Sistem

kesan buruk terhadap operasi dan keselamatan agensi. Individu atau suatu kumpulan tertentu perlu bertanggungjawab memantau penambahbaikan dan pembetulan yang dilakukan oleh *vendor*; (c) Mengawal perubahan dan/atau pindaan ke atas perisian dan memastikan sebarang perubahan adalah terhad mengikut keperluan sahaja; (d) Akses kepada *source code* aplikasi perlu dihadkan kepada pengguna yang diizinkan; dan (e) Memastikan perubahan tidak menyebabkan pembocoran maklumat.	
08-04-02 Pembangunan Perisian Secara Outsource	
Keterangan	**T/jawab**
Pembangunan perisian secara *outsource* perlu diselia dan dipantau oleh pentadbir sistem. Kod sumber (*source code*) bagi semua aplikasi dan perisian adalah menjadi hak milik Kerajaan.	Pentadbir Sistem ICT (Pentadbir Sistem Aplikasi)
08-05 Kawalan Teknikal Keterdedahan (Vulnerability)	
Objektif: Memastikan kawalan teknikal keterdedahan adalah berkesan, sistematik dan berkala dengan mengambil langkah-langkah yang bersesuaian untuk menjamin keberkesanannya.	
08-05-01 Kawalan dari Ancaman Teknikal	
Keterangan	**T/jawab**
Kawalan teknikal keterdedahan ini perlu dilaksanakan ke atas sistem pengoperasian dan sistem aplikasi yang digunakan. Perkara yang perlu dipatuhi adalah seperti berikut: (a) Memperoleh maklumat teknikal keterdedahan yang tepat pada masanya ke atas sistem maklumat yang digunakan; (b) Menilai tahap pendedahan bagi mengenal pasti tahap risiko yang bakal dihadapi; dan (c) Mengambil langkah-langkah kawalan untuk mengatasi risiko berkaitan.	Pentadbir Sistem ICT dan CERT KLN

PERKARA 09

PENGURUSAN PENGENDALIAN INSIDEN KESELAMATAN

09-01 Mekanisme Pelaporan Insiden Keselamatan ICT

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

09-01-01 Mekanisme Pelaporan

Keterangan	T/jawab
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 KLN sama ada yang ditetapkan secara tersurat atau tersirat. Insiden keselamatan ICT seperti berikut hendaklah dilaporkan kepada ICTSO dan CERT KLN dengan kadar segera: (a) Maklumat didapati hilang/disyaki hilang/didedahkan kepada pihak-pihak yang tidak diberi kuasa; (b) Sistem maklumat digunakan tanpa kebenaran atau disyaki sedemikian; (c) Kata laluan atau mekanisme kawalan akses hilang/disyaki hilang/dicuri/didedahkan; (d) Berlaku kejadian sistem yang luar biasa seperti kehilangan fail, sistem kerap kali gagal dan komunikasi tersalah hantar; dan (e) Berlaku percubaan menceroboh, menyeleweng dan insiden-insiden berisiko yang tidak dijangka. Prosedur pelaporan insiden keselamatan ICT berdasarkan: (a) Pekeliling Am Bilangan 1 Tahun 2001 – Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi; dan (b) Surat Pekeliling Am Bilangan 4 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi Sektor Awam.	CERT KLN dan Semua Pengguna ICT

09-02 Pengurusan Maklumat Insiden Keselamatan ICT

Objektif:

Memastikan sistem yang dibangunkan sendiri atau pihak ketiga mempunyai ciri-ciri keselamatan ICT yang bersesuaian.

09-02-01 Keperluan Keselamatan Sistem Maklumat	
Keterangan	**T/jawab**
Maklumat mengenai insiden keselamatan ICT yang dikendalikan perlu disimpan dan dianalisis bagi tujuan perancangan, tindakan pengukuhan dan pembelajaran bagi mengawal kekerapan, kerosakan dan kos baikpulih kejadian insiden. Maklumat ini juga digunakan untuk mengenal pasti insiden yang akan datang, mengenal pasti insiden yang kerap berlaku atau yang memberi kesan serta impak yang tinggi kepada KLN. Bahan-bahan bukti berkaitan insiden keselamatan ICT hendaklah disimpan dan disenggarakan. Kawalan-kawalan yang perlu diambil kira dalam pengumpulan maklumat dan pengurusan pengendalian insiden adalah seperti berikut: (a) Menyimpan jejak audit, *backup* secara berkala dan melindungi integriti semua bahan bukti; (b) Menyalin bahan bukti dan merekodkan semua maklumat aktiviti penyalinan; (c) Menyediakan pelan kontigensi dan mengaktifkan pelan kesinambungan perkhidmatan; (d) Menyediakan tindakan pemulihan segera; dan (e) Memaklumkan atau mendapatkan nasihat pihak berkuasa perundangan sekiranya perlu.	CERT KLN dan Bahagian Pentadbiran dan Keselamatan

PERKARA 10
PENGURUSAN KESINAMBUNGAN PERKHIDMATAN

10-01 Dasar Kesinambungan Perkhidmatan

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

10-01-01 Pelan Kesinambungan Perkhidmatan

Keterangan	T/jawab
Pelan Kesinambungan Perkhidmatan (*Business Continuity Plan – BCP*) hendaklah dibangunkan untuk menentukan pendekatan yang menyeluruh diambil bagi mengekalkan kesinambungan perkhidmatan. Ini bertujuan memastikan tiada gangguan kepada proses-proses dalam penyediaan perkhidmatan organisasi. Pelan ini mestilah diluluskan oleh JPICT KLN. Perkara-perkara berikut perlu dberi perhatian: (a) Mengenal pasti semua tanggungjawab dan prosedur kecemasan atau pemulihan; (b) Mengenal pasti peristiwa yang boleh mengakibatkan gangguan terhadap proses bisnes KLN yang berkemungkinan memberi impak terhadap keselamatan ICT KLN; (c) Melaksanakan prosedur-prosedur kecemasan bagi membolehkan pemulihan dapat dilakukan secepat mungkin atau dalam jangka masa yang telah ditetapkan; (d) Mendokumentasikan proses dan prosedur yang telah dipersetujui; (e) Mengadakan program latihan kepada pengguna mengenai prosedur kecemasan; (f) Membuat *backup*; dan (g) Menguji dan mengemas kini pelan sekurang-kurangnya setahun sekali. Pelan BCP perlu dibangunkan dan hendaklah mengandungi perkara-perkara berikut: (a) Senarai aktiviti teras yang dianggap kritikal mengikut susunan keutamaan; (b) Senarai personel KLN dan *vendor* beserta nombor yang boleh dihubungi (faksimili, telefon dan e-mel). Senarai kedua juga hendaklah disediakan sebagai menggantikan personel yang	Bahagian ICT, Bahagian Pentadbiran dan Keselamatan dan Pemilik Sistem

tidak dapat hadir untuk menangani insiden; (c) Senarai lengkap maklumat yang memerlukan *backup* dan lokasi sebenar penyimpanannya serta arahan pemulihan maklumat dan kemudahan yang berkaitan; (d) Alternatif sumber pemprosesan dan lokasi untuk menggantikan sumber yang telah lumpuh; dan (e) Perjanjian dengan pembekal perkhidmatan untuk mendapatkan keutamaan penyambungan semula perkhidmatan. Salinan BCP perlu disimpan di lokasi yang berasingan untuk mengelakkan kerosakan akibat bencana di lokasi utama. BCP hendalah diuji sekurang-kurangnya sekali setahun atau apabila terdapat perubahan dalam persekitaran atau fungsi bisnes untuk memastikan ianya sentiasa kekal berkesan. Penilaian secara berkala hendaklah dilaksanakan untuk memastikan pelan tersebut bersesuaian dan memenuhi tujuan dibangunkan. Ujian BCP hendaklah dijadualkan untuk memastikan semua ahli dalam pemulihan dan personel yang terlibat mengetahui mengenai pelan tersebut, tanggungjawab dan peranan mereka apabila pelan dilaksanakan. Salinan BCP hendaklah sentiasa di kemas kini dan dilindungi sama seperti di lokasi utama.	

PERKARA 11
PEMATUHAN

11-01 Pematuhan dan Keperluan Perundangan

Objektif:
Meningkatkan tahap keselamatan ICT bagi mengelak dari perlanggaran kepada Dasar Keselamatan ICT KLN

11-01-01 Pematuhan Dasar

Keterangan	T/jawab
(a) Setiap pengguna di KLN hendaklah membaca, memahami Dasar Keselamatan ICT KLN dan undang-undang atau peraturan-peraturan lain yang berkaitan yang berkuat kuasa. (b) Setiap pengguna perlu memastikan reka bentuk, operasi, penggunaan dan pengurusan sistem maklumat adalah selaras serta berkeupayaan menghalang perlanggaran mana-mana keperluan perundangan, peraturan dan perjanjian yang berkuat kuasa. (c) Semua aset ICT di KLN termasuk maklumat yang disimpan di dalamnya adalah hak milik Kerajaan. Ketua Jabatan/Bahagian atau pegawai yang diberi kuasa berhak untuk memantau aktiviti pengguna untuk mengesan penggunaan selain dari tujuan yang telah ditetapkan. (d) Sebarang penggunaan aset ICT KLN selain daripada maksud dan tujuan yang telah ditetapkan, adalah merupakan satu penyalahgunaan sumber KLN.	Semua Pengguna ICT

11-01-02 Pematuhan dengan Dasar, Piawaian dan Keperluan Teknikal

Keterangan	T/jawab
(a) ICTSO hendaklah memastikan semua prosedur keselamatan dalam bidang tugas masing-masing mematuhi dasar, piawaian dan keperluan teknikal. (b) Sistem maklumat perlu diperiksa secara berkala bagi mematuhi standard pelaksanaan keselamatan ICT.	ICTSO

11-01-03 Pematuhan Keperluan Audit

Keterangan	T/jawab
Pematuhan kepada keperluan audit perlu bagi meminimumkan ancaman dan memaksimumkan keberkesanan dalam proses audit sistem maklumat. Keperluan audit dan sebarang aktiviti pemeriksaan ke atas sistem operasi perlu dirancang dan dipersetujui bagi mengurangkan kebarangkalian berlaku gangguan dalam penyediaan	Semua Pengguna ICT

perkhidmatan. Capaian ke atas peralatan audit sistem maklumat perlu dijaga dan diselia bagi mengelakkan berlaku penyalahgunaan.	
11-01-04 Keperluan Perundangan	
Keterangan	**T/jawab**
Berikut adalah keperluan perundangan atau peraturan-peraturan lain berkaitan yang perlu dipatuhi oleh semua pengguna di jabatan: (a) Arahan keselamatan; (b) Pekeliling Am Bilangan 3 Tahun 2000 – "Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan"; (c) Pekeliling Am Bilangan 1 Tahun 2001 – "Mekanisme Pelaporan Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT)"; (d) Pekeliling Kemajuan Pentadbiran Awam Bilangan 1 Tahun 2003 – "Garis Panduan Mengenai Tatacara Penggunaan Internet dan Mel Elektronik di Agensi-agensi Kerajaan"; (e) Surat Pekeliling Am Bilangan 6 Tahun 2005 - "Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam"; (f) Surat Pekeliling Am Bilangan 6 Tahun 2006 – Pengurusan Pengendalian Insiden Keselamatan Teknologi Maklumat dan Komunikasi (ICT) Sektor Awam; (g) Surat Arahan Ketua Setiausaha Negara – Langkah-Langkah Untuk Memperkukuhkan Keselamatan Rangkaian Setempat Tanpa Wayar (*Wireless Local Area Network*) di Agensi-Agensi Kerajaan yang bertarikh 20 Oktober 2006. (h) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Mengenai Penggunaan Mel Elektronik di Agensi-Agensi Kerajaan yang bertarikh 1 Jun 2007; (i) Surat Arahan Ketua Pengarah MAMPU – Langkah-Langkah Pemantapan Pelaksanaan Sistem Mel Elektronik Di Agensi-Agensi Kerajaan yang bertarikh 23 November 2007; (j) Surat Pekeliling Am Bil. 2 Tahun 2000 – Peranan Jawatankuasa-jawatankuasa di Bawah Jawatankuasa IT dan Internet Kerajaan (JITIK); (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) *Malaysian Public Sector Management of Information and Communications Technology Security Handbook* (MyMIS);	Semua Pengguna ICT

(n) Akta Tanda Tangan Digital 1997; (o) Akta Rahsia Rasmi 1972; (p) Akta Jenayah Komputer 1997; (q) Akta Hak Cipta (Pindaan) Tahun 1997; (r) Akta Komunikasi dan Multimedia 1998; (s) Perintah-Perintah Am; (t) Arahan Perbendaharaan; (u) Arahan Teknologi Maklumat 2007; (v) Garis Panduan Keselamatan MAMPU 2004; (w) Standard Operating Procedure (SOP) ICT MAMPU; (x) Surat Pekeliling Am Bilangan 3 Tahun 2009 – Garis Panduan Penilaian Tahap Keselamatan Rangkaian dan Sistem ICT Sektor Awam yang bertarikh 17 November 2009; (y) Surat Arahan Ketua Pengarah MAMPU – Pengurusan Kesinambungan Perkhidmatan Agensi Sektor Awam yang bertarikh 22 Januari 2010.	

11-01-05 Perlanggaran Dasar	
Keterangan	**T/jawab**
Perlanggaran Dasar Keselamatan ICT KLN boleh dikenakan tindakan tatatertib.	Semua pengguna ICT

LAMPIRAN 1

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT

BAGI PENJAWAT AWAM DI KEMENTERIAN LUAR NEGERI

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

Adalah dengan sesungguhnya dan sebenarnya saya mengaku bahawa :-

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

Tanda tangan :
Tarikh :

Pengesahan Pegawai Keselamatan ICT KLN

.....
Nama:
b.p. Ketua Setiausaha KLN
Tarikh :

LAMPIRAN 2

SURAT AKUAN PEMATUHAN DASAR KESELAMATAN ICT

BAGI PIHAK KETIGA DI KEMENTERIAN LUAR NEGERI

Nama (Huruf Besar) :
No Kad Pengenalan :
Jawatan :
Syarikat :

Adalah dengan sesungguhnya dan sebenarnya saya mengaku bahawa :-

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

Tanda tangan :
Tarikh :

Pengesahan Pegawai Keselamatan ICT KLN

.....
Nama:
b.p. Ketua Setiausaha KLN
Tarikh :

GLOSARI

Antivirus	Perisian yang mengimbas virus pada media storan seperti disket, cakera padat, pita magnetik, *optical disk*, CDROM, *pendrive* untuk sebarang kemungkinan adanya virus.
Aset ICT	Peralatan ICT termasuk perkakasan, perisian, perkhidmatan, data atau maklumat dan manusia.
Backup	Proses penduaan sesuatu dokumen atau maklumat.
Bandwidth	Lebar Jalur Ukuran atau jumlah data yang boleh dipindahkan melalui kawalan komunikasi (contoh di antara cakera keras dan komputer) dalam jangka masa yang ditetapkan.
BICT	Bahagian Teknologi Maklumat dan Komunikasi
CIO	*Chief Information Officer* Ketua Pegawai Maklumat yang bertanggungjawab terhadap ICT dan sistem maklumat bagi menyokong arah tuju sesebuah organisasi. Timbalan Ketua Setiausaha III, KLN
Denial of service	Halangan pemberian perkhidmatan.
Downloading	Aktiviti muat-turun sesuatu perisian.
Encryption	Enkripsi ialah satu proses penyulitan data oleh pengirim supaya tidak difahami oleh orang lain kecuali penerima yang sah.
Firewall	Sistem yang direka bentuk 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 e-mel termasuk penyalahgunaan dan pencurian identiti, pencurian maklumat (*information theft/espionage)*, penipuan (*hoaxes)*.
GCERT	*Government Computer Emergency Responce Team* atau Pasukan Tindak Balas Insiden Keselamatan ICT Kerajaan. Organisasi yang ditubuhkan untuk membantu agensi mengurus pengendalian insiden keselamatan ICT di agensi masing-masing dan agensi di bawah kawalannya.
Hard disk	Cakera keras. Digunakan untuk menyimpan data dan boleh di akses lebih pantas.
Hub	Hab (*hub*) 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* (Teknologi Maklumat dan Komunikasi).
ICTSO	*ICT Security Officer* – Pegawai Keselamatan ICT Pegawai Keselamatan ICT, KLN adalah Timbalan Setiausaha Bahagian BICT, KLN
Internet	Sistem rangkaian seluruh dunia, dimana pengguna boleh membuat capaian maklumat daripada pelayan (server) atau komputer lain.
Internet Gateway	Merupakan suatu titik yang berperanan sebagai pintu masuk ke rangkaian 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 bertindak balas menyekat atau menghalang aktiviti serangan atau malicious code. Contohnya *Network-based IPS* yang akan memantau semua trafik rangkaian bagi sebarang kemungkinan serangan.
KLN	Kementerian Luar Negeri
Pemilik Sistem	Bahagian/Jabatan yang memiliki dan menggunakan sistem aplikasi khusus bagi menjalankan kerja-kerja operasi harian.
Pengendali Aset ICT	Pegawai yang bertanggungjawab mengendalikan inventori aset-aset ICT di Wisma Putra.
Pengguna ICT	Pegawai KLN atau pihak lain yang diberi kelulusan oleh KSU atau CIO untuk menggunakan kemudahan ICT di KLN.
Pentadbir Sistem ICT	Pengurus Projek / Pentadbir Rangkaian / Pentadbir Sistem Aplikasi / Pentadbi Pangkalan Data / Pengurus Pusat Data
Pihak Luar/ Ketiga	Kontraktor, Pembekal dan lain-lain pihak yang berkepentingan.
LAN	Rangkaian Kawasan Luas termasuk MOFA* Net dan agensi-agensi di bawah kawalan KLN.
Logout	*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 DEModular 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	Bermaksud menggunakan perkhidmatan luar untuk melaksanakan fungsi-fungsi tertentu ICT bagi suatu tempoh berdasarkan kepada dokumen perjanjian dengan bayaran yang dipersetujui.
Perisian Aplikasi	Ia merujuk pada perisian atau pakej yang selalu digunakan seperti *spreedsheet* dan *word processing* ataupun sistem aplikasi yang dibangunkan oleh sesebuah organisasi atau jabatan.
Public-Key Infrastructure (PKI)	Infrastruktur Kunci Awam merupakan satu kombinasi perisian teknologi enkripsi dan perkhidmatan yang membolehkan organisasi melindungi keselamatan berkomunikasi dan transaksi melalui Internet.
Router	Penghala yang digunakan untuk menhantar 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 komputer
Switches	Suis merupakan gabungan hab dan titi yang manapis bingkai supaya mensegmenkan rangkaian .

	Kegunaan suis dapat meperbaiki prestasi rangkaian *Carrier Sense Multiple Access/Collision Detection* (CSMA/CS) yang merupakan satu protokol penghantaran dengan menguragnkan perlanggaran yang berlaku.
Threat	Gangguan dan ancaman melalui pelbagai cara iaitu e-mel dan surat yang bermotif perosonal dan atas sebab tertentu.
Uninterruptible Power Supply (UPS)	Satu peralatan yang digunakan bagi membekalkan bekalan kuasa yang berterusan dari sumber berlainan ketika ketiadaan bekaln kuasa ke peralatan yang bersambung.
Video Conferencing	Media yang menerima dan memaparkan maklumat multimedia kepada pengguna dalam masa yang sama ia diterima oleh penghantar.
Video streaming	Teknologi komunikasi yang interaktif yang membenarkan dua atau lebih lokasi untuk berinteraksi melalui paparan video dua hala dan audio secara serentak.
Virus	Atur cara yang bertujuan merosakkan data atau sistem aplikasi.
Wireless LAN	Jaringan komputer yang terhubung tanpa melalui kabel.